MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

ESTUDO TÉCNICO PRELIMINAR - ETP Nº 7.2025.DTIC.1591885.2025.007562

1. INFORMAÇÕES BÁSICAS

O presente Estudo Técnico Preliminar (ETP) tem por finalidade apresentar a análise da necessidade de contratação de equipamentos e soluções de Tecnologia da Informação e Comunicação (TIC) com vistas à substituição dos equipamentos do atual ambiente de datacenter do MPAM. Tal iniciativa visa garantir a continuidade dos serviços essenciais, uma vez que parte significativa dos ativos de TIC utilizados em ambiente de datacenter encontra-se em situação crítica, com equipamentos que já ultrapassaram o período de suporte ativo pelos fabricantes (end of life), tornando-se obsoletos do ponto de vista técnico e funcional. Essa condição implica riscos relevantes à operação institucional, tais como falhas operacionais e indisponibilidade de sistemas.

Categoria que se enquadra o ETP: CONTRATAÇÕES DE TIC

Alinhamento ao plano institucional:

A contratação pretendida alinha-se ao definido no Plano Estratégico 2017-2027 do MPAM, por meio dos seguintes objetivos e iniciativas estratégicas:

- Objetivo 3.02 - Aprimorar a infraestrutura, gestão e governança de tecnologia da informação.
- Iniciativa estratégica 3.02.2.3 - Elaborar e implementar projeto de modernização do datacenter.

2. NECESSIDADE DA CONTRATAÇÃO

Em 2019, foi celebrado o Contrato Administrativo n. 006/2019 - MP/PGJ (SEI0299031), para o Sistema de Automação da Justiça para o Ministério Público - SAJ-MP. Paralelamente, foi adquirida uma solução de software e hardware para processamento e armazenamento de dados que suportasse as demandas requeridas pelo SAJ-MP e demais sistemas computacionais da instituição - Solução Nutanix de Hiperconvergência, através do Contrato Administrativo n. 010/2018 - MP/PGJ (SEI 0210232).

Ocorre, entretanto, que desde sua formação, o Ministério Público do Amazonas nunca contou com uma infraestrutura física adequada e exclusiva para a operação de seus ativos de processamento e armazenamento de dados responsáveis por seus sistemas computacionais - Datacenter.

O espaço reservado na Diretoria de Tecnologia da Informação (DTIC) para este fim não conta com a estrutura mínima recomendada para esta aplicação - caracterizando-se por uma sala improvisada com paredes de gesso acartonado, que não garantem segurança física, sem sistema de refrigeração adequado, sem proteção contra incêndio e demais sinistros, sem sistema de vigilância, controle de acesso ou monitoramento adequado.

Em 2020, para aumentar a capacidade de processamento e armazenamento, foi adquirido mais um servidor que fora incorporado à solução de Nutanix de Hiperconvergência, através do Contrato Administrativo n. 020/2020 - MP/PGJ, SEI 0572982.

A infraestrutura de hardware e software adquirida foi instalada no espaço físico mencionado e desde então segue em operação.

Esta é a infraestrutura física e computacional sobre a qual se mantêm os sistemas computacionais do MPAM, atualmente em situação crítica, com equipamentos que já ultrapassaram o período de suporte ativo pelos fabricantes (end of life), tornando-se obsoletos do ponto de vista técnico e funcional. Essa condição, como já mencionado, implica riscos relevantes à operação institucional, tais como falhas operacionais, indisponibilidade de sistemas e impossibilidade de atualização tecnológica.

Além disso, as aplicações institucionais em uso pelo MPAM estão em constante evolução, exigindo maior desempenho, escalabilidade e disponibilidade de recursos computacionais. A atual infraestrutura hiperconvergente, embora eficaz em sua concepção, já não atende plenamente às demandas atuais e futuras, especialmente diante da necessidade de implantação de novos sistemas e da manutenção dos já existentes.

Diante desse cenário, este ETP busca fundamentar a contratação de uma solução plataforma NUTANIX, com equipamentos em garantia técnica e alinhados às necessidades imediatas do órgão, de forma a promover a continuidade dos serviços e a proteção de dados institucionais.

2.1 Situação Atual do Datacenter

Em termos de equipamentos de processamento e armazenamento o atual datacenter do MPAM é composto pelos seguintes equipamentos em um único cluster NUTANIX:

-	Geração/ Modelo NUTANIX	Qtd Nós	Suporte
	G5 - 8035	2	Expirado

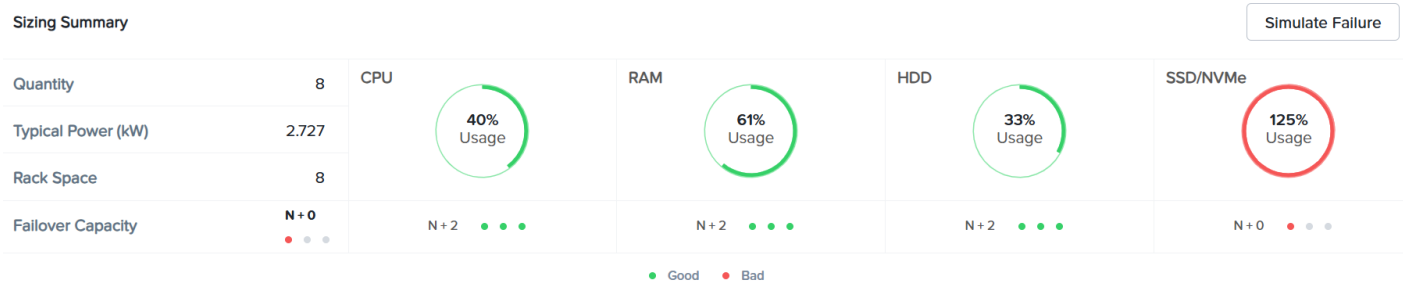
ESTRUTURA EXISTENTE	Geração/ Modelo NUTANIX	Qtd Nós	Suporte
DATACENTER MPAM	G5 - 8035	2	Expirado
	G5 - 8035	2	Expirado
	G7 - 8035	2	Expirado
	-	8	-

A análise detalhada do quadro apresentado evidencia a necessidade de ações estratégicas relacionadas à substituição dos servidores e software de virtualização com suporte expirado. O cluster NUTANIX composto por servidores do modelo NX-8035-G5 e NX-8035-G7, encontra-se em uma situação crítica devido à expiração da garantia e suporte técnico. Essa condição expõe a infraestrutura a riscos operacionais elevados, pois, sem o suporte do fabricante, não há garantia de assistência técnica em casos de falha, atualização de firmware ou correção de vulnerabilidades.

O cluster NUTANIX de produção apresenta uma capacidade reduzida o que destaca ainda mais a necessidade de substituição dos servidores, já que qualquer falha nesse cluster comprometeria diretamente a recuperação de sistemas críticos. Diante desse cenário, a substituição imediata dos servidores do referido cluster é essencial para assegurar a confiabilidade e a continuidade operacional.

Do ponto de vista técnico, a substituição dos servidores com suporte expirado evita a dependência de equipamentos obsoletos, promovendo maior eficiência e confiabilidade com a adoção de tecnologias mais recentes.

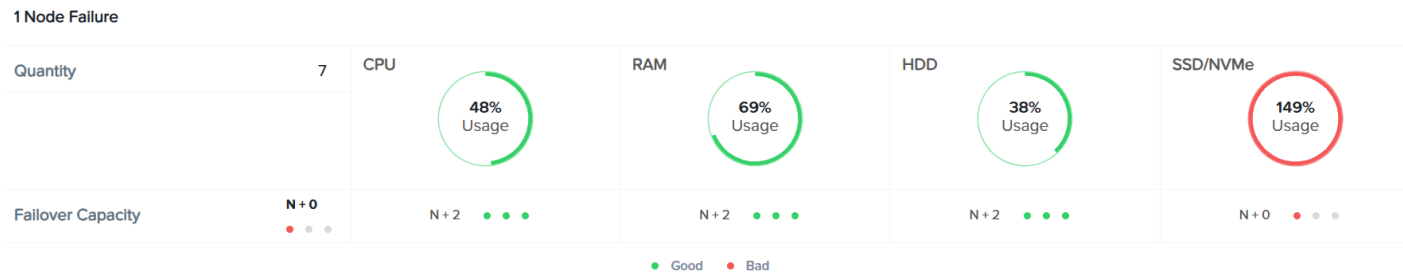
Atualmente, o cluster NUTANIX apresenta uma taxa de consumo de armazenamento em buffer em torno de 125%, o que reduz drasticamente a margem para crescer o ambiente e realizar práticas de proteção de dados e buffer para desempenho. Além disso, o uso de memória encontra-se em 63%, apontando para uma futura limitação na capacidade de absorver novas cargas de trabalho ou eventuais picos de demanda sem comprometer a estabilidade dos sistemas.



Um aspecto crítico a ser considerado é a resiliência do ambiente, que encontra-se 25% acima do seu limite projetado, ou seja com 125%, além da perda de desempenho associado. Nessas circunstâncias, é imperativo destacar que os nós não são capazes de suportar integralmente a carga de trabalho. Contudo, tal cenário se torna desafiador, o ambiente já opera próximo ao limite de memória e acima do armazenamento de buffer, comprometendo, assim, o desempenho – um requisito essencial em ambientes corporativos que demandam operação contínua e confiável.

Alta ocupação da camada de dados de alta velocidade (SSD/NVMe), que atualmente está acima do limite projetado, resulta em gargalos no acesso rápido às informações mais utilizadas, comprometendo a eficiência das operações e o tempo de resposta das aplicações institucionais.

Um aspecto crítico a ser considerado é a resiliência do ambiente em situações de perda/falha temporária de um dos nós do cluster, onde nessas circunstâncias, é imprescindível que os nós remanescentes sejam capazes de suportar integralmente alta ocupação da camada de dados de alta velocidade sem a insterrupção de qualquer serviço ou sistema.



Em cenários de falha ou manutenção de um dos nós, a atual utilização de recursos pode tornar inviável uma redistribuição das cargas sem afetar a performance do ambiente como um todo. Além disso, a disponibilidade limitada de recursos em discos de alta velocidade afeta diretamente o desempenho geral do ambiente, reduzindo a capacidade de atender a picos de carga e de manter operações em níveis ideais. Para sustentar a performance, é fundamental que a camada de armazenamento rápido opere com margens adequadas, assegurando tempos de resposta rápidos e suporte eficiente a aplicações de alta demanda. Isso garante que o ambiente se mantenha estável e funcional mesmo em cenários de uso intensivo.

Em termos de softwares e licenciamentos do cluster NUTANIX, o atual datacenter do MPAM é composto pelos seguintes itens:

a) Prism PRO para o controle e gerenciamento do cluster NUTANIX;

b) Software para backup e restore de VMs e dados.

2.1 Proposta para o Datacenter

A renovação tecnológica dos equipamentos do Datacenter proporcionará aumento significativo no throughput de sistemas críticos, redução de tempos de resposta e maior eficiência operacional, ao mesmo tempo que assegura a extensão do ciclo de vida de forma planejada e seguindo as melhores práticas de gestão de infraestrutura.

Processadores de última geração, assim como arquiteturas otimizadas para cargas intensivas de trabalho, são necessários para lidar com a execução de consultas complexas e o processamento paralelo de grandes volumes de dados. A estimativa da quantidade de recursos necessários para a execução do projeto foi realizada com base no conhecimento técnico consolidado a partir do atual cluster NUTANIX em produção, que forneceu dados concretos sobre o desempenho, a capacidade de armazenamento e as necessidades operacionais, permitindo uma análise detalhada para dimensionar os recursos propostos de forma precisa.

Dentre as opções de servidores disponibilizadas pelo fabricante, foram priorizadas configurações que oferecem maior capacidade de armazenamento, empregando equipamentos híbridos com discos mecânicos HDD. Essa decisão visa garantir uma maior volumetria disponível, aliada à economicidade, atendendo às demandas do projeto de forma eficiente e sustentável.

Foi selecionada, dentre as configurações disponíveis, uma opção de servidor equipada com unidade de processamento gráfico (GPU), projetada para suportar cargas de trabalho intensivas e ambientes computacionais mais exigentes. A inclusão deste recurso visa atender demandas específicas de processamento paralelo, aceleração gráfica e algoritmos avançados, comuns em aplicações como inteligência artificial, virtualização com uso intensivo de gráficos, simulações e análise de grandes volumes de dados. A escolha leva em consideração a necessidade de desempenho elevado com eficiência energética e compatibilidade com a arquitetura existente, permitindo expansão futura e garantindo que os recursos computacionais estejam adequados à complexidade crescente dos serviços institucionais.

A seguir apresenta-se a estimativa de contratação de solução com equipamentos e softwares para uma infraestrutura de nuvem privada na plataforma NUTANIX:

ITEM	DESCRIÇÃO	QUANTIDADE
1	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9	4
2	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU	1
3	SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX	5
4	SOFTWARE DE PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU	2
5	LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE	30
6	SOFTWARE DE BACKUP DE DADOS	1
7	EQUIPAMENTO PARA ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	1
8	SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	1
9	SWITCH CORE	2

3. UNIDADE DEMANDANTE

A unidade demandante é a Diretoria de Tecnologia, Informação e Comunicação - DTIC.

4. REQUISITOS DA CONTRATAÇÃO

4.1 Necessidades Técnologicas

a) Alta resiliência operacional e continuidade dos serviços

b) Otimização do desempenho dos sistemas institucionais

c) Proteção robusta contra falhas e ataques cibernéticos

d) Expansão modular sem necessidade de reestruturação

e) Interface de gerenciamento centralizada

f) Escalabilidade e Otimização de Recursos

g) Gerenciamento centralizado baseado em software

h) Alta eficiência operacional

i) Integração com o ambiente Hiperconvergente atual.

j) Todos os equipamentos a serem utilizados deverão pertencer à mesma plataforma de servidores (NUTANIX) atualmente em uso no órgão.

4.2 Requisitos Externos

a) Lei Federal nº. 14.133, que estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios, de 01/04/2021;

b) Ato PGJ Nº 008/2024, que define os procedimentos administrativos de contratação de bens e serviços no âmbito do Ministério Público do Amazonas os quais se realizarão por meio de etapas e atos estruturados de forma lógica para a consecução do interesse público envolvido;

4.3 Requisitos de Qualidade de Serviço

a) Garantia do FABRICANTE inclusa, com assistência técnica remota em regime contínuo, 24x7x365, durante toda a vigência contratual;

b) Garantia da CONTRATADA inclusa, com assistência técnica remota em regime contínuo, 24x7x365, durante toda a vigência contratual;

c) Reposição de componentes defeituosos conforme requisitos de níveis mínimos de serviço.

4.4 Requisitos Operacionais

A contratação, visa a efetividade e operacionalização, conforme abaixo:

a) Implantação e configuração da solução;

b) Migração do ambiente atual para o novo ambiente contratado;

c) Garantia e atualização por 60 (sessenta) meses;

d) Suporte técnico por 60 (sessenta) meses.

4.5 Requisitos de Segurança

a) A Contratada deve seguir as orientações de segurança do MPAM e legislação pertinente ao assunto.

b) A Contratada deverá submeter-se aos procedimentos contidos nas normas de segurança corporativa do MPAM e da administração pública em todos os eventos em que for necessária a presença de seus prepostos e/ou funcionários em suas dependências.

c) A Contratada deverá exigir dos seus empregados, quando em serviço nas dependências da Contratante, o uso obrigatório de uniformes e crachás de identificação.

d) A Contratada não poderá se utilizar da presente contratação para obter qualquer acesso não autorizado às informações de propriedade da Contratante.

e) A Contratada deverá assinar o Termo de Compromisso, e seus funcionários alocados na prestação de serviços, o Termo de Ciência, conforme definido no Termo de Referência.

f) A Contratada deverá comunicar imediatamente à Contratante qualquer ocorrência de transferência, remanejamento ou demissão de funcionários envolvidos diretamente na execução do objeto, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do Contratante, porventura colocados à disposição para realização dos serviços contratados.

4.6 Requisitos de Arquitetura Tecnológica

a) Escalabilidade: A nova contratação do ambiente deve ser dimensionada considerando o aumento da capacidade de processamento, armazenamento e análise de dados, acompanhando as demandas em constante evolução.

b) Resiliência: A arquitetura deve ser projetada para garantir a continuidade das aplicações e sistemas mesmo diante de falhas ou interrupções. Deve incluir mecanismos de redundância, recuperação e alta disponibilidade para minimizar o impacto de eventos adversos no funcionamento das ferramentas.

c) Segurança: A nova contratação do ambiente deve seguir boas práticas de segurança e adotar medidas robustas para proteger os dados e garantir a confidencialidade, integridade e disponibilidade das informações.

d) Monitoramento e análise: A nova contratação do ambiente deve permitir o monitoramento em tempo real.

e) Usabilidade: A nova contratação do ambiente deve permitir a total integração com as ferramentas de gerenciamento atualmente em uso no ambiente de nuvem privada segura do MPAM.

4.7 Requisitos de Processamento e Armazenamento de Dados

a) A substituição da infraestrutura hiperconvergente atual por uma solução fornecida por outro fabricante, distinta daquela já adotada pelo MPAM (NUTANIX), acarretaria impactos significativos à operação e à continuidade dos serviços de tecnologia da informação do órgão, além da necessidade de reconfiguração completa da arquitetura existente, gerando um elevado retrabalho técnico e administrativo.

b) A adoção de uma outra plataforma demandaria do corpo técnico do MPAM o aprendizado de novas ferramentas, metodologias de gerenciamento e procedimentos operacionais, o que implicaria em uma nova curva de aprendizado. Esse processo não apenas exigiria tempo e capacitação formal, mas também aumentaria a dependência de suporte externo no curto e médio prazo, prejudicando a autonomia operacional da equipe interna.

c) Manter a continuidade tecnológica com a solução já homologada e em operação representa uma medida de racionalidade administrativa, técnica e orçamentária, mitigando riscos, preservando o conhecimento técnico já consolidado e assegurando a estabilidade e o desempenho do ambiente de produção do MPAM

d) A solução para reposição da capacidade de processamento e armazenamento deve manter plena compatibilidade e integração total com a infraestrutura atualmente em operação - infraestrutura baseada em solução de hiperconvergência NUTANIX.

e) A contratação da capacidade de processamento e armazenamento deverá suprir e substituir a capacidade de processamento e armazenamento já comprometida desde de novembro de 2024, em virtude do fim de vida dos

equipamentos envolvidos e fim dos contratos de manutenção e garantia relacionados.

4.8 Requisitos de Entrega

a) A contratação deverá contar com suporte de configuração, migração, integração com a infraestrutura pré-existente no MPAM, assistência técnica, manutenções preventivas e manutenções corretivas, para fornecer o máximo de suporte a equipe técnica do MPAM.

b) A solução deverá ser implementada, disponibilizada e integrada ao contexto tecnológico pré-existente no MPAM sem que para isso haja interrupção superior a 48hs das atividades operacionais do MPAM.

c) Em decorrência da precariedade do espaço atual em uso e da urgência resultante do fim eminente do ciclo de vida dos equipamentos atuais, a solução de infraestrutura física para armazenamento e operação das unidades computacionais deverá ser disponibilizada, implementada, migrada e integrada ao contexto tecnológico pré-existente no MPAM em prazo máximo de 90 (noventa) dias a partir da assinatura de contrato.

d) A solução deverá contemplar toda e qualquer adequação física, elétrica ou lógica, bem como qualquer obra civil, equipamento, cabos e conectores necessários à sua implantação, disponibilização, migração e integração ao contexto tecnológico do MPAM.

4.9 Requisitos Gerais

a) Recomenda-se que os licitantes realizem a vistoria prévia ao processo licitatório, a fim de conhecer o atual datacenter do MPAM e obter informações detalhadas sobre a infraestrutura existente. Tal vistoria permite que os licitantes tenham uma visão mais precisa das necessidades e requisitos específicos da organização, facilitando a elaboração de propostas alinhadas com as demandas reais.

b) A vistoria prévia também proporciona aos licitantes a chance de esclarecer dúvidas, obter informações adicionais e interagir diretamente com os responsáveis pela área de tecnologia do MPAM. Essa troca de informações contribui para um melhor entendimento das expectativas do MPAM e permite que os licitantes ofereçam propostas alinhadas com as necessidades reais.

5. ANÁLISE DE MERCADO

5.1 INFRAESTRUTURA FÍSICA PARA ARMAZENAMENTO DAS UNIDADES COMPUTACIONAIS - DATACENTER

A análise de mercado para provimento de uma solução para a infraestrutura física para armazenamento das unidades computacionais – Datacenter, considerou as seguintes soluções:

a) Alocação de espaço em datacenter externo pré-existente de empresa especializada na prestação deste tipo de serviço e com sistemas essenciais já incluídos no contrato de alocação de espaço.

b) Utilização do atual espaço fisico já ocupado pelo datacenter no MPAM.

5.1.1 Alocação de Espaço em Datacenter Externo Pré-existente

A alocação de espaço físico em datacenter externo pré-existente de empresa especializada na prestação deste tipo de serviço mostrou-se viável considerando os seguintes critérios técnicos operacionais:

a) Prazos de disponibilização menor do que a construção convencional de novo datacenter ou aquisição de datacenter pré-fabricado;

b) Menor complexidade de especificação de projeto;

c) Redução da sobrecarga de atividades da limitada equipe técnica do MPAM, uma vez que as responsabilidades relacionadas ao espaço físico e aos sistemas essenciais necessários à manutenção do datacenter estariam no escopo do contrato de locação de espaço;

d) Otimização de espaço físico uma vez que este seria alocado externamente ao MPAM.

5.1.2 Utilização do Atual Espaço Físico já Usado pelo Datacenter

A utilização do espaço físico do datacenter já utilizado pelo MPAM mostrou-se viável considerando os seguintes critérios:

a) Prazos de disponibilização imediata do espaço, apesar das limitações de infraestrutura fisica já citadas no item "NECESSIDADE DA CONTRATAÇÃO";

b) Menor complexidade de especificação de projeto;

c) Menores prazos de entrega e implantação em relação as demais opções, em torno de 90 dias.

5.2 UNIDADES DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS – SERVIDORES NUTANIX

5.2.1 Aquisição de Servidores (nós) Nutanix de Acordo com os Requisitos Apresentados

A aquisição de equipamentos de processamento e armazenamento de dados segue o modelo adotado até aqui pelo MPAM, mostrando-se viável diante dos requisitos apresentados e com as seguintes implicações:

a) Desembolso imediato de maior volume financeiro, uma vez que a aquisição de equipamentos implica no pagamento dos valores no início do contrato – ainda que este preveja manutenção e garantias por alguns anos. Não há taxas de financiamento, uma vez que os valores são pagos de forma imediata.

b) A aquisição deve considerar, caso não use o atual espaço fisico do datacenter na PGJ, a execução de contrato adicional para o fornecimento de solução de Infraestrutura física para alocação das unidades computacionais.

5.2.2 Locação de Servidores NUTANIX de Acordo com os Requisitos Apresentados

A locação de equipamentos de processamento e armazenamento de dados mostrou-se solução viável para a reposição da capacidade de processamento e armazenamento de dados, apresentado as seguintes implicações:

a) Desembolso financeiro realizado de forma gradual ao longo do contrato, uma vez que que não há aquisição de equipamentos e sim contratação de um serviço com faturamento mensal, com as taxas de financiamento já embutidas nos valores, variando conforme o prazo do contrato.

b) A alocação deve considerar a contratação conjunta de solução de infraestrutura para armazenamento dos equipamentos – Datacenter remoto ou a instalação dos equipamentos em Datacenter próprio.

5.3 SOLUÇÕES COMBINADAS

Em virtude da necessidade de uma solução completa e combinada de (1) recursos computacionais de processamento e armazenamento de dados e de (2) local para instalação e operação desses recursos – Datacenter, as seguintes configurações foram consideradas:

a) Locação de nós Nutanix com uso em datacenter externo pré-existente de empresa especializada.

b) Locação de nós Nutanix com uso em datacenter próprio já existente.

c) Aquisição de nós Nutanix e instalação em datacenter próprio já existente.

5.3.1 Locação de Servidores NUTANIX em Datacenter Pré-existente de Empresa Especializada

Esta opção de solução pressupõe contratos único para locação das unidades de processamento e armazenamento, bem como alocação de espaço físico em datacenter pré-existente de empresa especializada.

As estimativas de recursos necessários para implantação estão baseadas em proposta comercial da Empresa de Processamento de Dados Amazonas S/A - PRODAM conforme abaixo:

Item	Descrição	Qtde	Valor Mensal	Valor Anual (12 meses)	Val (60
1	SERVIDORES HIPERCONVERGENTES – NUTANIX G9 + SOFTWARE DE HIPERCONVERGENCIA + NUS	3	R$ 119.701,53	R$ 1.436.418,36	R$ 7.
2	LICENÇAS WINDOWS SERVER DATACENTER - 6 SOCKETS	6	R$ 27.943,32	R$ 335.319,84	R$ 1.
3	BACKUP (ARMAZENAMENTO + SOFTWARE) - 40TB	40	R$ 70.961,60	R$ 848.299,20	R$ 4.
4	INSTALAÇÃO E MIGRAÇÃO (10 PACELAS)	10	R$ 86.555,55	R$ 865.555,50	R$ 8
5	GERENCIAMENTO E OPERAÇÃO	1	R$ 6.185,08	R$ 74.220,96	R$ 3
6	CIRCUITO DE TRANSMISSÃO DE DADOS 10Gbps - DUPLA ABORDAGEM	1	R$ 26.685,96	R$ 320.231,52	R$ 1.
VALOR GLOBAL DA SOLUÇÃO				R$ 3.880.045,38	**R$ 15.**

Considerações:

a) Prazo informado pela PRODAM para a instalação e finalização da migração do Plataforma Nutanix do MPAM é de 180 dias.

b) O link de dados entre o MPAM e a PRODAM será licitado, podendo gerar atraso no prazo informado no item anterior.

c) Valores para contrato com prazo de 60 meses.

d) Poderá haver renovação anual dos valores de locação.

e) Proposta encontra-se no ANEXO 1 (1663745).

5.3.2 Locação de Servidores NUTANIX e Instalação em Datacenter Próprio já Existente

Esta opção de solução pressupõe contrato único para locação das unidades de processamento e armazenamento, bem como o uso do espaço físico em datacenter próprio, já existente no MPAM.

As estimativas de recursos necessários para implantação estão baseadas em proposta comerciais de fornecedores e são as seguintes:

Item	Descrição	Qtde	Valor Mensal	Valor Anual (12 meses)	V (6
1	EQUIPAMENTO HIPERCONVERGENTE – NUTANIX G9 + SOFTWARE DE HIPERCONVERGENCIA + NUS + SOFTWARE DE BACKUP	4	R$ 120.750,00	R$ 1.449.000,00	R$ 7
2	EQUIPAMENTO HIPERCONVERGENTE – NUTANIX G9 COM GPU + SOFTWARE DE HIPERCONVERGENCIA + SOFTWARE DE BACKUP	1	R$ 50.122,75	R$ 601.473,00	R$ 3
3	EQUIPAMENTO PARA ARMAZENAMENTO DE DADOS DE BACKUP + SOFTWARE DO REPOSITÓRIO/GERENCIAMENTO	1	R$ 30.955,13	R$ 371.461,56	R$ 1
VALOR GLOBAL DA SOLUÇÃO				R$ 2.421.934,56	**12.**

Considerações:

a) Os serviços de instalação e migração dos equipamentos já estão incluidos nos valores dos itens.

b) Prazo informado pela empresa para a instalação e migração do Plataforma Nutanix do MPAM é de 90 dias.

c) Devido a compatibilidade dos sockets/processadores da solução será utilizado o sistema operacional Windows Server DataCenter de propriedade do MPAM.

d) O Switch Core a ser utilizado na solução será o mesmo em uso atualmente no Datacenter do MPAM.

e) Valores para contrato com prazo de 60 meses.

f) Poderá haver renovação anual dos valores de locação.

g) Proposta encontra-se no ANEXO 2 (1663748).

5.3.3 Aquisição de Nós NUTANIX e Instalação em Datacenter Próprio já Existente

Esta opção de solução pressupõe contrato único para locação das unidades de processamento e armazenamento, bem como alocação de espaço físico em datacenter próprio, já existente no MPAM.

As estimativas de recursos necessários para implantação baseado em ata de registro de preço são os seguintes:

Item	Descrição	Qtde	Valor Unit	Va
1	EQUIPAMENTO HIPERCONVERGENTE – NUTANIX G9 + SOFTWARE DE HIPERCONVERGENCIA	4	R$ 1.065.000,00	R$ 4
2	EQUIPAMENTO HIPERCONVERGENTE – NUTANIX G9 COM GPU + SOFTWARE DE HIPERCONVERGENCIA + SOFTWARE GPU + NUS	1	R$ 1.680.036,80	R$ 1
3	SWITCH CORE	2	R$ 334.500,00	R$
4	SOFTWARE DE BACKUP DE DADOS	1	R$ 645.040,00	R$
5	EQUIPAMENTO PARA ARMAZENAMENTO DE DADOS DE BACKUP + SOFTWARE DO REPOSITÓRIO/GERENCIAMENTO	1	R$ 1.052.556,00	R$ 1
VALOR GLOBAL DA SOLUÇÃO				**R$ 8**

Considerações:

a) Os serviços de instalação e migração dos equipamentos já estão incluidos nos valores dos itens.

b) Prazo informado pela empresa para a instalação e migração do Plataforma Nutanix do MPAM é de até 90 dias.

c) Devido a compatibilidade dos sockets/processadores da solução será utilizado o sistema operacional Windows Server DataCenter de propriedade do MPAM.

d) Valor poderá ser dividido em até 2 parcelas (a primeira no recebimento dos serviços e equipamentos e a segunda 90 dias após).

e) 60 meses de licenciamento, garantia e assistência técnica.

f) Proposta encontra-se no ANEXO 3 (1663750)

6. DESCRIÇÃO DA SOLUÇÃO ESCOLHIDA

Considerando as necessidades de contratações indicadas no item 2. NECESSIDADE DA CONTRATAÇÃO, os requisitos para a solução apresentados no item 4. REQUISITOS DA CONTRATAÇÃO, as soluções disponíveis no mercado com suas devidas estimativas de custo, prazos e riscos apresentados no item 5. ANÁLISE DE MERCADO, e a realidade orçamentária do MPAM, a **Aquisição de Nós NUTANIX e Instalação em Datacenter Próprio já Existente** mostra-se a solução mais viável segundo os parâmetros técnico, tempo/urgência e orçamentários.

A solução apresenta menor risco de implantação, podendo ser efetivada com a urgência que a demanda exige. Os prazos para efetivação são os menores em relação às demais alternativas.

A solução também apresenta menor complexidade técnica e de contratação, menor impacto operacional e melhores condições de viabilização financeira.

A solução deverá ser oferecida como aquisição, com pagamento único (ou negociado em até 2 parelas) e garantia contratual e assistência técnica de 60 meses, englobando as unidades de processamento e armazenamento de dados, softwares, instalação e migração do ambiente antigo para o novo.

A contratação deverá envolver:

a) Solução para repor a capacidade computacional, comprometida desde novembro de 2024 - os recursos computacionais ainda estarão disponíveis, mas já não estão mais cobertos por qualquer tipo de contrato de garantia e manutenção;

b) Aquisição de Servidores Nutanix de, no mínimo 9ª Geração (equipamento hiperconvergente), com fornecimento de sofwares e licencimentos associados, compatíveis com a infraestrutura já existente no MPAM e com as especificações mínimas apresentadas nesse documento e Termo de Referência;

c) Instalação dos equipamentos em espaço físico já existente no MPAM, ativação, migração dos dados para o novo ambiente, integrações necessárias para permitir acesso a partir da rede do MPAM;

d) Garantia e suporte técnico dos equipamentos e serviços por 60 meses.

A seguir apresenta-se a estimativa de aquisição de equipamentos e softwares para uma infraestrutura de nuvem privada:

ITEM	DESCRIÇÃO	QUANTIDADE

1	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9	4
2	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU	1
3	SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX	5
4	SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU	2
5	LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE	30
6	SOFTWARE DE BACKUP DE DADOS	1
7	EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	1
8	SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	1
9	SWITCH CORE	2

6.1 ITEM 01 - EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9

6.1.1 Características Gerais

a) Solução hiperconvergente com integração total entre hardware e software Nutanix.

b) Apenas appliances homologados pela Nutanix (AOS e AHV) serão aceitos.

c) Permite entrega de recursos adicionais, desde que integrados e certificados pela Nutanix.

d) Suporte a múltiplos nós por chassi.

e) Gerenciamento via Nutanix Prism (última versão ou equivalente), com funções de atualização (BIOS, firmware, hipervisor e SDS), visualização do hardware físico, diagnóstico, inventário e expansão de nós.

f) Alta disponibilidade, recuperação de desastres e expansão modular, e não disruptiva, com detecção automática de novos nós.

g) Armazenamento centralizado em discos compartilhados, redundantes.

h) Preparada para ambientes virtualizados com alta disponibilidade.

6.1.2 Configuração do Nó ou Chassi

a) Chassis com múltiplos nós permitidos.

b) Fontes e ventiladores redundantes com cabos de energia inclusos.

6.1.3 Características de Processamento por Nó

a) Mínimo de 2 processadores x86 com 10 núcleos e 20 threads cada, 2,4 GHz, DDR4 ou superior.

b) Processadores mais recentes aceitos com mesmas especificações mínimas.

6.1.4 Especificações de Memória por Nó

a) Mínimo de 3,84 GB RAM DDR4 ou superior, distribuída uniformemente entre os processadores.

6.1.5 Especificações de Rede por Nó

b) 2 interfaces 25/10 GbE SFP28 e 1 interface de gerenciamento 1000Base-T.

6.1.6 Especificações de Armazenamento por Nó

a) 4 SSDs (NVMe/SAS/SATA) de 3,84 TB e 8 HDDs de 8 TB.

6.1.7 Serviço de Implementação e Configuração

a) Instalação completa pela contratada ou fabricante.

b) Técnicos certificados obrigatórios (exceto se instalação for pelo fabricante).

c) Entrega de cronograma de implantação e proposta de configuração da solução, além de manuais e documentação digital.

d) Instalação inclui fixação, energização, atualização de firmware, conexão de rede, registro dos equipamentos no portal do fabricante e configuração.

6.1.8 Serviços de Suporte Técnico e Manutenção

a) Garantia de 60 meses, com suporte 24x7.

b) Acesso completo ao portal do fabricante.

c) Atualizações de software e firmware sem ônus à contratante durante o período de suporte.

d) Garantia de compatibilidade técnica durante o contrato.

6.2 ITEM 02 - EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU

6.2.1 Características Gerais

a) Solução hiperconvergente com integração total entre hardware e software Nutanix.

b) Apenas appliances homologados pela Nutanix (AOS e AHV) serão aceitos.

c) Permite entrega de recursos adicionais, desde que integrados e certificados pela Nutanix.

d) Suporte a múltiplos nós por chassi.

e) Gerenciamento via Nutanix Prism (última versão ou equivalente), com funções de atualização (BIOS, firmware, hipervisor e SDS), visualização do hardware físico, diagnóstico, inventário e expansão de nós.

f) Alta disponibilidade, recuperação de desastres e expansão modular, e não disruptiva, com detecção automática de novos nós.

g) Armazenamento centralizado em discos compartilhados, redundantes.

h) Preparada para ambientes virtualizados com alta disponibilidade.

6.2.2 Configuração do Nó ou Chassi

a) Chassis com múltiplos nós permitidos.

b) Fontes e ventiladores redundantes com cabos de energia.

6.2.3 Características de Processamento por Nó

a) Mínimo de 2 processadores x86 com 10 núcleos e 20 threads cada, 2,4 GHz, DDR4 ou superior.

b) Processadores mais recentes aceitos com mesmas especificações mínimas.

6.2.4 Especificações de Memória por Nó

a) Mínimo de 512 GB RAM DDR4 ou superior, distribuída entre os processadores.

6.2.5 Especificações de Rede por Nó

a) 2 interfaces 25/10 GbE SFP28 e 1 interface de gerenciamento 1000Base-T.

6.2.6 Especificações de Armazenamento por Nó

a) 4 SSDs (NVMe/SAS/SATA) de 3,84 TB e 8 HDDs de 8 TB.

6.2.7 Especificações de Processamento Gráfico

a) 1 GPU com 48 GB GDDR6, PCIe Gen4 (64 GB/s), suporte a DirectX, OpenGL, Vulkan, NVIDIA vPC/vApps/RTX/Virtual Compute Server, consumo máx. 300W.

6.2.8 Serviço de Implementação e Configuração

a) Instalação completa pela contratada ou fabricante.

b) Técnicos certificados obrigatórios (exceto se instalação for pelo fabricante).

c) Entrega de cronograma de implantação e proposta de configuração da solução, além de manuais e documentação digital.

d) Instalação inclui fixação, energização, atualização de firmware, conexão de rede, registro dos equipamentos no portal do fabricante e configuração.

6.2.9 Serviços de Suporte Técnico e Manutenção

a) Garantia de 60 meses, com suporte 24x7.

b) Acesso completo ao portal do fabricante.

c) Atualizações de software e firmware sem ônus à contratante durante o período de suporte.

d) Garantia de compatibilidade técnica durante o contrato.

6.3 ITEM 03 - SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX

6.3.1 – Camada de Armazenamento

a) Armazenamento compartilhado entre todos os servidores/appliances, baseado em Software Defined Storage (SDS).

b) Arquitetura otimizada para ambientes virtuais, com escalabilidade elástica e sem necessidade de licenças adicionais de virtualização.

c) Tecnologia RAID não será aceita para redundância de dados.

d) Exige-se uso de técnicas modernas como Erasure Coding para otimização de aplicações com baixa sensibilidade à latência de escrita.

e) Suporte a compressão e desduplicação de dados (inline, near-line ou pós-processada).

f) Recursos de QoS (Quality of Service) para controle de I/O por VM.

g) Expansão de armazenamento com nós dedicados, sem exigir licenças de virtualização.

h) Alta disponibilidade: falhas de disco ou de nó não devem impactar operações.

i) Criptografia em nível de cluster ou volume, com KMS nativo.

j) Distribuição automática e uniforme dos dados no cluster.

k) Suporte a snapshots e clonagem de VMs sem movimentação de dados.

l) Acesso externo ao armazenamento via iSCSI, inclusive para aplicações de alta disponibilidade.

6.3.2 – Replicação e Proteção de Dados

a) Replicação local com suporte a snapshots e clones para proteção contínua.

b) Suporte a Thin Provisioning e múltiplas formas de replicação (síncrona e assíncrona).

c) Múltiplos RPOs configuráveis (1min, 5min, 15min, 1h).

d) Replicação no nível de VM, com suporte a grupos de proteção:

i) Proteção simultânea de VMs com cópias point-in-time.

ii) Proteção consistente de aplicações em Linux e Windows, incluindo dados em memória.

e) Suporte a entidade concentradora de tráfego replicado, replicação bidirecional e múltiplos destinos.

f) Controle de banda e frequência de replicação por grupo de VMs.

g) Mecanismos de controle de split-brain em falhas de comunicação.

h) Orquestração de Disaster Recovery (DR) com Fluxos de trabalho, sequência de boot, scripts de failover e testes automatizados.

6.3.3 – Gerenciamento Integrado

a) Ferramenta de gerenciamento única para múltiplos clusters.

b) Monitoramento automático com alertas para fornecedor e contratante.

c) Dashboard completo com métricas de CPU, memória, armazenamento, IOPS, banda e latência.

d) Acesso ao portal do fabricante para atualizações.

e) Atualizações de firmware/software em pacotes com instalação assistida.

6.3.4 – Provisionamento de Containers

a) Plataforma de containers deverá ser entregue, integrada ou não à plataforma de virtualização.

b) Suporte a múltiplos clusters com seleção de SOs, rede, armazenamento e nós.

c) Fabricante deve ser membro da CNCF (Cloud Native Computing Foundation).

d) Suporte a RBAC, atualizações simultâneas, monitoramento com alertas.

e) Clusters HA para "Control Plane", com ou sem load balancer.

f) Integração com CSI (Container Storage Interface) e compatibilidade com S3 (Simple Storage Service).

g) Monitoramento com alertas em clusters Kubernetes.

6.3.5 – Segurança de Rede

a) Microssegmentação com políticas aplicadas por VM ou grupo de VMs.

b) Políticas independentes de VLAN, IP ou MAC.

c) Visualização de tráfego e fluxos entre VMs com descoberta automática.

d) Inspeção de tráfego leste-oeste, isolamento automático de VMs comprometidas.

e) Políticas por categoria de VMs, com atualização automática.

f) Integração com ferramentas de terceiros como IDS/IPS e load balancer.

6.3.6 – Licenciamento da Virtualização

a) Licenciamento completo na versão mais avançada da plataforma.

b) Suporte a VMs com múltiplas interfaces e arquiteturas (32/64 bits).

c) Compatibilidade com principais SOs (Windows Server, CentOS, Ubuntu, RHEL).

d) Alocação dinâmica de CPU/RAM, suporte a GPU virtual/passthrough.

e) Hypervisor em unidade flash dedicada.

f) Suporte a BIOS/UEFI, snapshots, exportação OVA.

g) Alta resiliência a falhas e armazenamento distribuído via console web.

6.3.7 – Implementação e Transferência de Conhecimento

a) CONTRATADA será responsável por instalar, configurar e registrar a solução, utilizando técnicos certificados.

b) Fabricante poderá realizar parte do serviço.

d) Entrega de manuais, licenças e documentação técnica.

e) Treinamento com:

i) 24h de carga horária;

ii) Até 8 participantes;

iii) Instrutor certificado ou do fabricante.

6.3.8 – Suporte Técnico e Manutenção

a) Garantia de 60 meses com suporte técnico completo e atualizações inclusas.

b) Acesso total ao site do fabricante, com direito a downloads e consulta à base de conhecimento.

c) Suporte remoto 24x7, via telefone e e-mail, com chamados ilimitados.

6.4 ITEM 04 - SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU

6.4.1 - Requisitos do Software

a) Licença perpétua para no mínimo 16 usuários simultâneos.

b) Suporte a Ray Tracing, inteligência artificial, renderização em tempo real e sombreamento avançado.

c) Capacidade de modelagem realista de objetos e ambientes.

d) Suporte a GPU pass-through e múltiplos monitores até 8K.

6.4.2 - Implementação e Configuração

a) Instalação completa pela contratada ou fabricante.

b) Equipe técnica certificada e qualificada.

c) Entrega de cronograma, proposta técnica e documentação digital.

d) Instalação deve seguir boas práticas, incluir atualizações e registro de licenças.

6.4.3 - Suporte Técnico e Manutenção

a) Suporte e atualizações por 60 meses.

b) Acesso ao portal do fabricante com base de conhecimento e downloads.

c) Suporte remoto ilimitado, 24/7, com atendimento inicial em português via 0800.

6.5 ITEM 05 - LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE

a) O item trata do fornecimento de licenças de software para armazenamento de dados não estruturados em ambientes hiperconvergentes Nutanix.

b) O software deve ser compatível e homologado com os equipamentos especificados no contrato.

c) O licenciamento pode ser por assinatura e deve cobrir toda a capacidade necessária, medida em terabytes binários.

d) A execução do software só será considerada válida se todas as licenças forem da mesma versão dentro do cluster.

e) O tipo de licença exigido é o “Nutanix Unified Storage”, com garantia e suporte técnico por 60 meses.

6.6 ITEM 06 - SOFTWARE DE BACKUP DE DADOS

6.6.1 Licenciamento e Compatibilidade

a) Deve proteger pelo menos 80 máquinas virtuais por subscrição.

b) Sem limites para uso de agentes, conectores, repositórios, etc.

c) Última versão obrigatória.

d) Console deve exibir licenças adquiridas e usadas.

6.6.2 Cópia e Restauração

a) Controle de banda durante backup.

b) Cópia de arquivos abertos com consistência.

c) Priorização e resumo de tarefas.

d) Multiplexação para gravação paralela.

e) Alertas por e-mail e traps SNMP.

f) Agendamento automático.

g) Retenção diferenciada para o mesmo dado.

6.6.3 Gerenciamento

a) Interface única para múltiplos sistemas (Windows, Linux, Acropolis, AD, SQL Server, PostgreSQL, Oracle).

b) Acesso via console gráfico ou navegador.

c) Balanceamento automático de carga entre servidores de backup.

d) Backup e recuperação rápida do catálogo.

6.6.4 Criptografia

a) Criptografia na origem (cliente).

b) Chaves de 128 ou 256 bits.

6.6.5 Desduplicação

a) Desduplicação para toda a capacidade licenciada.

b) Desduplicação na origem, no destino e em tarefas de cópia.

c) Suporte à compressão e restauração granular.

6.6.6 Alertas e Relatórios

a) Relatórios de rotinas de backup e recuperação (últimas 24h, 30 dias, 12 meses).

b) Resumo de status das rotinas.

c) Relatório de licenças adquiridas e usadas.

d) Alertas por e-mail sobre status das rotinas.

6.7 ITEM 07 - EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES

6.7.1 Características Gerais:

a) Sistema dedicado para backup em disco com criptografia, compressão, desduplicação e replicação.

b) Deve ser novo, da linha atual do fabricante, com hardware e software do mesmo fornecedor.

c) Não são aceitas soluções customizadas, OEM, usadas ou virtuais.

d) Compatível com racks de 19” e todos os acessórios necessários.

e) Suporte a arquiteturas Scale-Out (expansível, alta disponibilidade) ou Scale-Up (duas controladoras, continuidade em falhas).

6.7.2 Requisitos de Disponibilidade:

a) Tolerância a falhas (discos, fontes, ventiladores).

b) Proteção contra perda de dados (cache, RAID-6 ou equivalente, discos hot-spare).

c) Monitoramento remoto com detecção proativa de falhas.

6.7.3 Capacidade, Desempenho e Conectividade:

a) Mínimo de 70 TB úteis (sem compressão ou desduplicação).

b) Scale-Out: expansão com 10 unidades, 7 TB/hora mínimo, até 70 TB/hora com mais equipamentos.

c) Scale-Up: expansão até 700 TB, 70 TB/hora, interfaces de 25 Gbps e 1 Gbps, porta de gerenciamento, discos adicionais conforme necessário.

6.7.4 Serviço de Instalação e Configuração:

a) Responsabilidade da contratada, com profissionais certificados.

b) Pode ser feito pelo fabricante.

c) Inclui fixação, energização, atualização de firmware, conexão à rede, registro e entrega de manuais.

d) Cronograma e proposta de configuração devem ser aprovados pelo contratante.

6.7.5 Resumo – Suporte Técnico e Manutenção

a) Garantia de 60 meses, com suporte 24x7 e envio de peças até o próximo dia útil após abertura do chamado.

b) Atualizações de software e firmware devem ser fornecidas sem custo durante o período de suporte.

6.8 ITEM 08 - SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES

6.8.1 Licenciamento e Arquitetura

a) Licença perpétua, sem custos adicionais.

b) Compatível com arquiteturas Scale-Out e Scale-Up, mantendo desduplicação global dos dados.

6.8.2 Compatibilidade

a) Totalmente compatível com o software de backup (Item 06).

b) Suporte a protocolos CIFS, NFS, OST, SNMP e Syslog.

c) Permite backup direto de Oracle e SQL via CIFS/NFS, sem consumo de licenças adicionais.

6.8.3 Funcionalidades Operacionais

a) Backup e restore simultâneos.

b) Interface web de gerenciamento.

c) Desduplicação global e contínua.

d) Verificação e correção automática de integridade dos dados.

e) Replicação assíncrona via IP com suporte a várias topologias.

f) Integração com Active Directory.

g) Criptografia AES128-SHA ou superior.

h) Suporte a autenticação em dois fatores (2FA) e autorização dupla (Dual Auth).

i) Proteção contra ransomware com imutabilidade e air-gap.

j) Instalação, configuração e transferência de conhecimento inclusas.

6.8.4 Transferência de Conhecimento

a) Mínimo de 4 horas para até 8 participantes.

b) Instrutor certificado ou representante oficial do fabricante.

6.8.5 Suporte Técnico (por 60 meses)

a) Acesso contínuo a atualizações e suporte técnico ilimitado.

b) Atendimento 24x7 via telefone (0800) e e-mail.

c) Acesso completo ao portal do fabricante com documentação e downloads.

6.9 ITEM 09 - SWITCH CORE

6.9.1 Especificações Físicas

a) Mínimo de 48 portas SFP28 (1/10/25GbE) autoajustáveis.

b) Altura máxima: 1U, compatível com racks de 19".

c) Compatível com diversos tipos de transceivers e cabos DAC.

d) Inclui 10 cabos DAC 25GbE (mín. 3m) e 4 transceivers SFP+ 10GbE SR.

e) Pelo menos 6 portas QSFP28 (40/100GbE), com suporte a DAC e transceivers SR4/LR4.

f) Capacidade mínima: 4 Tbps de comutação, 1,5 Bpps de throughput, 32 MB de buffer, 900 ns de latência.

g) Suporte a 160.000 MACs, 64.000 entradas ARP, jumbo frames (mín. 9000 bytes).

h) Porta de gerenciamento RJ-45, fontes e ventiladores redundantes e hot-swappable.

6.9.2 Funcionalidades Gerais

a) LEDs por porta, console CLI, SSHv2, SNMPv3, Syslog, NTPv4/SNTP.

b) Criptografia FIPS 140-2, espelhamento de portas (local e remoto), Netflow/sFlow.

c) Suporte a autenticação RADIUS, TACACS+, IEEE 802.1x, controle de tráfego e QoS.

6.9.3 Virtualização de Switch

a) Suporte a MLAG/VLT/Multi-Chassis EtherChannel com redundância ativa/ativa.

b) Operação sem tempo de convergência em falhas.

c) Inclui todos os componentes e licenças necessários.

6.9.4 Funcionalidades de Camada 2

a) Suporte a até 4.000 VLANs, LAG (IEEE 802.3ad), STP (802.1d/s/w), LLDP/LLDP-MED.

b) Proteções de STP, bloqueio de BPDUs, suporte a DCB (PFC, ETS, DCBx).

6.9.5 Funcionalidades de Roteamento

a) Roteamento L3 entre VLANs, OSPFv3, BGPv4, VRF/VRF-Light, PBR, VRRPv3.

b) Suporte a IPv4/IPv6 simultaneamente, com capacidade mínima de 106.000 rotas IPv4 e 52.000 IPv6.

6.9.6 Instalação e Configuração

a) Responsabilidade da contratada, podendo ser feita pelo fabricante.

b) Técnicos certificados devem ser disponibilizados.

c) Proposta de configuração e documentação digital.

6.9.7 Serviços de Instalação

a) Montagem em rack, energização, atualização de firmware, integração à rede.

b) Registro no portal do fabricante e execução de atividades para pleno funcionamento.

6.9.8 Garantia do Switch

a) Garantia de 60 meses com suporte técnico 24x7.

b) Acesso completo ao portal do fabricante, incluindo documentação, base de conhecimento e atualizações.

c) Todas as atualizações de firmware e software incluídas sem custo adicional durante o período de suporte.

7. ESTIMATIVA DAS QUANTIDADES A SEREM CONTRATADAS

A aquisição de equipamentos da plataforma NUTANIX a ser instalada no proprio espaço fisico de datacenter do MPAM, foi escolhida como solução mais adequada em função das necessidades institucionais, sendo as estimativas das quantidades a serem contratadas conforme descrito no item "**DESCRIÇÃO DA SOLUÇÃO ESCOLHIDA**" para a composição da solução do novo cluster de equipamentos.

8. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

As estimativas de preços que contam do item **5. ANÁLISE DE MERCADO** foram realizadas com base em propostas comerciais específicas dos fornecedores, atas de registro de preço para itens similares e dados públicos de contratos similares realizados por outros órgãos da administração pública.

O valor estimado para a contratação da solução escolhida, conforme detalhamento e motivações desenvolvidas nos itens anteriores, é de **R$ 8.306.632,80**, a ser desembolsado em até duas parcelas sendo a primeira após o recebimento definitivo da solução e a segunda 90 dias após.

9. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

A união dos distintos itens em um único lote tem por objetivo a padronização da contratação, uma vez que todos os elementos destacados no objeto possuem a mesma natureza técnica. Tal fato resulta na otimização dos recursos humanos, dos recursos financeiros e no desenvolvimento das atividades relacionadas à gestão contratual, uma vez que a administração de um número diverso de fornecedores fomenta a ineficácia laboral na fiscalização do contrato.

Não obstante, em razão da complexidade da solução, a possibilidade do parcelamento torna o contrato técnica, econômica e administrativamente inviável ou, ainda, provocaria a perda da economia de escala vislumbrada. Neste sentido, corrobora-se o agrupamento dos itens técnicos em um lote único, uma vez que tal condição administrativa vislumbra-se como a opção mais vantajosa à administração pública. Tal condição mantém a qualidade do projeto, haja vista que o gerenciamento e a execução permanecem todo o tempo a cargo de um mesmo fornecedor.

Nesse diapasão, as vantagens seriam o maior nível de controle pela administração na execução técnica e na prestação de serviços previstos, a maior facilidade no cumprimento do cronograma preestabelecido, a concentração da responsabilidade pela execução a cargo de um fornecedor e a melhor garantia no acompanhamento dos resultados, para o objeto estabelecido neste Estudo Técnico Preliminar.

É importante entender que os equipamentos (servidores hiperconvergentes) estabelecem interdependência onde solução como um todo possui requisitos específicos de interconexão para o transporte e processamento dos dados. Nesse escopo, a interoperabilidade dos itens é essencial ao correto funcionamento das aplicações e serviços digitais sustentados por

este Ministério.

Esclarecido esse ponto, entende-se que o produto macro a ser contratado se refere ao fornecimento de serviço cujo escopo e cobertura atingem hardware, software e integração à infraestrutura atual do MPAM.

Portanto, consideramos os itens do lote único como sendo interdependentes e complementares na composição de uma solução de tecnologia, devendo, portanto, serem licitados em um único grupo e entregues por uma única empresa de forma a garantir uma única entrega; minimizando o risco de fornecimento apenas parcial da solução, ou ainda o risco de compartilhamento de responsabilidades entre diferentes fornecedores, o que comprometeria o seu correto funcionamento durante o período contratual.

Pelo exposto, não há restrição da competitividade ao contratar todos os itens de um mesmo fornecedor, já que é prática de mercado o fornecimento da solução como arquitetura integrada de processamento e infraestrutura, disponibilizada, configurada e gerida pelo mesmo fornecedor.

10. CONTRATAÇÕES CORRELATAS OU INTERDEPENDENTES

Não há contratações correlatas ou interdependentes na presente contratação.

11. ANÁLISE DE RISCOS

O gerenciamento de riscos permite ações contínuas de planejamento, organização e controle dos recursos relacionados aos riscos que possam comprometer o sucesso da contratação, da execução do objeto e da gestão contratual.

O Mapa de Gerenciamento de Riscos deve conter a identificação e a análise dos principais riscos, consistindo na compreensão da natureza e determinação do nível de risco, que corresponde à combinação do impacto e de suas probabilidades que possam comprometer a efetividade da contratação, bem como o alcance dos resultados pretendidos com a solução de TIC.

Para cada risco identificado, define-se: a probabilidade de ocorrência dos eventos, os possíveis danos e impacto caso o risco ocorra, possíveis ações preventivas e de contingência (respostas aos riscos), a identificação de responsáveis pelas ações, bem como o registro e o acompanhamento das ações de tratamento dos riscos.

Como exemplo, parâmetros escalares são utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão as ações relacionadas aos riscos durante as fases de contratação (planejamento, seleção de fornecedor e gestão do contrato).

Classificação	Valor
Baixo	5
Médio	10
Alto	15

A tabela a seguir apresenta a Matriz "Probabilidade x Impacto", instrumento de apoio para a definição dos critérios de classificação do nível de risco.

P	15	75	**150**	**225**
	10	50	100	**150**
	5	25	50	75
	x	5	10	15
-	-	**I**		

Probabilidade (P) x Impacto (I)

O produto da probabilidade pelo impacto de cada risco deve se enquadrar em uma região da matriz "probabilidade x impacto". Caso o risco enquadre-se na região numerica não destacada (sublinhada ou negrito), seu nível de risco é entendido como baixo, logo admite-se a aceitação ou adoção das medidas preventivas. Se estiver na região numerica sublinhada, entende-se como médio; e se estiver na região numerica em negrito, entende-se comonível de risco alto. Nos casos de riscos classificados como médio e alto, deve-se adotar obrigatoriamente as medidas preventivas previstas.

A tabela a seguir apresenta uma síntese dos riscos identificados e classificados neste documento.

ID	Risco	Relacionamento	P	I
1	Não aprovação dos artefatos do Planejamento da Contração	Planejamento da Contratação	5	15

2	Atraso no processo administrativo de contratação	Planejamento da Contratação	10	10
3	Ausência de recursos orçamentários ou financeiros	Planejamento da Contratação	10	15
4	Atraso ou suspensão no processo licitatório em face de impugnações	Seleção do Fornecedor	15	10
5	Baixa qualificação técnica dos profissionais da empresa para execução do contrato	Gestão Contratual e Solução Tecnológica	10	10
6	Vazamento de dados e informações pelos funcionários da contratada	Gestão Contratual	10	15
7	Solução não operante	Gestão Contratual	10	15
8	Solução insuficiente	Planejamento da Contratação	5	15

Riscos Identificados:

Risco 01	**Risco:**		Não aprovação dos artefatos do Planejamento da Contratação
	Probabilidade:		Baixa
	Impacto:		Alto
	Dano 1:		Principais sistemas de infraestrutura de TI estarão sem cobertura de garantia.
	Tratamento:		Produzir de modo eficaz.
	Id	**Ação Preventiva**	**Responsável**
	1	Alinhar estrategicamente com todas as áreas responsáveis e envolvidas para a elaboração coesa dos artefatos	DTIC
	2	Convocar reuniões de análise e verificação do material produzido, evitando possíveis erros.	DTIC
	Id	**Ação de Contingência**	**Responsável**
	1	Alocação de recursos humanos para agilizar e garantir a confecção correta dos artefatos associados a contratação	DTIC

Risco 02	**Risco:**		Atraso no processo administrativo de contratação.
	Probabilidade:		Média
	Impacto:		Médio
	Dano 1:		Possível interrupção nos serviços de TIC prestados aos usuários internos e externos.
	Tratamento:		Mitigar.
	Id	**Ação Preventiva**	**Responsável**
	1	Controle do cronograma da licitação por todas as áreas envolvidas	DTIC / SUBADM
	2	Entregar todos os pré-requisitos da contratação de forma organizada e dentro dos prazos	DTIC / SUBADM
	Id	**Ação de Contingência**	**Responsável**
	1	Alocação de recursos humanos para dar celeridade com eficiência no processo	DTIC / DG / SUBADM

	Risco:		Ausência de recursos orçamentários ou financeiros.
	Probabilidade:		Média
	Impacto:		Alto

Risco 03	**Dano 1:**		Possível interrupção nos serviços de TIC prestados aos nossos usuários internos e externos.
	Tratamento:		Produzir de modo eficaz.
	Id	**Ação Preventiva**	**Responsável**
	1	Diálogo prévio e gestão com as áreas responsáveis com vistas ao provimento dos recursos necessários a contratação	DTIC
	2	Reservar recursos financeiros essenciais a esta contratação	DOF / SUBADM
	Id	**Ação de Contingência**	**Responsável**
	1	Buscar recursos para viabilizar a contratação	DTIC / DOF / SUBADM

Risco 04	**Risco:**		Atraso ou suspensão no processo licitatório em face de impugnações.
	Probabilidade:		Alta
	Impacto:		Médio
	Dano 1:		Atraso na contratação e consequente indisponibilidade de sistemas por falta de manutenção em funcionalidades, acarretando a insatisfação e prejuízos aos usuários dos sistemas.
	Tratamento:		Mitigar.
	Id	**Ação Preventiva**	**Responsável**
	1	Elaboração do planejamento da contratação consultando soluções similares em outros órgãos.	DTIC / SCOMS
	2	Definição dos critérios de seleção de fornecedores com respaldo na jurisprudência dos órgãos de controle.	DTIC / DCCON / CPL
	3	Verificação do teor de impugnações e recursos em contrações similares.	DTIC / CPL
	4	Estrita observância às recomendações da área jurídica do órgão/entidade.	DTIC / CPL
	Id	**Ação de Contingência**	**Responsável**
	1	Alocação integral da Equipe de Planejamento da Contratação na resposta e mitigação das causas que originaram a suspensão do processo licitatório.	DTIC / CPL / SUBADM
	2	Mitigação e eliminação das causas que obstruem o processo licitatório.	DTIC / CPL

Risco 05	**Risco:**		Baixa qualificação técnica dos profissionais da empresa para execução do contrato
	Probabilidade:		Média
	Impacto:		Médio
	Dano 1:		Dificuldades no processo de implementação e de assistência técnica
	Tratamento:		Demandar nível técnico coeso ao edital
	Id	**Ação Preventiva**	**Responsável**
	1	Delimitar no escopo do projeto o nível técnico mínimo esperado da empresa a ser contratada	DTIC
	2	Acompanhar e fiscalizar constantemente o contrato no que tange a qualidade técnica dos profissionais	DTIC
	Id	**Ação de Contingência**	**Responsável**

	1	Aplicação das sanções previstas no Edital	DTIC / CPL

Risco 06	**Risco:**		Vazamento de dados e informações pelos funcionários da contratada.
	Probabilidade:		Média
	Impacto:		Alto
	Dano 1:		Distribuição de informações sensíveis do setor público
	Tratamento:		Mitigar.
	Id	**Ação Preventiva**	**Responsável**
	1	Explicitar no corpo do edital as sanções e medidas que serão tomadas diante de uma possível ação pela contratada	DTIC
	2	Definir camadas de segurança e políticas efetivas no edital para o controle apropriado da segurança	DTIC
	Id	**Ação de Contingência**	**Responsável**
	1	Aplicar sanções previstas no edital	DTIC / CPL

Risco 07	**Risco:**		Solução não operante
	Probabilidade:		Média
	Impacto:		Alto
	Dano 1:		Indisponibilidade completa das informações armazenadas pelo MPAM
	Tratamento:		Mitigar.
	Id	**Ação Preventiva**	**Responsável**
	1	Definir coerentemente níveis de serviços que devem ser executados pelo provedor da assistência técnica	DTIC
	2	Definir plano de contingência para serviços que são críticos para o MPAM	DTIC
	Id	**Ação de Contingência**	**Responsável**
	1	Levantar os serviços no ambiente de contingência	DTIC
	2	Acionar CONTRATADA para normalização imediata de possíveis problemas	DTIC

Risco 08	**Risco:**		Dimensionamento insuficiente devido a novas demandas
	Probabilidade:		Baixa
	Impacto:		Alto
	Dano 1:		Indisponibilidade ou impossibilidade de novas implementações no ambiente institucional
	Tratamento:		Buscar ARP para permitir o eventual crescimento
	Id	**Ação Preventiva**	**Responsável**
	1	Definir o quantitativo a ser contratado/adquirido, incluindo uma margem de segurança	DTIC
	Id	**Ação de Contingência**	**Responsável**
	1	Aditivo no contrato para aumentar o tamanho da estrutura	DTIC / SUBADM / DCCON

11. BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

a) Garantir a disponibilidade dos sistemas computacionais do MPAM.

b) Modernizar a infraestrutura de processamento, armazenamento de dados assegurando a confiabilidade e a continuidade operacional dos sistemas institucionais do MPAM.

c) Garantir assistência técnica e serviços de suporte contínuos à equipe técnica, viabilizando a manutenção

preventiva e corretiva dos sistemas.

d) Melhorar a capacidade de transporte de dados entre os ativos de rede, assegurando maior eficiência na comunicação e processamento das informações, com redução da latência e otimização da conectividade entre sistemas.

e) Desenvolver os mecanismos tecnológicos essenciais a seguridade digital do MPAM.

f) Contribuir com o alinhamento estratégico do Ministério Público do Estado do Amazonas.

12. PROVIDÊNCIAS PARA ADEQUAÇÃO DO AMBIENTE DO ÓRGÃO

Com exceção dos itens contemplados na solução descrita neste ETP, não existem mais adequações necessárias à implementação da solução a ser adquirida.

13. CRITÉRIOS E PRÁTICAS DE SUSTENTABILIDADE

13.1 A aquisição, do objeto, desta licitação, obedecerá aos critérios de sustentabilidade ambiental contidos no Art. 5º da Instrução Normativa nº 01, de 19 de janeiro de 2010, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão – SLTI/MPOG.

14. PREVISÃO DA CONTRATAÇÃO NO PLANO DE CONTRATAÇÕES ANUAL

Plano de Contratações Anual - 2025 do MPAM

Item 24 - Contratação de empresa para locação de solução de DataCenter pré-existente

Item 29 - Aquisição de software gerenciador de backups para o DATACENTER

15. DECLARÇÃO DE VIABILIDADE

A equipe técnica da contratação do MPAM declara como viável a contratação pretendida e de acordo com as especificidades estipuladas neste Estudo Técnico Preliminar.

CARLOS ALEXANDRE DOS SANTOS NOGUEIRA

Chefe do Setor de Infraestrutura e Telecomunicações

ANTOVILA FROTA BEZERRA JÚNIOR

Técnico em Computação

Documento assinado eletronicamente por **Carlos Alexandre dos Santos Nogueira**, **Chefe do Setor de Infraestrutura e Telecomunicação - SIET**, em 09/07/2025, às 10:42, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Antovila Frota Bezerra Junior**, **Requisitado**, em 09/07/2025, às 10:43, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1591885** e o código CRC **0E017FDD**.

DESPACHO Nº 1018.2025.01AJ-SUBADM.1991573.2025.007562

PROCESSO N.º: 2025.007562

ASSUNTO: Contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais do Ministério Público do Estado do Amazonas (MPAM).

INTERESSADO: Diretoria de Tecnologia de Informação e Comunicação (DTIC)

I. DO RELATÓRIO

Trata-se do **Ofício n.º 94.2025.DTIC (1666988)**, de lavra do Ilmo. **Sr. Eudo de Lima Assis Júnior**, **Diretor de Tecnologia de Informação e Comunicação (DTIC)**, por onde são encaminhados o **Estudo Técnico Preliminar (ETP) n.º 7.2025.DTIC (1591885)** e o **Termo de Referência n.º 9.2025.DTIC (1605182),** que tem por objeto a contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup para atender as necessidades institucionais do Ministério Público do Estado do Amazonas (MPAM), **com vigência de 60 (sessenta) meses**.

Na forma do **Despacho 1013 (1990622)**, determinei o seguinte:

I) **à Diretoria Geral** para que promova a **inclusão da demanda do Plano Anual de Contratações de 2026**, nos termos do art. 4º, §3º, do Ato nº 008/2024/PGJ;

II) À **Diretoria de Tecnologia da Informação e Comunicação (DTIC)** para adotar as providências necessárias à efetivação da contratação no início do **exercício de 2026,** via procedimento licitatório;

III) O arquivamento dos presentes autos, **com ressalva**, podendo ser desarquivados para instruir novo processo de contratação, com base nas diretrizes do Plano de

Todavia, em reavaliação diante das justificativas técnicas constantes no ETP e no Termo de Referência supracitados, **considero oportuno e conveniente que a instrução processual da contratação tenha prosseguimento ainda no exercício corrente**, com vistas à efetiva concretização da solução demandada, observando-se os ritos e exigências legais pertinentes.

É o relatório. Decido.

II. DOS FUNDAMENTOS

Inicialmente, cogitou-se a adesão à Ata de Registro de Preços n.º 19/2025/SEJUSP-DIVCL, cuja autorização constou no Despacho nº 657 (1686563). Entretanto, conforme Ofício nº 231/2025/DTIC (1989729), restou informado o iminente esgotamento do prazo de 90 (noventa) dias estabelecido pelo órgão gerenciador para a formalização da contratação, prazo esse que, embora passível de prorrogação excepcional, depende de justificativa específica e da anuência da fornecedora.

Embora tenha sido deliberado o processamento da aquisição no exercício de 2026, via licitação, as justificativas apresentadas pela equipe técnica nos artefatos de planejamento e os riscos envolvidos na contratação da presente solução indicam a necessidade de seu imediato impulsionamento.

Diante disso, no exercício da prerrogativa de governança prevista no art. 11, parágrafo único, da Lei nº 14.133/2021, esta Subprocuradoria-Geral para Assuntos Administrativos reconsidera a decisão proferida no **Despacho nº 1013 (1990622)**, com fundamento nos documentos já constantes dos autos (Estudo Técnico Preliminar e Termo de Referência), para determinar a trâmite imediato do processo licitatório.

Quanto aos requisitos dos artefatos de planejamento, mantêm-se os fundamentos já consignados no **Despacho nº 605 (1673215)**, o qual atestou a conformidade legal, a regularidade dos artefatos instrutórios, o alinhamento da contratação com o planejamento institucional, bem como sua conveniência e oportunidade.

III. DA CONCLUSÃO

Por todo o exposto, com fundamento no artigo 26, § 2º, da Lei Complementar nº 011, de 17 de dezembro de 1993, e no artigo 4º do Ato n.º 076/2013-PGJ, **DECIDO**, nesta oportunidade, manter a decisão de **não solicitar a prorrogação do prazo** para efetivação da adesão à Ata de Registro de Preços nº 19/2025/SEJUSP-DIVCL, objeto do presente processo, e

DETERMINO:

I. **À Diretoria-Geral**, para manter a demanda devidamente registrada no **Plano Anual de Contratações de 2025**, conforme art. 4º, §3º, do Ato nº 008/2024/PGJ;

II. **Ao Setor de Compras e Serviços**, que proceda à verificação da pesquisa de mercado já constante dos autos, promovendo, se necessário, sua atualização, com observância estrita aos critérios estabelecidos no art. 23 da Lei nº 14.133/2021, visando à adequada instrução da licitação do objeto em tela;

III. **À Diretoria de Orçamento e Finanças**, que promova a verificação e/ou adequação da disponibilidade orçamentária, visando assegurar a compatibilidade da despesa com o planejamento financeiro da Instituição;

IV. **À Divisão de Contratos e Convênios**, que elabore a minuta do Termo de Contrato, nos moldes do Termo de Referência e das demais peças técnicas;

V. À Comissão Permanente de Licitação, que promova a expedição do Edital do certame, observando as diretrizes estabelecidas no Estudo Técnico Preliminar, no Termo de Referência e nos demais documentos preparatórios;

VI. **À Assessoria Jurídica**, que proceda à manifestação jurídica prévia, nos termos do art. 53 da Lei nº 14.133/2021, após o cumprimento das etapas acima.

Após o cumprimento das providências, **retornem os autos a esta Subprocuradoria-Geral para continuidade do trâmite processual**.

Cumpra-se.

GABINETE DA SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, Manaus (AM), *data da assinatura eletrônica.*

ANDRÉ VIRGÍLIO BELOTA SEFFAIR

Subprocurador-Geral de Justiça para Assuntos Administrativos

Documento assinado eletronicamente por **André Virgílio Belota Seffair**, **Subprocurador(a)-Geral de Justiça para Assuntos Administrativos**, em 23/10/2025, às 09:33, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1991573** e o código CRC **2BC22594**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

OFÍCIO Nº 422.2025.CPL.2004913.2025.007562

Ao Senhor

EUDO LIMA DE ASSIS JUNIOR

Diretor de Tecnologia da Informação e Comunicação

Assunto: Despacho Nº 1018.2025.01AJ-SUBADM.1991573.2025.007562.

Senhor Diretor,

Ao cumprimentá-lo cordialmente, e considerando as ponderações apresentadas por essa Diretoria de Tecnologia da Informação e Comunicação - DITC quanto às especificações do objeto a ser licitado, conforme Despacho Nº 1018.2025.01AJ-SUBADM.1991573.2025.007562, vem esta Comissão Permanente de Licitação **restituir** os presentes autos p**ara avaliação da necessidade de atualização dos artefatos da contratação**.

Na oportunidade, renovam-se votos de estima, colocando-nos à disposição para quaisquer esclarecimentos que se fizerem necessários.

Sarah Madalena B. Côrtes de Melo

Presidente da Comissão Permanente de Licitação
Ato PGJ n.º 165/2025 - DOMPE, Ed. 3121, de 15.07.2025

Documento assinado eletronicamente por **Sarah Madalena Barbosa Santos Cortes**, **Presidente da Comissão Permanente de Licitação - CPL**, em 10/11/2025, às 18:16, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2004913** e o código CRC **7091661F**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

OFÍCIO Nº 298.2025.DTIC.2009577.2025.007562

A Sua Excelência o Senhor

Doutor **ANDRÉ VIRGÍLIO BELOTA SEFFAIR**

Subprocurador-Geral de Justiça para Assuntos Administrativos

Assunto: Apresentar o **TR revisado** para aquisição de solução de datacenter

Excelentíssimo Senhor Subprocurador-Geral de Justiça para Assuntos Administrativos,

Honrado em cumprimentar Vossa Excelência, oportunidade em que **submeto** à aprovação, o Termo de Referência Nº 28.2025.DTIC (2002143) **revisado**, que trata da contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais do Ministério Público do Estado do Amazonas (MPAM).

Para identificação das necessidades, foi realizado o Estudo Técnico Preliminar - ETP Nº 7.2025.DTIC (1591885), considerando a necessidade de dispor de uma nova solução de datacenter uma vez que a atual solução encontra-se em situação crítica, no limite do processamento e armazenamento de dados, com equipamentos que já ultrapassaram o período de suporte ativo pelos fabricantes (end of life), tornando-se obsoletos do ponto de vista técnico e funcional.

A contratação está alinhada ao planejamento Estratégico 2017-2027:

- Objetivo 3.02: Aprimorar a infraestrutura gestão e governança de tecnologia da informação;
- Iniciativa Estratégica: Elaborar e implementar projeto de modernização do Datacenter.

Ante o exposto, solicito vossa aprovação do sobredito termo de referência. Caso seja aprovado, os autos devem ser encaminhados ao **SETOR DE COMPRAS E SERVIÇOS**, para realização da pesquisa de mercado.

Respeitosamente,

EUDO DE LIMA ASSIS JUNIOR

Diretor de Tecnologia da Informação e Comunicação

Documento assinado eletronicamente por **Eudo de Lima Assis Júnior**, **Diretor de Tecnologia da Informação e Comunicação (DTIC)**, em 16/11/2025, às 22:31, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2009577** e o código CRC **59526CA1**.

2025.007562 v4

TERMO DE REFERÊNCIA Nº 28.2025.DTIC.2002143.2025.007562

1. OBJETO DA CONTRATAÇÃO

1.1 Contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais do Ministério Público do Estado do Amazonas (MPAM).

1.2 Justificativa para a Contratação

Em 2019, foi celebrado o Contrato Administrativo n. 006/2019 - MP/PGJ (SEI0299031), para o Sistema de Automação da Justiça para o Ministério Público - SAJ-MP. Paralelamente, foi adquirida uma solução de software e hardware para processamento e armazenamento de dados que suportasse as demandas requeridas pelo SAJ-MP e demais sistemas computacionais da instituição - Solução Nutanix de Hiperconvergência, através do Contrato Administrativo n. 010/2018 - MP/PGJ (SEI 0210232).

Em 2020, para aumentar a capacidade de processamento e armazenamento, foi adquirido mais um servidor que fora incorporado à solução de Nutanix de Hiperconvergência, através do Contrato Administrativo n. 020/2020 - MP/PGJ, SEI 0572982.

A infraestrutura de hardware e software adquirida foi instalada no espaço físico mencionado e desde então segue em operação.

Esta é a infraestrutura física e computacional sobre a qual se mantêm os sistemas computacionais do MPAM, atualmente em situação crítica, com equipamentos que já ultrapassaram o período de suporte ativo pelos fabricantes (end of life), tornando-se obsoletos do ponto de vista técnico e funcional. Essa condição, como já mencionado, implica riscos relevantes à operação institucional, tais como falhas operacionais, indisponibilidade de sistemas e impossibilidade de atualização tecnológica.

Além disso, as aplicações institucionais em uso pelo MPAM estão em constante evolução, exigindo maior desempenho, escalabilidade e disponibilidade de recursos computacionais. A atual infraestrutura hiperconvergente, embora eficaz em sua concepção, já não atende plenamente às demandas atuais e futuras, especialmente diante da necessidade de implantação de novos sistemas e da manutenção dos já existentes.

Diante desse cenário, especificamos a contratação de uma solução plataforma NUTANIX, com equipamentos em garantia técnica e alinhados às necessidades imediatas do órgão, de forma a promover a continuidade dos serviços e a proteção de dados institucionais.

2. FORMA DE CONTRATAÇÃO

2.1 Tipo de contratação

2.1.1 A contratação será realizada por meio de licitação.

2.2 Modalidade da licitação

2.2.1 A modalidade adotada será o Pregão, na forma eletrônica, nos termos da legislação vigente.

2.3 Justificativa para não adoção do Sistema de Registro de Preços

2.3.1 A presente contratação refere-se a serviços de natureza contínua, com necessidade de execução imediata, regular e ininterrupta, cujas quantidades e especificações estão previamente definidas no Termo de Referência. Tais características não se compatibilizam com o modelo de contratação por demanda variável previsto no Sistema de Registro de Preços.

2.3.2 A demanda é certa, contínua e previamente dimensionada, tratando-se de prestação direta e específica ao contratante. Diante disso, a forma de execução contratual exige vínculo estável e unitário durante todo o período de vigência, não sendo adequada a contratação por meio de adesões esporádicas ou fracionadas.

2.3.3 Ressalta-se, ainda, que o uso do SRP é facultativo, conforme previsto no art. 82 da Lei nº 14.133/2021, sendo recomendado apenas quando se verificar vantagem para a Administração, o que não se configura no caso em questão.

2.4 Critério de julgamento da proposta

2.4.1 Será adotado o critério de julgamento pelo menor preço.

2.5 Critério de adjudicação

2.5.1 A adjudicação será realizada pelo critério de menor preço **global**.

2.6 Consórcios

2.6.1 Fica vedada a participação de empresas em consórcio nesta licitação. A natureza dos serviços – homogêneos, integrados e de execução contínua – não apresenta volume financeiro de alta monta ou risco elevado que justifique a união de empresas. Além disso, a formação de consórcios poderia acarretar dificuldades na gestão e fiscalização contratual, bem como possível elevação de custos, contrariando os princípios da vantajosidade e da eficiência.

2.7 Previsão de subcontratação

2.7.1 É vedada a subcontratação dos serviços objeto desta contratação. Considerando a natureza sensível e estratégica das atividades, as quais exigem controle direto e permanente da contratada, a subcontratação representaria risco à continuidade, à segurança da informação e à qualidade dos serviços prestados. Tal vedação está amparada no art. 122, § 2º, da Lei nº 14.133/2021, sendo medida necessária para preservar a eficiência e a efetividade da execução contratual.

2.8 Aplicação de tratamento diferenciado para ME/EPP/MEI (microempresa e afins)

2.8.1 Será assegurado o tratamento diferenciado às Microempresas (ME), Empresas de Pequeno Porte (EPP) e Microempreendedores Individuais (MEI) conforme previsto na legislação vigente, mediante comprovação de enquadramento no momento da habilitação, nos termos e condições a estabelecidas no edital.

2.9 Aplicação de direito de preferência

2.9.1 Em caso de empate ficto entre propostas, será assegurado o exercício do direito de preferência às ME, EPP e MEI, conforme disposto nos arts. 44 e 45 da Lei Complementar nº 123/2006, e no art. 62, inciso III, da Lei nº 14.133/2021. Os prazos e procedimentos para o exercício do referido direito serão disciplinados no instrumento convocatório.

3. REQUISITOS DO FORNECEDOR

3.1 Da necessidade de vistoria técnica

3.3.1 As empresas LICITANTES DEVERÃO realizar, sob o acompanhamento de servidor especialmente designado, vistoria às unidades da Procuradoria-Geral de Justiça, em data e horário previamente acordados segundo a conveniência deste Órgão, com o objetivo de conhecer as instalações onde serão executados os serviços e sanar as dúvidas porventura existentes, a fim de subsidiar a elaboração das propostas a serem submetidas ao certame.

3.3.1.1 A vistoria deverá ser realizada por representante devidamente credenciado pela empresa LICITANTE, devidamente municiado de documento próprio de credenciamento;

3.3.1.2 A comprovação de realização da vistoria será efetuada por meio de apresentação d e Atestado de Realização de Vistoria Técnica , que será emitido pelo interessado, ssinado por servidor designado da DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - DTIC desta PGJ/AM, e apresentado oportunamente, à sua habilitação;

3.3.1.3 O Atestado de Realização de Vistoria Técnica será assinado por servidor do MPAM que acompanhar a vistoria, e deverá ser encaminhada juntamente com a proposta;

3.3.1.4 As visitas deverão ser previamente agendadas, com 24 (vinte e quatro) horas de antecedência, pelo telefone (92) 3655-0670/0660 – DTIC, no período das 8h às 14h e poderão ser realizadas em até 2 (dois) dias úteis anteriores à data estipulada para abertura da licitação.

3.3.2 Caso a LICITANTE renuncie à vistoria técnica, deverá entregar a Declaração de Dispensa de Vistoria, o qual deverá ser preenchido e assinado pelo interessado em participar da licitação, anexando, oportunamente, à sua habilitação.

3.3.3 Não serão aceitas alegações posteriores advindas de desconhecimento das condições prediais, das características do ambiente de prestação dos serviços ou erro orçamentário por parte da futura contratada, quando da execução dos serviços propostos.

3.2 Da capacidade técnica

3.2.1 A licitante deve apresentar, juntamente com os demais documentos de habilitação, atestado de capacidade técnica expedido(s) em seu nome e respectivo CNPJ, fornecido por pessoas jurídicas de direito público ou privado, que comprovem já ter fornecido solução de datacenter, contemplando infraestrutura integrada de hardware e software, serviço de implantação, configuração e transferência de conhecimento, similares ao objeto deste Termo.

3.2.2 A licitante deverá apresentar na qualificação técnica, documento que indique o pessoal técnico operacional, das instalações e do aparelhamento adequado e disponíveis para a realização do objeto da licitação, bem como a qualificação de cada membro da equipe técnica que se responsabilizará pelos trabalhos. (art. 67, III da Lei 14.133/21).

3.2.3 Os atestados apresentados poderão ser objeto de diligência a critério do CONTRATANTE, para

verificação da autenticidade do conteúdo. Caso seja encontrada divergência entre o especificado nos documentos e o apurado em eventual diligência, além da desclassificação no presente processo licitatório, fica sujeita a licitante às penalidades cabíveis.

3.3 Apresentação de amostras

3.3.1 A critério da autoridade competente, não será exigida a apresentação de amostras.

4. DA FORMALIZAÇÃO E PRAZO DE VIGÊNCIA DO CONTRATO

A CONTRATANTE formalizará um contrato administrativo observando as seguintes condições:

4.1 Do prazo

4.1.1 A CONTRATADA deverá em, **no máximo, 60 (sessenta) dias corridos**, contados a partir da assinatura do contrato, finalizar a entrega de todos os itens do objeto especificado, com funcionamento e funcionalidades da solução de Datacenter completamente operacionais, totalmente ativadas e disponíveis na estrutura da CONTRATADA, conforme descritas neste Termo.

4.2 Das condições de fornecimento

4.2.1 A CONTRATADA será responsável pelo transporte dos produtos, desde o local de sua fabricação/embalagem, conforme o caso, até o local de entrega, na sede da PROCURADORIA GERAL DE JUSTIÇA, a qual ocorrerá em dias úteis, no horário das 14h às 17h, no seguinte endereço:

Av. Coronel Teixeira, nº 7.995, Nova Esperança II

CEP. 69037-473, Manaus-AM

4.2.2 A entrega dos produtos deverá ser previamente agendada com o SETOR DE PATRIMÔNIO E MATERIAL – SPAT pelo telefone (92) 3655-0767.

4.2.3 Os produtos deverão ser entregues em perfeitas condições, conforme a quantidade e especificações pactuadas, observando o Edital, a Proposta da CONTRATADA e este Termo de Referência, devendo, também, ser acondicionado adequadamente, em seu invólucro original, que deverão ser entregues devidamente acompanhados da respectiva nota fiscal, na qual constarão os valores discriminados dos itens que integram o conjunto, assim como as indicações referentes a: marca, modelo, procedência e prazo de garantia ou validade.

4.2.4 Os produtos devem estar em plena fabricação, não sendo aceitos aqueles com avisos de end-of-sale, end-of-support ou end-of-life emitidos pelo fabricante.

4.3 Da vigência do contrato

4.3.1 O Contrato terá vigência de **60 (sessenta) meses**, contados da data de publicação do extrato no Diário Oficial do MPAM, sendo resguardados os direitos relacionados à garantia e a assistência técnica vinculados aos equipamentos e serviços adquiridos, conforme descrito neste Termo.

5. MODELO DE GESTÃO

5.1 O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133/21, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

5.2 Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

5.3 As comunicações entre a CONTRATANTE e a CONTRATADA devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

5.4 A CONTRATANTE poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

5.5 Após a assinatura do contrato ou instrumento equivalente, a CONTRATANTE poderá convocar o representante da CONTRATADA para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da CONTRATADA, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

5.6 Preposto

5.6.1 A CONTRATADA deverá manter preposto junto à PGJ-AM, aceito pela respectiva FISCALIZAÇÃO, durante o período de vigência do contrato, para representá-la administrativamente, sempre que for necessário, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado, o qual deverá ser indicado mediante declaração de que deverá constar o nome completo, nº do CPF e do documento de identidade, além dos dados relacionados à sua qualificação profissional.

5.6.2 A empresa orientará o seu PREPOSTO quanto à necessidade de acatar as orientações da Administração, inclusive quanto ao cumprimento das Normas Internas e de Segurança e Medicina do Trabalho.

5.6.3. A Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em quea Contratada designará outro para o exercício da atividade.

5.7 Fiscalização

5.7.1 A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos, conforme indicação em portaria específica publicada no Diario Oficial do MPAM.

5.7.2 Compete ao Gestor da Ata/Contrato, além de outras atribuições, nos termos da lei:

a) Acompanhar os prazos de execução e de vigência do contrato, conforme as rotinas e procedimentos estabelecidos pelo MPAM, e as cláusulas do contrato ou instrumento equivalente, comunicando à CONTRATADA e à unidade competente da Administração eventuais atrasos e encaminhando, em tempo hábil, expediente para a prorrogação do Contrato;

b) Coordenar e acompanhar a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração;

c) Acompanhar a manutenção das condições de habilitação da CONTRATADA, para fins de empenho de despesa e pagamento, e anotar os problemas que obstam o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais;

d) Comunicar à Autoridade Competente as ocorrências relacionadas à execução do contrato que ultrapassarem a sua competência;

e) Emitir TERMO DE RECEBIMENTO DEFINITIVO, juntamente com a FISCALIZAÇÃO, comprovando a avaliação do cumprimento das obrigações assumidas pelo CONTRATADO;

f) Receber e conferir as faturas/notas fiscais emitidas pela CONTRATADA, e encaminhar, devidamente certificadas/atestadas ao setor competente, observando, previamente, se a fatura apresentada pela CONTRATADA refere-se ao objeto que foi efetivamente CONTRATADO;

g) Encaminhar o processo à unidade competente para proceder à liquidação da despesa, alertando para a data limite para pagamento das notas fiscais/fatura;

h) Requisitar a prorrogação de contrato, se possível, junto à Autoridade Competente, que deve ser providenciada antes de seu término, reunindo as justificativas necessárias;

i) Elaborar a comunicação à área competente para abertura de nova licitação, antes de findo a prestação de serviços e com antecedência razoável;

j) Cuidar das alterações de interesse da CONTRATADA, que deverão ser por ela formalizadas e devidamente fundamentadas, principalmente em se tratando de pedido de reequilíbrio econômico-financeiro ou repactuação, sendo que, no caso de pedido de prorrogação de prazo, deverá ser comprovado o fato impeditivo da execução, o qual, por sua vez, deverá corresponder àqueles previstos na Lei n. 14.133/21 e alterações, se possível;

k) Esclarecer dúvidas e transmitir instruções ao CONTRATADO, comunicando alterações de prazos, cronogramas de execução e especificações do projeto, inclusive solicitando ao setor competente da Administração, quando necessário a emissão de parecer técnico;

l) Deflagrar e conduzir os procedimentos de fiscalização à CONTRATADA, com base nos termos contratuais, sempre que houver descumprimento de suas cláusulas por culpa da CONTRATADA, acionando as instâncias superiores e/ou os órgãos públicos competentes quando o fato exigir;

m) Verificar se a entrega de materiais ou a prestação do serviço está sendo executada em conformidade com o pactuado, no tocante a prazo, especificações, preço e quantidade;

n) Rejeitar equipamentos e serviços que estejam em desacordo com as especificações do objeto contratado;

o) Zelar pelo efetivo cumprimento das obrigações contratuais assumidas e pela qualidade dos produtos fornecidos e dos serviços prestados;

p) Notificar a CONTRATADA em qualquer ocorrência desconforme com as cláusulas contratuais, sempre por escrito, com prova de recebimento da notificação (procedimento formal, com prazo);

q) Verificar a regularidade fiscal, trabalhista e previdenciária da contratada para fins de pagamento; e

r) Orientar a CONTRATADA, por intermédio do preposto, sobre a correta execução do Contrato e, pelo mesmo meio, levar ao seu conhecimento as situações temerárias, recomendando medidas e estabelecendo prazo de resolução.

5.7.3 Compete ao Fiscal Técnico, além de outras atribuições, nos termos da lei:

a) Acompanhar e fiscalizar a execução do contrato nos aspectos técnicos da solução, conforme o

respectivo regramento técnico aplicável;

b) Zelar pelo efetivo cumprimento das obrigações contratuais assumidas e pela qualidade dos produtos fornecidos e dos serviços prestados, de modo a assegurar os melhores resultados para a Administração;

c) Ler atentamente o Termo de Contrato e anotar em registro próprio todas as ocorrências relacionadas à sua execução, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados;

d) Esclarecer dúvidas do preposto/representante da CONTRATADA que estiverem sob a sua alçada, encaminhando às áreas competentes os problemas que surgirem quando lhe faltar competência;

e) Notificar a CONTRATADA para a correção da execução do contrato, determinando prazo para a correção, quando identificada qualquer inexatidão ou irregularidade;

f) Informar ao Gestor do Contrato, em tempo hábil, irregularidades que possam demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso;

g) Comunicar ao Gestor do Contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual;

h) Avaliar a qualidade dos serviços realizados ou dos itens entregues e justificativas, de acordo com os critérios de aceitação definidos em contrato; e

i) Orientar a CONTRATADA, por intermédio do preposto, sobre a correta execução do contrato e, pelo mesmo meio, levar ao seu conhecimento as situações temerárias, recomendando medidas e estabelecendo prazo de resolução.

6. ENTREGA DO OBJETO

6.1 Do recebimento provisório e definitivo

6.1.1 O recebimento dos produtos será conduzido por uma COMISSÃO especialmente designada para essa finalidade. Essa comissão será composta por, no mínimo, três servidores ou empregados públicos, em conformidade com o disposto no Art. 117, §1º e Art. 140, inciso II da Lei n.º 14.133/21, conforme estabelecido neste subitem.

6.1.2 O RECEBIMENTO PROVISÓRIO será realizado pelo SETOR DE PATRIMÔNIO E MATERIAL - SPAT no ato da entrega da totalidade dos produtos empenhados, devidamente acompanhados da nota fiscal. Constitui-se de uma inspeção quantitativa, para posterior verificação de sua conformidade com as especificações do Termo de Referência, e Ata de Registro de Preços.

a) O RECEBIMENTO PROVISÓRIO não constitui aceitação dos mesmos.

6.1.3 O RECEBIMENTO DEFINITIVO será realizado por FISCAL TÉCNICO ou COMISSÃO especialmente designada, no prazo máximo de 30 (trinta) dias, a contar do recebimento provisório, para verificação da conformidade dos equipamentos com as condições, especificações e obrigações contratuais.

a) É condição para RECEBIMENTO DEFINITIVO o fornecimento do TERMO DE GARANTIA E ASSISTÊNCIA TÉCNICA, informando que os referidos produtos estão cobertos por garantia de fábrica, de acordo com as exigências constantes neste instrumento;

b) O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais;

c) Uma vez constatado o cumprimento das obrigações de fornecimento, o TERMO DE RECEBIMENTO DEFINITIVO será emitido, que consistirá na declaração formal de que os itens fornecidos atendem aos requisitos estabelecidos no contrato, comprovando o atendimento das exigências contratuais.

6.1.4 Para avaliação da adequação às exigências contratuais e qualidade, o FISCAL TÉCNICO ou COMISSÃO submeterá os equipamentos recebidos a testes de aceitação, para aferição da boa execução do objeto contratado, após o qual, emitirá um relatório completo dos testes efetuados, devidamente assinado. Os testes serão constituídos das seguintes fases:

a) Abertura das embalagens;

b) Comprovação de que o equipamento/solução atende às especificações mínimas exigidas ou superiores oferecidas;

c) Testes funcionais de configuração e desempenho dos mesmos.

6.1.5 Os itens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência, seus Anexos e na proposta, sem prejuízo da aplicação das penalidades, cabendo à CONTRATADA o dever de substituir os itens que não estejam de acordo com as especificações, observando-se o disposto no Art. 140, §1º da Lei n.º 14.133/21.

6.1.6 O RECEBIMENTO PROVISÓRIO ou DEFINITIVO do objeto não exclui a responsabilidade civil a ele relativa, nem a ético-profissional, pela perfeita execução do objeto deste Termo.

6.1.7 As não conformidades e desvios de qualidade observados serão descritos em relatório, e não serão

recebidos definitivamente, devendo a pendência ser completamente sanada pela CONTRATADA, em no máximo 15 (quinze) dias consecutivos, contados da notificação da CONTRATANTE.

6.1.8 Se, a qualquer tempo, vier a ser constatado que o material fornecido o foi em desacordo com as especificações e, em decorrência desse fato, observar-se qualquer tipo de dano ao equipamento onde está sendo utilizado, o reparo do equipamento ou, se for o caso, a sua substituição, será de inteira responsabilidade da CONTRATADA, nos termos da lei pertinente.

7. DAS OBRIGAÇÕES DO CONTRATANTE E DA CONTRATADA

7.1 Obrigações da CONTRATADA

7.1.1 A CONTRATADA deverá cumprir todas as obrigações constantes neste termo de referência, minuta de contrato e seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando:

7.1.2 Apresentar, no prazo de até 10 (dez) dias corridos, contados a partir da assinatura do Contrato ou do recebimento da Nota de Empenho e da Autorização de Fornecimento de Materiais/Serviços:

7.1.2.1 Indicação formal do preposto da CONTRATADA apto a representá-la junto à CONTRATANTE, que deverá responder pela fiel execução do contrato, designado para acompanhar sua execução e atuar como interlocutor principal junto à CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

a) A indicação do preposto deverá ser acompanhada de seus dados pessoais, (no mínimo o nome completo e CPF do funcionário da empresa) e dados de contrato, como e-mail, telefone, whatsapp e outros.

7.1.2.2 Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste Termo de Referência.

7.1.3 Efetuar a entrega do objeto contratado, dentro do prazo e de acordo com as especificações constantes deste Termo de Referência, observando as prescrições e as recomendações do fabricante, a legislação estadual ou municipal, se houver, bem como outras normas correlatas, ainda que não estejam explicitamente citadas neste documento e seus anexos.

7.1.4 Apresentar, no prazo de até 10 (dez) dias úteis, contados a partir da entrega do objeto, o correspondente TERMO DE GARANTIA E ASSISTÊNCIA TÉCNICA, para os equipamentos/softwares/licenças fornecidos incluindo seus números de série, com o prazo de garantia solicitado neste Termo de Referência.

7.1.5 Não transferir a outrem, no todo ou em parte, o objeto deste Termo, sem prévia e expressa anuência da CONTRATANTE, não sendo aceita a transferência de responsabilidade para outras entidades, sejam fabricantes, técnicos, subempreiteiros ou quaisquer outros.

7.1.6 Comunicar imediatamente à CONTRATANTE, formalmente, toda e qualquer anormalidade que dificulte ou impossibilite a execução do objeto deste Termo e prestar os esclarecimentos julgados necessários.

7.1.7 Aceitar todas as decisões, métodos de inspeção, verificação e controle, obrigando-se a fornecer todos os dados, elementos e explicações que a CONTRATANTE julgar necessário.

7.1.7.1 A ação de fiscalização não exonera a CONTRATADA de suas responsabilidades contratuais.

7.1.8 Manter contato e realizar o planejamento dos serviços com o CONTRATANTE de forma a executar quaisquer tarefas ou ajustes inerentes ao objeto contratado.

7.1.9 Acatar as observações feitas pela FISCALIZAÇÃO da CONTRATANTE quanto à execução dos serviços.

7.1.10 Atender prontamente quaisquer orientações e exigências da equipe de FISCALIZAÇÃO do contrato ou autoridade superior (art. 137, II, da Lei n.º 14.133/21, e prestar todo esclarecimento ou informação por eles solicitados, inerentes à execução do objeto contratual;

7.1.10.1 A CONTRATADA deverá responder por escrito, no prazo máximo de até 2 (dois) dias consecutivos, a quaisquer comunicações e/ou esclarecimentos requisitados pela CONTRATANTE, pertinentes à execução do contrato e que venham a ser solicitados pelo MPAM.

7.1.11 A CONTRATADA deverá responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com Código de Defesa do Consumidor, Lei nº 8.078/90, e às demais normas pertinentes.

7.1.12 Apresentar justificativa por escrito, devidamente comprovada, nos casos de ocorrência de fato superveniente, excepcional ou imprevisível, estranho à vontade das partes, e de impedimento de execução por fato ou ato de terceiro reconhecido pela CONTRATANTE em documento contemporâneo a sua ocorrência, quando não puder cumprir os prazos estipulados para a execução, total ou parcial, do objeto deste Termo.

7.1.12.1 Nos casos de eventual atraso na entrega do objeto, comunicar à CONTRATANTE antes de expirar tal prazo, quaisquer problemas que impossibilitem o cumprimento do prazo previsto, com a devida comprovação.

7.1.13 Substituir, reparar, corrigir, remover, refazer ou reconstituir, às suas expensas, no todo ou em parte, no prazo fixado pela FISCALIZAÇÃO, os itens que não atendam às especificações exigidas e foram rejeitados, os que se verifiquem imperfeições, vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.

7.1.14 Responsabilizar-se por falhas na execução dos serviços que venham a se tornar aparentes em data posterior à sua entrega, ainda que tenha havido aceitação do mesmo.

7.1.15 Responsabilizar-se pela garantia e assistência técnica *on-site* dos itens, caso o fabricante e/ou assistência técnica autorizada por este não puder fazê-lo ou se recusar.

7.1.16 Manter, durante toda a execução do contrato, todas as condições de habilitação e qualificação exigidas na respectiva licitação, em compatibilidade com as obrigações assumidas.

7.1.17 Responder pela idoneidade moral e técnica dos seus empregados, sendo única, integral e exclusivamente responsável, em qualquer caso, por todos os danos e prejuízos, de qualquer natureza, causados, direta ou indiretamente, à CONTRATANTE ou a terceiros, provenientes da execução dos serviços objeto deste termo de referência, quaisquer que tenham sido as medidas preventivas adotadas, respondendo por si e seus procuradores.

7.1.18 Responsabilizar-se por obter todas as franquias, licenças, aprovações e demais exigências de órgãos competentes, inclusive responsabilizando-se por todos os ônus decorrentes.

7.1.19 A inobservância das especificações constantes deste termo de referência implicará a não aceitação parcial ou total dos serviços, devendo a CONTRATADA refazer as partes recusadas sem direito a indenização.

7.2. Obrigações da CONTRATANTE

7.2.1 Acompanhar e fiscalizar, como lhe aprouver e no seu exclusivo interesse, na forma prevista na Lei n.º 14.133/21, exigindo o cumprimento de todas as obrigações assumidas, de acordo com o contrato e seus anexos.

7.2.2 Nomear GESTOR e FISCALIZAÇÃO técnica e administrativa, para acompanhar e fiscalizar, a execução dos contratos.

7.2.3 As ações de fiscalização não excluem nem reduzem a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios ou emprego de material inadequado ou de qualidade inferior.

7.2.4 Fornecer à CONTRATADA as informações necessárias à fiel execução do objeto deste termo de referência.

7.2.5 Permitir o acesso, acompanhar e fiscalizar a execução do contrato, verificando a conformidade da prestação dos serviços e regular a entrega dos itens, de forma a assegurar o perfeito cumprimento do contrato.

7.2.6 Anotar em registro próprio e notificar a CONTRATADA, por escrito, a ocorrência de eventuais imperfeições, defeitos de fabricação, e avarias nos itens, fixando prazo para a sua reposição.

7.2.7 Rejeitar, no todo ou em parte, serviço ou fornecimento executado em desacordo com o contrato.

7.2.8 Efetuar regularmente o pagamento da CONTRATADA, dentro dos critérios estabelecidos neste termo de referência e no contrato, quanto aos serviços devidamente realizados, por meio de Ordem Bancária, após o atesto das notas fiscais/faturas pelo comitê responsável.

8. DAS PENALIDADES

8.1 O descumprimento de quaisquer das obrigações relacionadas à prestação do serviço, salvo nos casos devidamente justificados e comprovados, a critério da CONTRATANTE, sujeitará a CONTRATADA às sanções previstas na Lei Federal n.º 14.133/2021, sem prejuízo das responsabilidades civil e criminal, garantindo-se o direito ampla defesa e ao contraditório, quais sejam:

I. Advertência: Será aplicada no caso de atraso no cumprimento dos prazos para apresentação de uma solução definitiva para um problema com solução provisória, ainda que mantidos os níveis de serviço acordados com tal solução provisória, bem como, nos casos de atraso no encaminhamento do diagnóstico da ocorrência e comprovação da correção após a solução definitiva do problema e nos casos de repetidos descumprimentos dos acordos de nível de serviço que gerem impacto ao funcionamento do MPAM.

II. Multa, nos seguintes termos:

Item	Penalidade	Sanção	Limite

Item	Penalidade	Sanção	Limite
1	Atraso injustificado na entrega do objeto contratado, ou pelo não cumprimento dos prazos estabelecidos no Edital	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor total da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
2	Atraso injustificado na regularização pertinente quando da recusa do objeto fornecido, na fase de **RECEBIMENTO**.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor total da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
3	Recusa em substituir o produto defeituoso, que vier a ser rejeitado, ou que na execução dos serviços de garantia e assistência técnica, apontem a necessidade de troca;	Multa de mora diária de **1% (um por cento)** sobre o valor da Nota de Empenho	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
4	Deixar de utilizar peças, componentes ou insumos originais ou certificados pelo fabricante, novos e de primeiro uso.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho. Por ocorrência	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
5	Atraso injustificado para efetiva recolocação do produto em seu pleno estado de funcionamento, conforme condições de GARANTIA E ASSISTÊNCIA TÉCNICA deste Termo.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
6	Deixar de fornecer equipamento backup nos casos em que não for possível recuperar os produtos dentro dos prazos de atendimento previstos.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.

Item	Penalidade	Sanção	Limite
7	Atraso injustificado para a substituição de determinado item (equipamento, serviço, software, licença), no atendimento de chamado de garantia e assistência técnica.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da CONTRATADA às sanções correlatas.
8	Atraso injustificado para a análise e correção dos itens (equipamento, serviço, software, licença), no atendimento de chamado de garantia e assistência técnica.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 10º (décimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 11.º (décimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
9	Atraso injustificado para o fornecimento do TERMO DE GARANTIA E ASSISTÊNCIA TÉCNICA.	Multa de mora diária de **0,3% (três décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 10º (décimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 11.º (décimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
10	Atraso injustificado na resposta aos pedidos de esclarecimentos de ordem técnica.	Multa de mora diária de **0,2% (dois décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 10º (décimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 11.º (décimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
11	Deixar de cumprir qualquer outra obrigação não prevista neste Termo de Referência	Multa de mora diária de **1% (um por cento)** sobre o valor da Nota de Empenho	Limitada a sua aplicação até **15% (quinze por cento)**.
12	Quando, sem justificativa aceita pela **CONTRATANTE**, o vencedor não providenciar o devido cadastramento junto ao Sistema de Administração Financeira e Contabilidade – Cadastramento de Credores da SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ-AM, na forma prevista no Edital.	Multa de 2**,5% (dois inteiros e cinco décimos por cento)** sobre o valor total da proposta.	Não se aplica.
13	Inexecução parcial do objeto contratado.	Multa de até **30% (trinta por cento)** sobre o valor da Nota de Empenho, sem prejuízo das demais sanções previstas.	Não se aplica.
14	Inexecução total do objeto.	Multa de até **30% (trinta por cento**) sobre o valor total do contrato, sem prejuízo das demais sanções previstas.	Não se aplica.

III. Com fundamento no artigo 156, inciso III, da Lei n.º 14.133/2021, ficará impedido de licitar e contratar, pelo prazo de até 3 (três) anos, sem prejuízo de multa de até 10% (dez por cento) do valor estimado para a contratação e demais cominações legais, nos seguintes casos:

a) Apresentar documentação falsa;

b) Ensejar o retardamento da execução do objeto;

c) Comportar-se de modo inidôneo;

d) Não manter a proposta;

e) Deixar de entregar a documentação exigida no certame, e quando esta conduta caracterizar fraude à licitação pública;

f) Cometer fraude fiscal;

g) Fazer declaração falsa.

8.2. Para fins da subcondição da alínea "c" do item III, reputar-se-ão inidôneos atos como os descritos nos arts. 337-F, 337-H, 337-I, 337-J, 337-K e 337-M do Código Penal.

8.3 A sanção de impedimento de licitar e contratar prevista no item III também aplicável em quaisquer das hipóteses previstas como infração administrativa deste Termo de Referência.

8.4 Serão descontados dos pagamentos porventura devidos à CONTRATADA as importâncias alusivas a multas, ou efetuar sua cobrança mediante inscrição na dívida ativa do Estado, ou por qualquer outra forma prevista em lei.

8.5 Caso a CONTRATANTE determine, a multa deverá ser recolhida no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

8.6 Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a CONTRATANTE poderá cobrar o valor remanescente judicialmente.

8.7 A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

8.8 Se, durante o processo de aplicação de penalidade, houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846/2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou processo administrativo.

8.9 A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846/2013, seguirão seu rito normal na unidade administrativa.

9. ACORDO DE NÍVEL DE SERVIÇO (SLA)

9.1 Os chamados de suporte técnico serão classificados conforme o nível de severidade, com base no impacto causado no ambiente computacional da CONTRATANTE, conforme as tabelas a seguir:

9.1.1 Impacto:

Nível	Descrição do Impacto
1	Serviços totalmente indisponíveis
2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos
3	Acesso aos aplicativos

9.1.2 Níveis de Severidade:

Modalidade	Prazo	Níveis de Severidade		
		1	2	3
Remoto	Início do Atendimento	1 hora	4 horas	8 horas
	Solução do Contorno	8 horas	12 horas	24 horas

9.2 Quando for necessário atendimento presencial, a CONTRATADA deverá disponibilizar técnicos para resolver os problemas no local. Preferencialmente, essas atividades devem ser previamente acordadas entre as partes, exceto em casos de severidade máxima ou evidente indisponibilidade da infraestrutura da CONTRATANTE.

9.3 O início do atendimento será considerado a partir da abertura do chamado técnico.

9.4 O atendimento será considerado encerrado quando a solução estiver disponível e funcionando perfeitamente no local de instalação.

9.5 Durante toda a vigência do contrato, a CONTRATANTE poderá abrir chamados ilimitados para suporte técnico.

9.6 A CONTRATADA será integralmente responsável por quaisquer danos ou prejuízos causados ao patrimônio da CONTRATANTE ou de terceiros, decorrentes de ações ou omissões de seus colaboradores durante a execução dos serviços solicitados.

9.7 Qualquer atividade relacionada a configurações, ajustes ou parametrizações após a implantação deverá ser precedida da abertura de um chamado técnico.

9.8 Caso a atividade seja realizada de forma proativa, a CONTRATADA deverá comunicar à CONTRATANTE, via e-mail, justificando a execução antecipada.

9.9 Se alguma atividade exigir a interrupção da solução, a CONTRATANTE deverá ser imediatamente notificada para autorizar ou reagendar a execução.

9.10 Atualizações que impliquem indisponibilidade do ambiente devem ser previamente agendadas com a equipe técnica da CONTRATANTE.

9.11 A CONTRATADA deverá manter uma Central de Atendimento em português (Brasil), operando 24 horas por dia, 7 dias por semana, durante todo o ano (24x7x365), para abertura de chamados e demais comunicações.

9.12 A CONTRATANTE poderá solicitar serviços específicos por meio dos seguintes canais de comunicação:

a) E-mail;

b) Telefone 0800;

c) Sistema de Chamados Web.

9.13 O serviço será considerado concluído somente após a confirmação da área técnica da CONTRATANTE quanto à sua execução satisfatória.

9.14 O encerramento de solicitações técnicas dependerá da anuência de ambas as partes: CONTRATADA e CONTRATANTE.

9.15 A CONTRATADA manterá um cadastro com os nomes das pessoas indicadas pela CONTRATANTE autorizadas a abrir e encerrar chamados.

9.16 O prazo para encerramento do atendimento não poderá ultrapassar os limites estabelecidos para cada nível de criticidade.

9.17 Considera-se suporte técnico as atividades que requerem acompanhamento por parte de um técnico da CONTRATANTE.

9.18 Quando for necessário atendimento local, o cronograma de execução deverá ser acordado entre as partes.

9.19 A CONTRATADA deverá iniciar o atendimento conforme os prazos definidos para cada nível de criticidade.

9.20 A manutenção corretiva inclui os serviços necessários para restaurar o funcionamento adequado dos equipamentos, com fornecimento de peças conforme especificações do fabricante, em caso de falhas ou defeitos de hardware.

9.21 A CONTRATADA deverá realizar os serviços de manutenção com ferramentas próprias e técnicos especializados, devidamente identificados.

9.22 O suporte técnico compreende ações para restabelecer o funcionamento correto das soluções contratadas, incluindo configuração, habilitação, implementação, manutenção e colocação em produção de funcionalidades.

9.23 Caso seja necessária a atualização de firmware, a CONTRATADA deverá fornecer o pacote de software e realizar a atualização.

9.24 Considerando que a resolução de problemas de software pode envolver o desenvolvimento de patches, admite-se a adoção de soluções de contorno (workaround) até a implementação da solução definitiva.

9.25 O período para solução de ocorrências de software será contado entre a formalização e o encerramento efetivo da ocorrência, seja com solução definitiva ou provisória.

9.26 Para ocorrências de hardware não resolvidas dentro do prazo, a CONTRATADA deverá substituir o equipamento ou módulo defeituoso em até 72 (setenta e duas) horas úteis. Após a substituição, deverá ser entregue um documento com as descrições e números de série dos equipamentos substituídos e novos.

9.27 A substituição definitiva de hardware deverá ser feita com equipamento novo, original, recomendado pelo fabricante, com configuração igual ou superior à do substituído.

9.28 Durante a substituição, a CONTRATADA deverá entregar documento contendo a descrição e número de série do equipamento defeituoso e do novo equipamento.

9.29 O prazo para solução de ocorrências de hardware será contado entre a formalização e o encerramento efetivo da ocorrência. Quando houver substituição, o encerramento será considerado apenas após o novo equipamento entrar em operação.

9.30 Para cálculo do tempo de atendimento, serão desconsiderados os períodos em que a CONTRATANTE estiver responsável por ações necessárias à análise e solução da ocorrência.

9.31 Não haverá limitação quanto ao número de técnicos da CONTRATANTE autorizados a abrir chamados, desde que previamente registrados como pontos de contato.

9.32 Durante o período de garantia, a CONTRATADA deverá fornecer todas as atualizações de software (versões, releases, patches), firmware ou microcódigos dos hardwares cobertos pela manutenção, sem custo adicional.

10. FORMA DE PAGAMENTO

10.1 O pagamento será realizado à CONTRATADA de forma integral e condicionado ao marco da emissão do Termo de Recebimento Definitivo do objeto assinado por ambas partes;

10.2 O pagamento devido à CONTRATADA será creditado em conta-corrente por meio de ordem bancária, efetuado mediante apresentação de DANFE com o devido "atesto" de recebimento pela fiscalização da PGJ.

10.2.1 O documento fiscal, emitido em conformidade com o Protocolo ICMS 42/2009 (NF-e), deverá estar devidamente discriminado, em nome da PROCURADORIA-GERAL DE JUSTIÇA, CNPJ n.º 04.153.748/0001-85, e acompanhada das respectivas Certidões Negativas de Débito para com a Seguridade Social, para com o Fundo de Garantia por Tempo de Serviço, junto à Justiça Trabalhista e, ainda, das certidões de regularidade junto à Fazenda Federal, Estadual e Municipal, conforme o disposto no artigo 68 da Lei nº 14.133/2021, bem como da formalização do pedido de pagamento e do recibo a PGJ;

10.2.2 Deverão constar do documento fiscal as especificações dos produtos, o número da Nota de Empenho e da Ata/Contrato, conforme o caso; e

10.2.3 Enquanto pendente de liquidação, por obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência contratual, nenhum pagamento será efetuado à Contratada, sem que isso gere direito a acréscimos de qualquer natureza.

10.2.4 Na emissão da nota fiscal/fatura, a CONTRATADA deverá atentar para as orientações de retenção tributária na legislação aplicável.

10.3 Qualquer atraso ocorrido na apresentação do DANFE, ou dos documentos exigidos como condição de pagamento por parte da Contratada, importará prorrogação automática do prazo de vencimento da obrigação do Contratante.

10.4 Nenhum pagamento isentará o fornecedor das responsabilidades atinentes ao objeto contratual, nem tampouco implicará a aprovação definitiva da entrega, total ou parcialmente.

10.5 O documento fiscal, devidamente atestado, e os documentos exigidos neste Termo, no Edital e na Ata/Contrato, para fins de liquidação e pagamento das despesas, deverão ser entregues no Setor de Protocolo da Contratante (email: protocolo@mpam.mp.br) e na Diretoria de Tecnologia da Informação e Comunicação (e-mail: dtic@mpam.mp.br).

10.6 Como condição para emissão da Nota de Empenho, a licitante vencedora manterá a condição de habilitação, cuja confirmação será feita através de consulta ao SICAF ou através da *internet* nos respectivos *sites* dos órgãos emissores das certidões de regularidade fiscal.

10.7 Como condição inafastável a que seja emitida Nota de Empenho à Contratada, esta deverá, também, estar cadastrada junto ao Sistema de Administração Financeira e Contabilidade – Cadastramento de Credores – da Secretaria da Fazenda do Estado do Amazonas – SEFAZ.

11. ESPECIFICAÇÕES TÉCNICAS DO OBJETO

11.1 O objeto deste Termo compreende a contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais do Ministério Público do Estado do Amazonas (MPAM).

11.2 Por tratar-se de solução integrada, onde o funcionamento efetivo e satisfatório depende de cada um dos seus itens em conjunto, como um todo, ou seja, o simples funcionamento de itens separadamente não tem nenhuma funcionalidade, conforme indicado no Estudo Técnico Preliminar (ETP), a contratação terá lote único, organizado conforme tabela a seguir:

ITEM	DESCRIÇÃO	QUANTIDADE
01	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9	4
02	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU	1
03	SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX	5
04	SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU	1

05	LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE	50
06	SOFTWARE DE BACKUP DE DADOS	1
07	EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	1
08	SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	1
09	SWITCH CORE	2

11.3 Nas especificações técnicas mínimas apresentadas a seguir, os termos "possui", "permite", "suporta" e "é" implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo "ou" implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo "e" implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções citadas.

11.4 A CONTRATADA não poderá oferecer serviço inferior as especificações apresentadas neste Termo, sendo permitido, porém, a oferta de serviço superior as especificações mínimas apresentadas, de acordo com a conveniência da CONTRATADA e aprovação do CONTRATANTE.

11.5 Toda documentação gerada durante a prestação dos serviços será de propriedade do CONTRATANTE, em virtude de sua elaboração tomar por base informações críticas do funcionamento intrínseco à sua infraestrutura, que afetam diretamente a segurança do CONTRATANTE.

11.6 A CONTRATADA deverá guardar inteiro sigilo dos serviços contratados e dos dados processados, bem como de toda e qualquer documentação gerada, reconhecendo serem esses de propriedade e uso exclusivo do CONTRATANTE, sendo vedada sua cessão, locação ou venda a terceiros.

11.7 CONTRATADA deverá manter o CONTRATANTE atualizado sobre todos os fluxos adotados para a execução das atividades objeto da contratação durante o período contratual, bem como sobre a forma de automatização de quaisquer serviços, documentando todos os procedimentos detalhadamente para que possam servir de base para a continuidade dos serviços independentemente da metodologia que possa ser adotada.

11.8 ITEM 01 - EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9

11.8.1 Características Gerais

11.8.1.1 A infraestrutura deverá ser composta por appliances Nutanix com integração completa entre hardware e software, armazenamento e rede, entregando uma solução hiperconvergente pronta para operação.

11.8.1.2 Serão aceitos apenas appliances homologados pela Nutanix para uso com o Nutanix AOS (Acropolis Operating System) e Nutanix AHV (Acropolis Hypervisor) ou outro hipervisor suportado pela plataforma.

11.8.1.3 Caso necessário, será permitida a entrega de equipamentos ou recursos adicionais para atender aos requisitos mínimos, desde que todos os componentes estejam integrados e certificados pela Nutanix.

11.8.1.4 É permitida a entrega de múltiplos nós em um único chassi, desde que compatível com a arquitetura Nutanix.

11.8.1.5 A solução deve incluir a ferramenta unificada de monitoração, em sua ultima versão ou equivalente, que oferece gerenciamento centralizado e interface gráfica para monitoramento, atualizações e operação da infraestrutura, incluindo:

11.8.1.5.1 Atualização de BIOS, firmware, hipervisor e SDS;

11.8.1.5.2 Visualização do hardware físico;

11.8.1.5.3 Diagnóstico, inventário e expansão de nós.

11.8.1.6 Caso alguma funcionalidade não esteja disponível na ferramenta unificada ou equivalente para monitoramento ou atualização, a CONTRATADA deverá realizar este serviço de forma remota/on-line ou presencial.

11.8.1.7 Todas as atualizações devem ser homologadas pela Nutanix e aplicadas conforme as melhores práticas da fabricante. Esta ferramenta deve ser gráfica, com suporte a apresentação de visões do hardware físico dos nós, suporte a troca de drives, com controle do inventário, com ferramenta de diagnóstico e com módulo para a adição de novos nós.

11.8.1.8 A arquitetura deve garantir alta disponibilidade (HA) e resiliência a falhas, com suporte a recuperação de desastres (DR).

11.8.1.9 Os appliances devem permitir expansão modular e não disruptiva dos serviços de rede e

aplicações, com detecção automática de novos nós.

11.8.1.10 Deve centralizar o armazenamento de dados em discos compartilhados, redundantes.

11.8.1.11 Cada nó deverá conter armazenamento dedicado para o sistema operacional da plataforma.

11.8.1.12 A solução deve estar preparada para ambientes de virtualização em alta disponibilidade, conforme as práticas recomendadas pela Nutanix.

11.8.1.13 Deve suportar software de virtualização para consolidação de servidores e recuperação automática em caso de falhas físicas, minimizando o downtime.

11.8.1.14 A entrega deve ser feita com todos os componentes física e logicamente integrados, sem ponto único de falha, com acesso imediato ao ambiente via sistema de gestão da plataforma após energização e conexão.

11.8.1.15 A instalação deve ser compatível com racks padrão de 19 polegadas, incluindo todos os acessórios necessários para montagem no ambiente da CONTRATANTE.

11.8.1.16 O equipamento deve integrar a linha de produtos Nutanix da família “NX”, assegurando total compatibilidade com atual ambiente e possibilidade de expansão das zonas de disponibilidade já estabelecidas, conforme informações disponibilizadas no endereço eletrônico oficial da fabricante: https://www.nutanix.com/products/hardwareplatforms/specsheet?platformProvider=Nutanix

11.8.2 Configuração do Nó ou Chassi

11.8.2.1 Serão admitidas ofertas de chassis que comportam múltiplos servidores (nós/nodes), para o atendimento da especificação técnica.

11.8.2.2 Cada nó, ou chassi, deverá possuir ventiladores e fontes redundantes para a operação adequada dos equipamentos.

11.8.2.3 Todas as fontes de alimentação deverão ser acompanhadas de seus respectivos cabos de energia compatíveis.

11.8.3 Características de Processamento por Nó

11.8.3.1 Cada servidor deverá possuir, no mínimo, 02 (dois) processadores com arquitetura x86, voltados ao uso em servidores, contendo as seguintes características mínimas:

11.8.3.1.1 12 (doze) núcleos físicos e 24 (vinte e quatro) threads por processador;

11.8.3.1.2 Frequência de clock nominal de, no mínimo, 2,4 GHz;

11.8.3.1.3 Controladora de memória integrada com suporte à tecnologia DDR5 ou superior.

11.8.3.2 Será admitida a entrega de processadores de geração superior ao modelo originalmente especificado, desde que mantenham no mínimo a mesma quantidade de núcleos e threads, independentemente de demais especificações.

11.8.4 Especificações de Memória por Nó

11.8.4.1 Cada servidor deverá ser fornecido com, no mínimo, 1536 GB (um mil quinhentos e trinta e seis gigabytes) de memória RAM, distribuída uniformemente entre os processadores, utilizando módulos DDR5 ou superior.

11.8.5 Especificações de Rede por Nó

11.8.5.1 Cada servidor deverá ser entregue com as seguintes interfaces de rede:

11.8.5.1.1 Mínimo de 2 (duas) interfaces de 25/10 GbE SFP28, integradas em uma placa de rede;

11.8.5.1.2 Mínimo de 1 (uma) interface exclusiva de gerenciamento Ethernet 1000Base-T.

11.8.5.2 A interface de gerenciamento deverá vir acompanhada de cabos UTP categoria 6 (ou superior), com comprimento mínimo de 5 (cinco) metros e conectores RJ-45.

11.8.6 Especificações de Armazenamento por Nó

11.8.6.1 Cada servidor deverá ser entregue com a seguinte configuração mínima de discos:

11.8.6.1.1 04 (quatro) unidades de SSD NVMe, ou SSD SAS/SATA, com capacidade mínima de 3,84 TB por unidade (volumetria bruta);

11.8.6.1.2 08 (oito) unidades de disco rígido (HDD), com capacidade mínima de 12 TB por unidade (volumetria bruta).

11.9 ITEM 02 - EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU

11.9.1 Características Gerais

11.9.1.1 A solução deverá ser composta exclusivamente por appliances de nuvem privada, com integração total entre recursos de computação, armazenamento e rede, entregues como infraestrutura unificada.

11.9.1.2 Serão aceitos apenas appliances homologados para uso com a solução de armazenamento definido por software (Software Defined Storage – SDS) ofertada.

11.9.1.3 A entrega de equipamentos ou recursos adicionais será aceita, desde que necessária para o atendimento aos requisitos mínimos e que todos os componentes estejam devidamente integrados.

11.9.1.4 É permitida a entrega de múltiplos nós consolidados em um único chassi modular.

11.9.1.5 A solução deverá incluir ferramenta unificada de gerenciamento e atualização, com capacidade de monitorar e atualizar BIOS, firmwares, hypervisor e componentes do SDS. Caso não realize todos os procedimentos listados, a CONTRATADA deverá garantir a execução dessas tarefas online e / ou presencial.

11.9.1.6 A ferramenta de gestão deverá ser gráfica, com visualização física dos nós, suporte à substituição de drives, inventário automatizado, diagnóstico integrado e capacidade de adicionar novos nós ao cluster.

11.9.1.7 A arquitetura deverá contemplar alta disponibilidade nativa e recursos para recuperação de desastres (DR), de forma a garantir continuidade dos serviços mesmo em caso de falhas parciais.

11.9.1.8 Os equipamentos devem possuir arquitetura modular, permitindo expansão de capacidade com inclusão de novos appliances sem interrupção dos serviços.

11.9.1.9 O armazenamento deverá ser centralizado, com discos compartilhados e redundância nativa.

11.9.1.10 Cada servidor deverá conter unidade de armazenamento dedicada ao sistema operacional da plataforma e aos softwares de virtualização , processamento gráfico e calculo aritmético.

11.9.1.11 A infraestrutura deverá estar preparada para suportar ambientes virtualizados de alta disponibilidade, de acordo com as boas práticas do fabricante da solução.

11.9.1.12 A solução deverá oferecer suporte a consolidação de servidores e recuperação automática em caso de falhas de hardware.

11.9.1.13 A entrega deverá ocorrer com a solução fisicamente e logicamente pré-integrada, sem ponto único de falha, com acesso imediato à plataforma após energização e conexão física.

11.9.1.14 A instalação deverá ser compatível com racks padrão de 19"(dezenove polegadas), com todos os acessórios de fixação inclusos.

11.9.1.15 O equipamento deve integrar a linha de produtos Nutanix da família “NX”, assegurando total compatibilidade com atual ambiente e possibilidade de expansão das zonas de disponibilidade já estabelecidas, conforme informações disponibilizadas no endereço eletrônico oficial da fabricante: https://www.nutanix.com/products/hardwareplatforms/specsheet?platformProvider=Nutanix

11.9.2 Configuração do Nó ou Chassi

11.9.2.1 Serão admitidas ofertas de chassis que comportam múltiplos servidores (nós/nodes), para o atendimento da especificação técnica.

11.9.2.2 Cada nó ou chassi deverá possuir ventiladores e fontes de alimentação redundantes.

11.9.2.3 Cada fonte deverá ser entregue com seu respectivo cabo de energia.

11.9.3 Características de Processamento por Nó

11.9.3.1 Cada servidor deverá possuir, no mínimo, dois processadores com arquitetura x86, dedicados a ambientes de datacenter, com as seguintes características mínimas:

11.9.3.2 12 (doze) núcleos físicos e 24 (vinte e quatro) threads por processador;

11.9.3.3 Frequência mínima de 2,4 GHz;

11.9.3.4 Controladora de memória integrada DDR5 ou superior.

11.9.3.5 A substituição por processadores mais recentes será aceita, desde que observadas as quantidades mínimas de núcleos e threads.

11.9.4 Especificações de Memória por Nó

11.9.4.1 Cada servidor deverá ser entregue com no mínimo 1024 GB (um mil e vinte e quatro gigabytes) de memória RAM, utilizando módulos DDR4 ou superior, distribuídos de forma equilibrada entre os processadores.

11.9.5 Especificações de Rede por Nó

11.9.5.1 Cada servidor deverá conter no mínimo:

11.9.5.1.1 2 (duas)interfaces de rede 25/10 GbE SFP28;

11.9.5.1.2 1 (uma) interface de gerenciamento 1000Base-T;

11.9.5.1.3 A interface de gerenciamento deverá ser acompanhada de cabos UTP Cat-6 ou superior, com 5 metros de comprimento e conectores RJ-45.

11.9.6 Especificações de Armazenamento por Nó

11.9.6.1 Cada servidor deverá ser fornecido com a seguinte configuração de discos:

11.9.6.1.1 2 discos SSD NVMe, SAS ou SATA, com capacidade mínima de 3,84 TB cada (volumetria bruta);

11.9.6.1.2 4 discos HDD com capacidade mínima de 12 TB cada (volumetria bruta).

11.9.7 Especificações de Processamento Gráfico e Cálculo Aritmético

11.9.7.1 Cada servidor deverá conter uma placa gráfica com as seguintes características mínimas:

11.9.7.1.1 48 GB de memória GDDR6 de GPU;

11.9.7.1.2 Interconexão PCIe Gen4 com largura de banda de 64 GB/s;

11.9.7.1.3 Suporte a DirectX 12.075, Shader Model 5.175, OpenGL 4.686 e Vulkan 1.186;

11.9.7.1.4 Compatibilidade com NVIDIA vPC/vApps, NVIDIA RTX Virtual Workstation e NVIDIA Virtual Compute Server;

11.9.7.1.5 Consumo máximo de 350W.

11.10 ITEM 03 – SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX

11.10.1 Camada de Armazenamento da Solução:

11.10.1.1 A solução deverá contar com camada de armazenamento compartilhada entre todos os servidores e appliances descritos neste Termo, utilizando tecnologia de armazenamento definido por software (Software Defined Storage – SDS).

11.10.1.2 A arquitetura de armazenamento deverá ser otimizada para ambientes virtuais, com escalabilidade contínua e elástica, permitindo expansão de capacidade pela adição de novos nós/appliances sem necessidade de licenciamento adicional de virtualização.

11.10.1.3 Não serão aceitas soluções baseadas em tecnologia RAID para redundância de dados.

11.10.1.4 A solução deverá suportar as tecnologias de compressão e desduplicação de dados inline, near-line ou pós-processada, com o objetivo de otimização do armazenamento.

11.10.1.5 A solução deverá prover recursos de QoS (Quality of Service), para controle do volume de I/Os de VMs.

11.10.1.6 Deverá permitir uso de técnicas de Erasure Coding para otimização de aplicações com baixa sensibilidade à latência de escrita.

11.10.1.7 A solução deverá permitir a expansão do cluster através da adição de nós/servidores que incrementem tão somente a capacidade de armazenamento, sem a necessidade de emprego de licenças de virtualização nesses nós/servidores;

11.10.1.8 A substituição de discos defeituosos deverá ocorrer sem impacto nas operações de leitura e escrita das aplicações.

11.10.1.9 A falha de um nó da solução não poderá comprometer a disponibilidade da camada de armazenamento das VMs.

11.10.1.10 A criptografia deverá ser aplicada em nível de cluster ou volume, via hardware ou software, com KMS nativo. Caso não possua, será aceita entrega de servidor redundante externo com essa funcionalidade.

11.10.1.11 A distribuição dos dados deverá ocorrer de forma automática e uniforme dentro do cluster.

11.10.1.12 A solução deverá permitir criação de cópias no tempo (snapshots) sem movimentação dos dados originais e com redirecionamento de escritas subsequentes.

11.10.1.13 Deverá suportar clonagem de instâncias virtuais a partir de snapshots, sem movimentação dos dados.

11.10.1.14 Acesso ao armazenamento deverá ser possível via iSCSI por instâncias físicas ou virtuais externas ao cluster, garantindo suporte a aplicações de alta disponibilidade.

11.10.2 Tecnologia de Replicação e Proteção de Dados:

11.10.2.1 Deverá ser fornecida funcionalidade de replicação local realizando clones e snapshots com proteção contínua dos dados da máquina virtual;

11.10.2.2 A solução deve prover as funcionalidades de Thin Provisioning e Serviços de Cópias de dados;

11.10.2.3 Deverá permitir a configuração de um grupo ou domínio de proteção de instâncias virtuais, que poderão ser protegidas por cópias point-in-time, bem como replicadas para um cluster remoto;

11.10.2.4 Deverá permitir a união de máquinas virtuais em um único grupo de proteção.

11.10.2.5 Deverá proteger, por cópias point-in-time, simultaneamente todas as máquinas virtuais

pertencentes ao grupo;

11.10.2.6 Deverá contemplar, também, a proteção nativa de máquinas virtuais consistentes com aplicações, onde há proteção dos dados em memória a partir da movimentação das operações de escrita para disco, de sistemas operacionais Linux e Windows. Caso a plataforma de nuvem privada não permita executar esta funcionalidade nativamente, a CONTRATADA deverá atender este requisito compondo com outra solução.

11.10.2.7 Deverá permitir a configuração de uma entidade capaz de centralizar todo o fluxo do tráfego replicado entre clusters distintos, convergindo assim os recursos para um único ponto focal. Esse recurso centralizado deverá posteriormente redirecionar o tráfego corretamente para os equipamentos específicos do cluster de contingência;

11.10.2.8 Deverá permitir ajustar o consumo de banda em replicações;

11.10.2.9 Deverá permitir a existência de frequências distintas de replicação para instâncias virtuais em grupos diferentes;

11.10.3 Gerenciamento Integrado:

11.10.3.1 A solução deve oferecer solução de gerenciamento integrado, licenciado para gerenciar inclusive múltiplos clusters.

11.10.3.2 Monitoração automática e periódica da solução, com o envio de notificações preventivamente em caso de falhas, notificando o suporte do fornecedor a tomar medidas preventivas e acordadas com a CONTRATANTE a fim de evitar tempo de inatividade e impactos na produção.

11.10.3.3 Deve oferecer portal de acesso do próprio fornecedor para download de atualizações e de softwares agregados.

11.10.3.4 A ferramenta de gerenciamento, local, deve fornecer um dashboard reportando a utilização dos recursos do cluster como CPU, Memória, Armazenamento, IOPS do cluster, largura de banda do cluster, latência do cluster e informações sobre o virtualizador empregado e os alertas de saúde.

11.10.3.5 A solução deve fornecer atualização de todos os componentes (Firmware, e softwares de virtualização que fazem parte da solução) em forma de pacote com instalação assistida.

11.10.3.6 Contemplar as funcionalidades como:

11.10.3.6.1 Emissão de relatório avançados do ambiente;

11.10.3.6.2 Personalização da console principal;

11.10.3.6.3 Planejamento e previsão de capacidade;

11.10.3.6.4 Detecção de ineficiência de cargas de trabalho e dimensionamento ideal;

11.10.3.6.5 Planejamento de capacidade ou cargas de trabalho ao longo do tempo;

11.10.3.6.6 Permitir automação de operações de gerência do ambiente

11.10.4 Provisionamento de Containers:

11.10.4.1 Deverá ser entregue uma plataforma de provisionamento de containers, integrada, a plataforma de virtualização.

11.10.4.2 A plataforma deverá permitir a criação de múltiplo clusters.

11.10.4.3 A fabricante da solução deverá, comprovadamente, pertencer a categoria de membro da CNCF (Cloud Native Computing Foundation).

11.10.4.4 Seleção de sistemas operacionais, bem como suas distintas versões de microcódigo para implementação automática, sendo compatível com sistemas Linux.

11.10.4.5 Seleção das configurações de rede do cluster de containers ou microserviços.

11.10.4.6 Seleção do tipo de armazenamento persistente a ser empregado em containers.

11.10.4.7 Seleção da quantidade de nós dos tipos “Control Plane” e “Workers” que serão implementados simultaneamente.

11.10.4.8 A plataforma de containers deverá permitir a criação de alertas, facilitando a gestão do cluster.

11.10.4.9 Deverá ter suporte a implementação de clusters de plataformas de containers, similares a Kubernetes, NCI, baremetal, public cloud.

11.10.4.10 A plataforma de containers deverá possuir integração para o acesso através de RBAC, permitindo seu uso completo através de acesso administrativo e permitindo seu uso parcial através de acesso controlado aos demais usuários.

11.10.4.11 Suporte implementação de clusters de plataformas de containers, similares a Kubernetes com suporte a Bring-Your-Own-OS: Rocky Linux, Ubuntu, RHEL e similares.

11.10.4.12 Permitir a configuração de clusters com alta-disponibilidade para os “Control Plane”

nodes, com ou sem balanceador de carga;

11.10.4.13 Prover armazenamento persistente através de integração com Container Storage Interface (CSI), para armazenamento de blocos e arquivos. Também deverá ser possível configurar armazenamento de arquivos compatível com protocolo Simple Storage Service;

11.10.4.14 Deverá fornecer um mecanismo de monitoramento que aciona alertas no cluster Kubernetes;

11.10.4.15 Oferecer as seguintes funcionalidades em ambiente Kubernetes:

11.10.4.15.1 Gerenciamento de Dados;

11.10.4.15.2 Proteção e Restauração de Dados;

11.10.4.15.3 Aceleração da Entrega de Aplicativos;

11.10.4.15.4 Gerenciamento de Autoatendimento de Aplicativos;

11.10.4.15.5 Automação e Monitoramento de Infraestrutura;

11.10.4.15.6 Padronização de Políticas de Governança e Conformidade;

11.10.4.16 Para a estratégia de criação de cópias dos dados para ambiente de containers Kubernetes, a solução deverá permitir:

11.10.4.16.1 Fornecimento de software para “worker nodes” Kubernetes, garantindo o suporte unificado e conjunto da solução como um todo;

11.10.4.16.2 Plataformas de container baseadas em Kubernetes.

11.10.4.16.3 Permitira realização de copias e armazenamento em repositório externo.

11.10.4.16.4 Movimentação das imagens de backup para compartilhamentos NFS por meio de solução de armazenamento compatível com protocolo S3, permitindo que o repositório NFS seja utilizado como backend de Object Storage.

11.10.4.16.5 Capacidade de restaurar o Namespace para seu local original e para um novo Namespace.

11.10.5 Segurança de Rede:

11.10.5.1 Suportar microssegmentação para prover controle granular e governança de todo o tráfego de entrada e saída de uma máquina virtual (VM), grupos de máquinas virtuais (VMs) e containers.

11.10.5.2 Permitir a associação de políticas de rede a VMs e conteiners em vez de segmentos de rede específicos (por exemplo VLANs) ou identificadores (endereços IP ou MAC).

11.10.5.3 Prover visualização de tráfego e relacionamentos com a descoberta automática dos fluxos entre as máquinas virtuais e containers.

11.10.5.4 Permitir políticas de segurança centradas na carga de trabalho em vez de uma abordagem centrada na rede, permitindo examinar o tráfego de, e para as VMs, independentemente de como as configurações de rede mudam e onde residem no data center

11.10.5.5 Políticas aplicadas por categorias de VMs e containers.

11.10.5.6 Permitir isolamento de conteiners e VMs comprometidas, colocando-a em quarentena.

11.10.5.7 - Permitir restrição de tráfego entre camadas de aplicação.

11.10.5.8 Atualização automática de políticas.

11.10.5.9 Integração com ferramentas de terceiros como IDS/IPS e load balancer.

11.10.6 Licenciamento do Software de Virtualização:

11.10.6.1 Entrega do licenciamento completo da plataforma de virtualização, versão mais avançada.

11.10.6.2 Suporte à criação de VMs com múltiplas interfaces de rede e múltiplas arquiteturas (32/64 bits).

11.10.6.3 Permitir provisionamento aos principais sistemas operacionais (Windows Server 2022, CentOS 8, Ubuntu 20, RHEL 9) ou superiores.

11.10.6.4 Alocação dinâmica de recursos (CPU/RAM).

11.10.6.5 Hypervisor deverá estar instalado em unidade flash dedicada.

11.10.6.6 Suporte a GPU virtual ou passthrough nativo.

11.10.6.7 Suporte a BIOS/UEFI, snapshots, exportação OVA.

11.10.6.8 Deverá permitir o provisionamento de máquinas virtuais, e grupos de máquinas virtuais, em equipamentos específicos com o propósito de respeitar licenciamentos de aplicações. Em caso de falha do equipamento, a máquina virtual não deverá ser migrada para outro equipamento remanescente;

11.10.6.9 Alta resiliência a falhas de nós/discos.

11.10.6.10 Armazenamento distribuído e gerenciado via console web.

11.10.6.11 Deverá permitir a inicialização, a reinicialização, o reset, o desligamento da VM e o desligamento do sistema operacional dela;

11.10.6.12 Suportar a tecnologia de snapshot nativos do Hypervisor;

11.10.6.13 Permitir a adição de novos servidores no cluster;

11.10.6.14 Permitir criar uma área de armazenamento compartilhada, distribuída e otimizada para ambientes virtuais;

11.10.6.15 Permitir o agrupamento dos volumes lógicos de todos os servidores no cluster provendo uma área de armazenamento comum para o ambiente virtual;

11.10.6.16 Possuir mecanismo de redundância e proteção de dados nativo que armazena cópias dos dados em diversos discos e hosts do cluster de forma transparente;

11.10.6.17 Deverá ser fornecido licenciamento do software de virtualização na versão mais completa para todos os servidores do ambiente de armazenamento distribuído.

11.10.6.18 Deverá contemplar pelo menos 20 (vinte) núcleos de processamento virtuais (vCPU) ou físicos (pCPU) de solução para gestão de base de dados como serviço (DBaaS).

11.10.6.19 Deverá ser totalmente compatível com a solução ofertada para atendimento aos requisitos deste termo de referência.

11.10.6.20 Permitir automatizar as tarefas para provisionamento, emprego de correções de software (patching), gerenciamento do ciclo de vida, clonagem, atualização dos dados em bases clonadas (refresh), proteção contínua e recuperação de bases de dados.

11.10.6.21 Deverá ser compatível pelo menos com Oracle, Microsoft SQL, PostgreSQL, MariaDB, MongoDB e MySQL.

11.10.6.22 Permitir o uso de uma chave SSH pública para acesso ao servidor de banco de dados com opção através do upload de um arquivo e através da inserção direta da chave em campo de texto.

11.10.6.23 A solução deverá permitir registrar bancos de dados existentes para emprego de proteção contínua capturando e mantendo snapshots e registros (logs) transacionais da base de dados de origem conforme definições contidas no agendamento.

11.10.6.24 A mesma tecnologia deverá permitir a clonagem de bases de dados.

11.10.6.25 Durante a clonagem, a solução deverá permitir a escolha para o administrador utilizar um servidor de banco de dados registrado ou criar um novo servidor.

11.10.6.26 Permitir que o administrador realize o clone de uma base de dados a partir de um snapshot.

11.10.6.27 Permitir que o administrador realize o clone de uma base de dados dentro de uma política de proteção contínua, ou seja, clonar uma base de dados em determinado dia, hora, minuto e segundo.

11.10.6.28 Permitir a definição de agendamento da periodicidade para realizar a atualização (refresh) dos dados da base clonada através do estado atual na base de dados de origem.

11.10.6.29 Permitir a definição de uma data para remoção ou exclusão do clone.

11.10.6.30 Permitir a execução de scripts ou comandos de pré e pós clonagem.

11.10.6.31 Deverá ser possível definir as políticas de retenção dos snapshots diários, semanais, mensais e trimestrais.

11.11 ITEM 04 – SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU

11.11.1 Software para Processamento Gráfico e Cálculo Aritmético:

11.11.1.1 Permitir a seleção, implantação e gestão de modelos de IA Generativa (LLMs) provenientes da Hugging Face e NVIDIA, bem como a importação de modelos personalizados ou treinados pelo contratante em clusters Kubernetes.

11.11.1.10 Permitir a criação de um endpoint de inferência e o compartilhamento dele com desenvolvedores para incorporar em seus aplicativos de IA. Permitir gerenciar e validar esses endpoints para garantir que eles estejam configurados corretamente.

11.11.1.11 Permitir o acesso a um endpoint de inferência por um aplicativo usando chaves de API. O gerenciamento de chaves de API deverá permitir o fornecimento e revogação do acesso à API para garantir controles de segurança de acesso adequados.

11.11.1.12 Permitir o controle de acesso baseado em função (RBAC), para fornecer permissões de acesso personalizadas aos usuários com base em suas funções atribuídas.

11.11.1.13 Possuir uma interface de usuário simples e dinâmica que simplifique o processo de implantação.

11.11.1.14 Possuir um painel dinâmico que permita monitorar a integridade da implantação com ferramentas de monitoramento em tempo real que identifiquem gargalos, rastreiem o desempenho e solucionem problemas.

11.11.1.15 Suportar a instalação e o funcionamento em estruturas sem qualquer conexão com a Internet (dark-site ou air-gapped).

11.12 ITEM 05 - LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE

11.12.1 A solução deverá incluir unidade de subscrição de software para armazenamento de objetos e arquivos, licenciada por terabyte (TB), com suporte técnico durante 60 (sessenta) meses, contemplando ambiente de produção em operação contínua (24x7).

11.12.2. Caso a solução proposta não ofereça suporte nativo a armazenamento de objetos e arquivos, será permitida a utilização de unidade externa dedicada, desde que esta disponha de todos os componentes, funcionalidades e suporte equivalentes à solução principal.

11.12.3. O sistema de armazenamento definido (SDS) deverá otimizar dados utilizando tecnologia de erasure coding na camada de capacidade, de modo a garantir eficiência e resiliência no armazenamento de arquivos e objetos.

11.12.4. A solução deverá permitir a recuperação granular de arquivos pelos usuários, sem necessidade de intervenção do administrador.

11.12.4.1 Para o protocolo SMB, a restauração deverá ocorrer por meio da funcionalidade “Versões Prévias” da pasta de destino.

11.12.4.2 Para o protocolo NFS, a recuperação deverá ser possível pela listagem do subdiretório oculto (snapshot).

11.12.5. O sistema deverá integrar-se a softwares antivírus de terceiros por meio do protocolo ICAP (Internet Content Adaptation Protocol), possibilitando varredura em tempo real de arquivos compartilhados via SMB sempre que forem abertos, modificados ou encerrados.

11.12.6. A interface de gerenciamento deverá exibir o estado dos arquivos após a varredura antivírus, incluindo status como limpo, em quarentena ou deletado, além do histórico de eventos correspondentes.

11.12.7. A interface de gerenciamento deverá também exibir relatórios detalhados contendo a lista de arquivos analisados, ameaças detectadas e arquivos colocados em quarentena.

11.12.8. A interface de gerenciamento deverá permitir ações diretas sobre os arquivos, incluindo:

11.12.8.1. Reexecução de varredura (Rescan);

11.12.8.2. Remoção de arquivos da quarentena;

11.12.8.3. Exclusão permanente de arquivos em quarentena.

11.12.9. A solução deverá possibilitar a configuração de ambiente de detecção avançada de intrusão (AIDE), capaz de identificar e corrigir automaticamente desvios na configuração de segurança do servidor de arquivos, sem necessidade de intervenção manual.

11.12.10. Deverá ser possível configurar políticas de senha forte (strong password) para o acesso à linha de comando (CLI) do servidor de arquivos.

11.12.11. O sistema deverá suportar configuração de qualidade de serviço (QoS), utilizando valores DSCP para diferenciação de códigos de serviço em rede.

11.12.12. Deverá suportar o protocolo NFS v4.2, otimizando as operações de entrada/saída (I/O) e reduzindo o consumo de rede.

11.12.13. A solução deverá contemplar as seguintes funcionalidades para compartilhamento de arquivos via protocolo SMB:

11.12.14. Autenticação integrada ao Active Directory.

11.12.15. Enumeração baseada em acesso (ABE), exibindo apenas pastas e arquivos aos quais o usuário possui permissão.

11.12.16. Assinatura digital de pacotes SMB (SMB Signing), garantindo autenticidade e integridade das transmissões.

11.12.17. Criptografia em nível de pasta (SMB Encryption), assegurando a confidencialidade dos dados.

11.12.18. Organização de compartilhamentos em um único espaço de nomes (Single Namespace), suportando ambientes locais ou geograficamente distribuídos, por meio do protocolo DFS-N (DFS Namespaces).

11.12.19. Suporte à autenticação via Active Directory e LDAP, além de acesso não gerenciado a

compartilhamentos NFSv4 (autenticação LDAP) e NFSv3.

11.12.20. Suporte a acesso multiprotocolo (SMB e NFS) sobre o mesmo compartilhamento, preservando permissões via Windows ACLs e Unix mode bits.

11.12.21. Suporte a Home Shares por diretório, permitindo o provisionamento automático de pastas pessoais de usuário.

11.12.22. Suporte à aplicação de cotas de uso do sistema de arquivos, com notificações (soft limit) e bloqueio (hard limit), configuráveis por usuário, grupo ou diretório no momento da criação (Directory Level Quotas).

11.12.23. O módulo de armazenamento de objetos deverá possuir API REST compatível com AWS S3, apta a lidar com petabytes de dados não estruturados, atendendo casos de uso como backup, retenção de longo prazo e aplicações nativas de nuvem.

11.12.24. Deverá permitir que os usuários armazenem e gerenciem dados não estruturados em arquitetura de nuvem privada escalável.

11.12.25. A solução deverá permitir a gestão de objetos via interface gráfica de administração e via API REST compatível com S3, mediante autorização prévia do administrador.

11.12.26. Suportar integração com serviços de diretório (Microsoft Active Directory e OpenLDAP), possibilitando o controle de acesso a objetos.

11.12.27. Permitir o compartilhamento de buckets com usuários portadores de chaves de acesso, com delegação de permissões de leitura e escrita conforme o nível definido.

11.12.28. Exibir a listagem de buckets compartilhados, indicando os respectivos usuários com acesso.

11.12.29. Permitir o gerenciamento de buckets e objetos por meio de APIs REST compatíveis com a solução de gerenciamento central ou S3, mediante autorização administrativa.

11.12.30. Suportar o versionamento de múltiplas versões de um mesmo objeto dentro de um bucket.

11.12.31. Possibilitar a definição de regras de ciclo de vida, como exclusão automática de objetos ou versões após período determinado (dias, meses ou anos).

11.12.32. Implementar mecanismo de proteção contra exclusão ou alteração de objetos, com base em políticas de retenção WORM (Write-Once-Read-Many).

11.12.33. Disponibilizar painel de monitoramento de desempenho, apresentando requisições por segundo, taxa de banda (MB/s) e tempo médio de leitura (GET).

11.12.34. Suportar políticas de cotas de utilização, notificando usuários conforme o consumo de espaço ou número de buckets criados.

11.12.35. Suportar o envio de notificações em tempo real — como criação, deleção, leitura, gravação ou alteração de permissões — para fins de auditoria e retenção, compatível com servidores syslog ou sistemas equivalentes.

11.13 ITEM 06 - SOFTWARE DE BACKUP DE DADOS

11.13.1 Características Gerais do Licenciamento:

11.13.1.1 Aquisição de 200 (duzentas) licenças pelo período de 05 (cinco) anos ou 60 (sessenta) meses.

11.13.1.2 Não deverão existir limites quanto ao uso de agentes, conectores, repositórios de armazenamento, hosts físicos e outras tecnologias agregadas a arquitetura da solução especificada.

11.13.1.3 Ser a última versão disponível, não será aceita a utilização de versões anteriores para cobrir algum item desse descritivo técnico.

11.13.1.4 Mostrar na console de gerenciamento a quantidade de licenças adquiridas e utilizadas.

11.13.1.5 Caso a solução ofertada necessite de algum banco de dados, o mesmo deverá ser fornecido devidamente licenciado sem nenhum custo extra.

11.13.1.6 A solução deve ser compatível com o Item 07 Equipamento de Armazenamento de Dados de Backup on-premises.

11.13.2 Cópia e Restauração de Dados:

11.13.2.1 Permitir o controle da banda utilizada durante a operação de cópia de proteção dos backups.

11.13.2.2 Ser capaz de realizar cópia de arquivos abertos sem que a consistência deles seja comprometida.

11.13.2.3 Possuir a opção de priorização de tarefas de proteção com opção de resumo da cópia caso uma atividade de menor prioridade seja colocada em estado de espera por uma tarefa de maior prioridade.

11.13.2.4 Possuir a funcionalidade de paralelizar a gravação dos dados em dispositivos de armazenamento (funcionalidade conhecida como multiplexação).

11.13.2.5 Ser capaz de enviar alertas através de e-mail com o objetivo de reportar eventos ocorridos na operação e configuração da solução.

11.13.2.6 Ser capaz de enviar traps SNMP (Simple Network Management Protocol) com o objetivo de reportar eventos ocorridos na operação da solução.

11.13.2.7 Possuir a funcionalidade de agendamento automático de tarefas de cópia.

11.13.2.8 Para um mesmo dado armazenado deve haver a possibilidade de configuração de diferentes períodos de retenção.

11.13.3 Gerenciamento das Operações de Proteção e Restauração:

11.13.3.1 Possuir interface única, que seja capaz de gerenciar e executar operações de proteção e recuperação dos sistemas operacionais Windows, Unix e Linux; ambiente de virtualização Acropolis Operating System; aplicações, Microsoft Active Directory e banco de dados Microsoft SQL Server, PostgreSQL e Oracle.

11.13.3.2 O acesso administrativo ao console do servidor de gerenciamento da solução poderá ser feito através de ferramenta disponibilizada no próprio software (console gráfico) ou através de navegador Web.

11.13.3.3 Implementar distribuição automática de carga entre os movimentadores de dados, ou seja, os dados oriundos dos clientes de backup deverão ser distribuídos de forma automática entre os servidores de cópia, e em caso de falha de um dos servidores, o cliente automaticamente irá encaminhar seus dados para o outro servidor de cópia ativo. Esta funcionalidade deverá ser nativa do produto, e não pode ser construída com o uso de soluções baseadas em softwares de cluster de terceiros.

11.13.3.4 A base de dados para armazenamento do catálogo deverá possuir mecanismo de proteção (backup) das informações armazenadas no catálogo e funcionalidades de recuperação rápida do catálogo em caso de desastre.

11.13.4 Criptografia dos Dados Protegidos

11.13.4.1 Implementar criptografia de dados na origem (cliente de backup), de uma forma que seja garantido que o dado que trafegará na rede de modo criptografado.

11.13.4.2 Deverá implementar no mínimo chaves de criptografia de 128 bits ou 256 bits.

11.13.5 Desduplicação dos Dados Protegidos

11.13.5.1 Permitir uso da tecnologia de desduplicação de dados para toda a capacidade licenciada, eliminando blocos repetidos, para cópias e arquivamento em disco e movimentação de dados desduplicados, independentemente do quantitativo de dispositivos de armazenamento que compõem a infraestrutura da CONTRATANTE.

11.13.5.2 Implementar desduplicação de blocos na origem (client-side desduplication), de forma que o cliente envie apenas novos blocos de dados criados e/ou modificados a partir da última cópia total completa;

11.13.5.3 Implementar desduplicação de dados nos servidores de armazenamento (target desduplication), de forma que tais servidores tratem adequadamente blocos repetidos enviados pelos clientes, evitando assim o armazenamento de blocos redundantes;

11.13.5.4 Implementar desduplicação de dados em tarefas de cópia;

11.13.5.5 Implementar desduplicação e compressão em uma mesma tarefa;

11.13.5.6 Permitir a restauração granular de arquivos ou sistemas de arquivos a partir de cópias em disco ou fita. Em caso de backup armazenado em disco a recuperação granular poderá ser feito utilizando-se cópias que possam estar desduplicados;

11.13.6 Alertas e Relatórios da Proteção de Dados

11.13.6.1 Quantidade de rotinas de backup concluídos nas últimas 24 horas, nos últimos 30 dias e nos últimos 12 meses.

11.13.6.2 Quantidade de recuperações efetuadas nas últimas 24 horas, nos últimos 30 dias e nos últimos 12 meses.

11.13.6.3 Resumo de rotinas de backup concluídos com sucesso, com erro ou não concluídos.

11.13.6.4 Mostrar o total de licenças adquiridas e o total de licenças utilizadas e caso ocorra uma nova aquisição de licenças as novas licenças deverão constar nesse relatório.

11.13.6.5 Enviar os seguintes alertas via e-mail: rotina de backup finalizada com sucesso, rotina de backup finalizada com erro e rotina de backup com problema.

11.13.7 Fornecimento de licenciamento do Sistema Operacional

11.13.7.1 Fornecimento de licenciamento do sistema operacional Microsoft Windows Server

Datacenter, baseado em núcleo (core-based licensing , para 48 cores físicos).

11.13.7.2 As licenças deverão ser entregues em formato eletrônico, acompanhadas de instruções para instalação e ativação, devendo incluir garantia mínima de 60 (sessenta) meses ou suporte técnico equivalente.

11.13.7.3 O licenciamento deverá ser compatível com servidores físicos e virtuais , observando o licenciamento mínimo exigido pela fabricante.

11.13.7.4 As licenças fornecidas deverão ser originais, legítimas e adquiridas por meio de canal autorizado da Microsoft, com comprovação documental no momento da entrega.

11.13.7.5 As licenças deverão ser entregues em formato eletrônico, acompanhadas de instruções para instalação e ativação, incluindo garantia mínima de 60 (sessenta) meses ou suporte técnico equivalente.

11.13.7.6 O item deverá ser plenamente compatível com a infraestrutura tecnológica do MPAM, em especial com ambientes físicos e virtuais já existentes.

11.13.7.7 Incluir Software Assurance (SA), garantindo direito a atualizações, suporte técnico estendido e benefícios de mobilidade de licenças durante todo o período contratual;

11.14 ITEM 07 - EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES

11.14.1 Características gerais:

11.14.1.1 Deverá corresponder a um sistema inteligente dedicado ao armazenamento de backups em disco, com funcionalidades integradas de criptografia, compressão, desduplicação e replicação dos dados já desduplicados;

11.14.1.2 O equipamento deve estar listado no site oficial do fabricante como um appliance ou sistema de armazenamento de backup em disco, em produção ativa;

11.14.1.3 O hardware e o software devem ser do mesmo fabricante. Não serão aceitas soluções customizadas especificamente para esta licitação, nem combinações OEM, equipamentos usados, recondicionados, de demonstração ou gateways;

11.14.1.4 O equipamento deve ser novo, sem uso anterior, pertencente à linha mais recente do fabricante, em produção contínua e sem previsão de fim de suporte (EOSL) nos próximos cinco anos a partir da data de abertura da licitação;

11.14.1.5 Soluções baseadas exclusivamente em software (appliances virtuais) não serão aceitas;

11.14.1.6 Deve ser compatível com montagem em racks padrão de 19”, acompanhado de trilhos, cabos, conectores, manuais e todos os itens necessários para instalação, configuração e operação completa;

11.14.1.7 Para soluções com arquitetura Scale-Out:

11.14.1.7.1 Deve permitir conexão com outros sistemas do mesmo fabricante para expansão de desempenho e capacidade;

11.14.1.7.2 Deve operar em modo ativo-ativo (alta disponibilidade com balanceamento de carga), redirecionando automaticamente os backups em caso de falha de um dos sistemas;

11.14.1.8 Para soluções com arquitetura Scale-Up:

11.14.1.8.1 Deve incluir duas controladoras, operando em modo ativo-ativo ou ativo-passivo, garantindo continuidade das operações de backup em caso de falha de uma das controladoras.

11.14.2 Requisitos de disponibilidade:

11.14.2.1 Deve possuir tolerância a falhas em componentes como discos, fontes de alimentação e ventiladores;

11.14.2.2 Deve contar com mecanismos que assegurem a integridade dos dados mesmo em casos de interrupção abrupta ou desligamento acidental;

11.14.2.3 Deve incluir proteção de cache de escrita para evitar perda de dados em caso de falha de energia;

11.14.2.4 Deve ser entregue com arranjos RAID-6, RAID-DP ou equivalente, com tolerância a falha de até dois discos e pelo menos um disco hot-spare por grupo RAID;

11.14.2.5 Os discos devem ser hot-pluggable e hot-swappable, permitindo substituição sem interrupção do sistema;

11.14.2.6 Deve oferecer monitoramento remoto pelo fabricante, com recursos como Call-Home para detecção proativa de falhas ou pré-falhas.

11.14.3 - Capacidade, desempenho e conectividade:

11.14.3.1 Deve oferecer no mínimo 100 TB (cem terabytes) úteis, sem considerar compressão, desduplicação ou espaço reservado ao sistema;

11.14.4 Para soluções Scale-Out:

11.14.4.1 Deve atingir taxa mínima de 5 TB/hora (cinco terabytes por hora) para operações de backups, sem considerar desduplicação;

11.14.4.2 Capacidade de ampliar a solução previamente fornecida, através da interconexão de módulos similares ou não, do mesmo fabricante. Para a expansão, volumes em nuvem, off-site, replicação ou similar para o atendimento a este requisito não serão aceitos, mantendo a característica de desduplicação global da solução.

11.14.4.3 A criptografia deve ser feita via hardware. Caso seja por software, a taxa de transferência deve ser 30% superior à mínima exigida, considerando apenas a desduplicação.

11.14.5 Para soluções Scale-Up:

11.14.5.1 Deve permitir expansão para pelo menos 500 TB (quinhentos terabytes) de capacidade útil, sem considerar compressão ou desduplicação, por meio de gavetas de discos, sem troca ou upgrade das controladoras originais, mantendo a desduplicação global;

11.14.5.2 Deve atingir taxa mínima de 15 TB/hora (quinze terabytes por hora) para operações de backup, considerando apenas a desduplicação;

11.14.5.3 A criptografia deve ser realizada por hardware. Se for por software, a taxa de transferência deve ser 30% superior à exigida, considerando apenas a desduplicação;

11.14.5.4 Deve incluir no mínimo duas interfaces de rede de 25 Gbps com conectores SFP28 para backup via LAN, fornecidos com o equipamento;

11.14.5.5 Deve incluir pelo menos duas interfaces de 1 GbE com conectores UTP CAT6 para gerenciamento, também fornecidos;

11.14.5.6 Deve possuir ao menos uma porta IPMI/iLO/iDRAC ou equivalente;

11.14.5.7 Interfaces adicionais devem ser fornecidas conforme as melhores práticas do fabricante para garantir o desempenho requerido;

11.14.5.8 Fornecer a quantidade necessária de discos para atingimento da performance mínima solicitada, ou seja, se a solução requerer mais discos além dos necessários para atender a capacidade solicitada no item 8.3.1, discos adicionais deverão ser fornecidos. Não é obrigatório o licenciamento de capacidade desses discos adicionais

11.14.5.9 Comprovar a taxa de transferência através da ferramenta de dimensionamento do fabricante da solução, desconsiderando o uso de ferramentas/protocolos de otimizações na origem no seu dimensionamento, caso a solução ofertada não seja fornecida com todos os discos possíveis para sua capacidade total.

11.15 ITEM 08 - SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES

11.15.1 Características gerais

11.15.1.1 Permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, de maneira perpétua, irrestrita e sem necessidade de licenciamentos ou ônus adicionais;

11.15.1.2 -Possuir licenças na modalidade de uso perpétuo para todo para o completo atendimento das especificações técnicas do equipamento, ou seja, o equipamento deverá continuar a operar normalmente mesmo após o período de manutenção e assistência técnica contratado;

11.15.1.3 Para soluções com arquitetura Scale-Out:

11.15.1.3.1 A desduplicação de dados deve ser mantida de forma global em todo o ambiente de armazenamento, independentemente da quantidade de dispositivos interligados;

11.15.1.4 Para soluções com arquitetura Scale-Up:

11.15.1.4.1 A desduplicação global deve ser preservada em todo o conjunto de armazenamento.

11.15.2 Requisitos de compatibilidade:

11.15.2.1 O software deve ser homologado e plenamente compatível com o com o software de backup fornecido no ITEM 06 - SOFTWARE DE BACKUP DE DADOS;

11.15.2.2 Deve permitir leitura e gravação simultâneas via protocolos CIFS, NFS e OST;

11.15.2.3 Deve oferecer suporte aos protocolos de monitoramento SNMP e Syslog;

11.15.2.4 Deve possibilitar que aplicações como Oracle (via RMAN) e Microsoft SQL realizem backups tipo Stream Based (Oracle Stream Backup) e “database dump” diretamente no equipamento, por meio de CIFS e NFS, sem uso de software de backup, evitando o consumo de licenças e sem necessidade de licenciamento por volume (TB) ou por servidor (CPU, Core, Tier). Caso essa funcionalidade exija licenciamento, todos os itens necessários devem ser incluídos na proposta.

11.15.3 - Funcionalidades operacionais:

11.15.3.1 Deve permitir a execução simultânea de processos de backup e restore;

11.15.3.2 Deve dispor de interface de gerenciamento baseada em navegador (WEB);

11.15.3.3 A desduplicação deve ser global, mesmo com volumes lógicos distintos, identificando dados redundantes entre diferentes fontes de backup e armazenando-os apenas uma vez;

11.15.3.4 A desduplicação deve ocorrer em conjunto com os processos de backup e restore, sem necessidade de janelas específicas;

11.15.3.5 Deve incluir mecanismos nativos para verificação da integridade dos dados desduplicados, com capacidade de correção automática em caso de inconsistência, sem uso de scripts externos;

11.15.3.6 Deve permitir replicação de dados via rede IP (LAN/WAN), de forma assíncrona, entre sistemas compatíveis do mesmo fabricante, utilizando desduplicação para otimizar o uso da banda;

11.15.3.7 Deve suportar topologias de replicação como 1:1, 1:N, N:1 e o cascateamento de equipamentos;

11.15.3.8 Deve integrar-se ao Microsoft Active Directory 2012 ou superior, para autenticação e controle de acesso;

11.15.3.9 Os dados armazenados devem ser criptografados com algoritmos de no mínimo AES128-SHA ou AES256-SHA;

11.15.3.10 Deve permitir autenticação em dois fatores (2FA), com integração a soluções OTP como Google Authenticator, Microsoft Authenticator ou equivalentes;

11.15.3.11 Caso a solução exija um sistema OTP específico com licenciamento ou hardware dedicado (ex: Common Access Card /Personal Information Verification cards, sistemas de OTP/tokenização licenciados, etc), todos os componentes necessários devem ser fornecidos para pelo menos 5 usuários;

11.15.3.12 Deve oferecer recurso de autorização dupla (Dual Auth) para alterações em configurações de proteção contra ransomware;

11.15.3.13 Deve incluir funcionalidades avançadas de segurança cibernética para proteção contra ransomware, assegurando a integridade dos dados de backup;

11.15.4 Deve possuir mecanismo de imutabilidade dos dados:

11.15.4.1 A proteção deve estar sempre ativa, independente do software de backup, sem necessidade de janelas específicas ou scripts;

11.15.4.2 A proteção deve ser aplicada imediatamente após a desduplicação dos dados, sem depender de agendamento;

11.15.4.3 Deve adotar o conceito de air-gap, tornando os dados protegidos invisíveis à rede e inacessíveis por softwares de backup, independentemente do protocolo utilizado.

11.16 ITEM 09 – SWITCH CORE

11.16.1 Especificações Físicas

11.16.1.1 O equipamento deve contar com, no mínimo, 48 portas SFP28 compatíveis com velocidades de 1, 10 e 25 Gigabit Ethernet.

11.16.1.2 As interfaces devem ser auto-sensíveis, ajustando automaticamente a velocidade conforme o transceiver conectado, sem necessidade de configuração manual.

11.16.1.3 A altura máxima permitida é de 1 unidade de rack (1 RU).

11.16.1.4 Deve ser compatível com racks padrão de 19 polegadas, incluindo os kits de fixação apropriados.

11.16.1.5 As portas SFP28 devem aceitar transceivers dos tipos SFP+ 10GBase-SR, 10GBase-LR, 10GBase-ER, SFP 1000Base-SX, 1000Base-LX, 1000Base-ZX, 1000Base-T e cabos DAC.

11.16.1.6 Devem ser entregues ao menos 10 cabos DAC 25GbE SFP28 com comprimento mínimo de 3 metros, compatíveis com os appliances do item 1.

11.16.1.7 O switch deve possuir pelo menos 6 portas QSFP28 de 100GbE, com suporte a velocidades de 40GbE.

11.16.1.7.1 Deve ser compatível com transceivers 40GBase-SR4 e 40GBase-LR4.

11.16.1.7.2 Deve aceitar transceivers 100GBase-SR4 e 100GBase-LR4.

11.16.1.7.3 Deve suportar cabos DAC.

11.16.1.8 Deve acompanhar pelo menos 1 cabo DAC 100GbE com no mínimo 1 metro de comprimento, para conexão redundante entre switches.

11.16.1.9 A capacidade da matriz de comutação deve ser de no mínimo 4 Tbps.

11.16.1.10 O throughput mínimo exigido é de 1,5 Bpps.

11.16.1.11 O buffer deve ter capacidade mínima de 32 MB.

11.16.1.12 A latência máxima permitida é de 900 nanosegundos.

11.16.1.13 Deve suportar ao menos 160.000 endereços MAC.

11.16.1.14 A tabela ARP deve comportar até 64.000 entradas ou mais.

11.16.1.15 Deve aceitar jumbo frames com tamanho mínimo de 9000 bytes.

11.16.1.16 É obrigatória a presença de pelo menos uma porta RJ-45 para gerenciamento fora de banda.

11.16.1.17 O equipamento deve vir com CPU e memória (RAM e Flash) suficientes para suportar todas as funcionalidades descritas.

11.16.1.18 Fontes de alimentação internas devem ser redundantes e com ajuste automático para 110/220V.

11.16.1.19 O sistema de ventilação deve ser redundante, com fluxo de ar configurável (frontal-traseiro ou traseiro-frontal), sendo fornecido com ventiladores de fluxo frontal-traseiro.

11.16.1.20 Fontes e ventiladores devem ser hot-swappable e redundantes, permitindo substituição sem interrupção.

11.16.1.21 O equipamento deve ser projetado para ambientes de datacenter, com comutação de pacotes de alto desempenho.

11.16.2 - Funcionalidades Gerais

11.16.2.1 LEDs por porta devem indicar status e atividade do link.

11.16.2.2 A arquitetura da solução deve ser baseada em “spine-leaf”, com VxLAN como plano de dados e BGP EVPN como plano de controle.

11.16.2.3 Deve possuir porta de console para configuração via CLI, com conector RJ-45 ou RS-232, incluindo cabos e adaptadores necessários.

11.16.2.4 Gerenciamento via SSHv2 deve ser suportado.

11.16.2.5 O switch deve ter criptografia FIPS 140-2 validada pelo NIST.

11.16.2.6 Deve permitir espelhamento de uma ou mais portas para outra porta específica.

11.16.2.7 Também deve permitir espelhamento para porta remota via tunelamento, mesmo em domínios L2 distintos.

11.16.2.8 Deve implementar Netflow, sFlow ou tecnologia equivalente.

11.16.2.9 Gerenciamento via SNMPv3 deve ser possível.

11.16.2.10 Deve suportar o protocolo Syslog.

11.16.2.11 Deve implementar NTPv4 ou SNTP.

11.16.2.12 Autenticação via RADIUS deve ser suportada.

11.16.2.13 Autenticação via TACACS+ também deve ser suportada.

11.16.2.14 Controle de acesso por porta (IEEE 802.1x) deve estar presente.

11.16.2.15 Deve haver controle de broadcast, multicast e unicast por porta.

11.16.2.16 Deve implementar pelo menos uma fila de saída com prioridade estrita (SP Strict Priority) e divisão de banda ponderada (WRED, WRR ou similar).

11.16.2.17 Deve classificar, marcar e priorizar tráfego com base em IEEE 802.1p CoS.

11.16.2.18 Deve classificar, marcar e priorizar tráfego com base em DSCP (Differentiated Services CodePoint), conforme IETF.

11.16.2.19 Deve permitir classificação de tráfego por IP, portas TCP/UDP e endereços MAC.

11.16.3 - Virtualização de Switch

11.16.3.1 Deve permitir agregação de portas multi-chassi com redundância ativa/ativa sem Spanning Tree, usando MLAG, MC-LAG, M-LAG, VLT (Virtual Link Trunking), Multi-Chassis EtherChannel ou equivalentes.

11.16.3.2 Todos os componentes necessários para alta disponibilidade devem ser fornecidos, incluindo cabos, transceivers e licenças.

11.16.3.3 Em modo virtualizado, os switches devem operar com processamento local, sem tempo de convergência em caso de falha.

11.16.4 - Funcionalidades de Camada 2

11.16.4.1 Suporte a até 4.000 VLANs conforme IEEE 802.1Q.

11.16.4.2 Implementação de VLAN Trunking conforme IEEE 802.1Q, com controle de VLANs

permitidas por tronco.

11.16.4.3 Suporte a Link Aggregation (LAG) conforme IEEE 802.3ad.

11.16.4.4 Deve suportar no mínimo 80 grupos LAG com até 16 portas cada.

11.16.4.5 Implementação dos padrões IEEE 802.1d, 802.1s e 802.1w.

11.16.4.6 Deve possuir mecanismo de proteção da root bridge do Spanning Tree.

11.16.4.7 Deve permitir bloqueio de BPDUs em portas em modo fast forwarding, com desativação automática ao recebê-los.

11.16.4.8 Implementação de LLDP e LLDP-MED para descoberta de vizinhos.

11.16.4.9 Suporte a DCB com PFC (IEEE 802.1Qbb), ETS (IEEE 802.1Qaz) e DCBx.

11.16.5 - Funcionalidades de Roteamento

11.16.5.1 Deve realizar roteamento de camada 3 entre VLANs.

11.16.5.2 Suporte ao protocolo OSPFv3.

11.16.5.3 Suporte ao protocolo BGPv4.

11.16.5.4 Capacidade para no mínimo 106.000 rotas IPv4.

11.16.5.5 Capacidade para no mínimo 52.000 rotas IPv6.

11.16.5.6 Operação simultânea com IPv4 e IPv6.

11.16.5.7 Implementação de VRF ou VRF-Light.

11.16.5.8 Suporte a roteamento baseado em políticas (PBR).

11.16.5.9 Implementação do protocolo VRRPv3.

11.17 IMPLANTAÇÃO DA SOLUÇÃO E SERVIÇOS CORRELATOS

11.17.1 A CONTRATADA será responsável por toda a instalação e configuração dos equipamentos, firmwares e softwares, incluindo o fornecimento de quaisquer itens adicionais necessários à sua execução.

11.17.2 A instalação poderá ser realizada integral ou parcialmente pelo fabricante, devendo a CONTRATADA prever esses serviços em sua proposta.

11.17.3 A CONTRATADA deverá disponibilizar técnicos certificados pelo fabricante, habilitados a instalar, operar e configurar os equipamentos fornecidos. Caso a instalação seja conduzida diretamente pelo fabricante, essa exigência estará dispensada.

11.17.4 A CONTRATANTE reserva-se o direito de solicitar a substituição parcial ou total da equipe da CONTRATADA durante a fase de implantação, caso seja constatada a ausência de qualificação técnica adequada.

11.17.5 Deverá ser apresentado cronograma de implantação e proposta de configuração da solução, ambos sujeitos à aprovação da equipe técnica da CONTRATANTE.

11.17.6 Ao final da instalação, deverão ser entregues, em meio digital, os manuais e procedimentos utilizados.

11.17.7 A instalação deverá incluir, no mínimo:

a) Fixação dos equipamentos em rack padrão 19”;

b) Conectorização elétrica e energização dos equipamentos;

c) Atualização de firmwares de todos os componentes (BIOS, Gerência Out of Band, controladoras HBA, interfaces de rede, discos, etc.);

d) Atualizações e releases disponíveis no site oficial;

e) Registro dos equipamentos e licenças no portal do fabricante.

f) Conectorização das interfaces de rede com os respectivos cabos/conectores;

g) Instalação, atualização e configuração dos componentes conforme boas práticas;

h) Integração dos equipamentos à rede do CONTRATANTE;

i) Outras atividades correlatas para garantir a operação da solução no ambiente da CONTRATANTE.

11.17.8 A aceitação dos itens do objeto contratado no ato da sua entrega ao Ministério Público do Estado do Amazonas será considerada como de caráter provisório. A aceitação definitiva dar-se-á após a instalação e configuração dos itens do objeto e a verificação do atendimento às especificações técnicas constantes deste Termo de Referência.

11.17.9 Serão recusados os objetos imprestáveis ou defeituosos, que não atendam as especificações constantes neste termo de referência e/ou que não estejam adequados para uso.

11.17.10 Os itens deverão ser instalados, configurados e ativados pela CONTRATADA em local indicado

pelo DTIC do MPAM.

11.17.11 O prazo para conclusão da instalação e configuração dos equipamentos e softwares será de até 30 (trinta) dias, contados a partir da data do recebimento provisório dos mesmos pela DTIC e emissão do termo provisório de recebimento.

11.17.12 Os equipamentos e serviços serão aceitos se, e somente se, houver comprovação de que todos os requisitos técnicos especificados neste Termo de Referência tenham sido atendidos e os itens se encontre em operação plena. Essa comprovação será feita mediante observação direta das características dos equipamentos, consulta à documentação técnica fornecida e verificação dos serviços de instalação e configurações.

11.17.13 Os serviços de instalação, configuração, migração e transferência de conhecimento técnico deverão ser realizados conforme especificado em cada item.

11.17.14 O serviço de instalação e configuração tem a finalidade de garantir que os itens fornecidos estejam operacionais no ambiente de Produção, e de Contingência caso exista.

11.17.15 Todos os serviços de instalação, configuração, migração e transferência de conhecimento técnico deverão ser executados de forma presencial, por especialista(s) técnico(s) certificado(s) nos componentes pelo fabricante dos mesmos com a devida apresentação de certificado(s) técnico(s) emitido(s) pelo fabricante do(s) produto(s).

11.17.16 Os serviços de instalação, configuração, migração e transferência de conhecimento técnico, deverão ser agendados previamente entre as partes, através de e-mail ou telefone, e deverão ser realizados em dias úteis e em horário de expediente do MPAM.

11.17.17 A transferência de conhecimento técnico será feita através de treinamento referente aos componentes do objeto deste Termo de Referência, abrangendo todos os recursos de hardware e software do ambiente, para até 10 (dez) técnicos designados pela CONTRATANTE, cobrindo no mínimo os seguintes tópicos:

a) Instalação.

b) Configuração básica e avançada.

c) Operação básica e avançada.

d) Gerenciamento da solução/expansão.

e) Administração.

f) Solução de problemas (troubleshouting).

g) Laboratório prático baseado na solução/expansão adquirida.

11.17.18 O treinamento deverá ser realizado nas seguintes condições:

a) Deverá ser ministrado em língua portuguesa do Brasil, de forma presencial;

b) Local: Av. Coronel Teixeira, nº 7.995, Nova Esperança II, CEP. 69037-473, Manaus-AM;

c) Carga horária mínima de 30 (trinta) horas, divididas em, no máximo, 4 (quatro) horas diárias;

d) O conteúdo programático deverá ser aprovado pela DTIC antes da realização de cada treinamento.

11.17.19 O material didático e os certificados deverão ser disponibilizados pela CONTRATADA com finalidade específica para ministrar o treinamento à DTIC.

11.17.20 Ao final do treinamento, os participantes deverão estar aptos a operar e administrar as tecnologias referenciadas neste Termo de Referência.

11.17.21 A transferência de conhecimento técnico deverá ocorrer no período correspondente ao recebimento definitivo da expansão, ou em caso de impedimento justificado, em nova data aceita pela fiscalização do contrato.

11.17.22 Caberá ainda a CONTRATADA a execução de todas as atividades, bem como o fornecimento de todos os materiais necessários e suficientes para a instalação e configuração dos equipamentos fornecidos.

11.17.24 O planejamento, instalação, configuração e migração dos equipamentos deverão ser executados por técnicos habilitados e credenciados pelo fabricante.

11.17.25 A CONTRATADA deverá designar um profissional Técnico Responsável para acompanhar a execução dos serviços desde o planejamento até a implantação da expansão.

11.17.26 Antes da implantação dos equipamentos, a equipe técnica da CONTRATADA deverá apresentar o cronograma da implantação contendo: o plano de instalação, plano de contingência e prazos máximos para a realização da mudança.

11.17.27 A CONTRATADA deverá realizar a migração completa do ambiente computacional atualmente em operação para a nova infraestrutura fornecida, incluindo, mas não se limitando a: máquinas virtuais, clusters Kubernetes, bancos de dados, configurações nativas, políticas de segurança, integrações existentes e demais componentes necessários para garantir a continuidade dos serviços. A migração

deverá ser executada de forma planejada, segura e sem impacto significativo na disponibilidade dos sistemas, observando as melhores práticas recomendadas pelo fabricante e garantindo a integridade dos dados e das aplicações.

11.17.28 A CONTRATADA deverá prover PDU´s ou réguas smart adequadas para a devida conecção elétrica necessária dos equipamentos específicados neste Termo de Referência.

11.17.29 Após a conclusão das atividades de instalação, configuração, migração e pré-operação, deve ser iniciada a fase de operação assistida do objeto contratado.

11.17.30 A operação assistida terá duração total de 90 (noventa) dias corridos, sendo 15 (dias) dias corridos de forma presencial, e o restante do período podendo ser de forma remota, de modo a assegurar o auxílio e pronta ação corretiva da CONTRATADA necessária em questões relacionadas com a configuração, monitoramento e estabilização da nova solução com o objetivo de garantir o bom funcionamento dos equipamentos e serviços.

11.17.31 Durante a fase de operação assistida, a CONTRATADA deverá atuar de maneira a mitigar os riscos decorrentes da transição tecnológica da plataforma atualmente existente para a nova solução.

11.17.32 As atividades de operação assistida devem ser realizadas somente nas dependências da sede do MPAM em Manaus-AM, em horário de expediente da Procuradoria-Geral, e devem se iniciar logo após a migração tecnológica, testes e ativação dos serviços. Caso seja necessária a consecução de atividades que possam afetar a disponibilidade dos serviços, as atividades de operação assistida podem ser prolongadas após o horário de expediente da Procuradoria-Geral, sem qualquer ônus para o MPAM.

11.17.33 O período de operação assistida deve englobar, dentre outras, as seguintes atividades:

a) Monitoramento de funcionamento e da capacidade dos serviços;

b) Identificação e abertura de chamados técnicos para solução de falhas na solução;

c) Resolução de problemas (troubleshooting);

d) Análise da efetividade de regras e configurações;

e) Simulação de abertura de chamados;

f) Instalação de patches;

g) Execução/revisão de procedimentos de backup e restore de configurações;

h) Geração de relatórios técnicos, administrativos e gerenciais;

12. GARANTIA TÉCNICA

12.1 Todos os equipamentos e softwares utilizados na fornecimento do objeto deverão estar cobertos por suporte, garantia e assistência técnica do fabricante, durante toda a vigência do contrato.

12.2 A garantia dos hardwares deverá ser na modalidade on-site no Datacenter da CONTRATANTE.

12.3 A CONTRATADA é a única responsável pelos equipamentos e softwares disponibilizados na prestação dos serviços fornecidos ao CONTRATANTE, mesmo que tenham sido adquiridos de terceiros.

12.4 A CONTRATADA responderá pela reparação dos danos causados por defeitos relativos ao serviço prestado, conforme descrição e exigências deste Termo. Por isso, deve prezar pela qualidade e eficiência, garantindo que o serviço e as soluções definitivas fornecidas não causem problemas adicionais àqueles apresentados pelo CONTRATANTE, quando do recebimento de alertas ou da abertura dos chamados de suporte técnico.

12.5 Serviços de Suporte Técnico e Manutenção:

12.5.1 Os equipamentos deverão possuir garantia de 60 (sessenta) meses, com suporte 24x7 e prazo de envio de peças até o próximo dia útil após abertura do chamado.

12.5.2 -O CONTRATANTE poderá acionar diretamente o suporte do fabricante, sem necessidade de autorização prévia da CONTRATADA. Não haverá limitação quanto à quantidade de chamados, seja para dúvidas, configurações ou problemas relacionados a hardware e software.

12.5.3 - Chamados poderão ser abertos via telefone 0800, portal web ou e-mail.

12.5.4 - O atendimento telefônico inicial deverá ser realizado em português.

12.5.5 - A contratada deverá garantir acesso completo ao portal do fabricante, incluindo base de conhecimento, atualizações de software e documentação.

12.5.7 - Durante a vigência do suporte, todas as atualizações de firmware e software deverão ser fornecidas sem ônus à CONTRATANTE.

12.5.8 - A contratada deverá apresentar os códigos de serviço (SKU, part number) referentes à garantia do fabricante, com os equipamentos devidamente registrados em nome da contratante.

12.5.9 - É de responsabilidade da contratada garantir a compatibilidade técnica entre todos os componentes da solução durante toda a vigência contratual.

13. DA ELABORAÇÃO

O presente Termo de Referência foi elaborado pela **DIRETORIA DE TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO**, em conformidade com as atribuições legais e regimentais, estando em consonância com as disposições legais e normativas aplicáveis, com a necessidade, interesse e conveniência da Administração, sendo parte integrante do procedimento interno respectivo.

14. DECLARAÇÃO DO SOLICITANTE

Declaro que este Termo de Referência está de acordo com a Lei nº 14.133/2021 e alterações.

ANTOVILA FROTA BEZERRA JUNIOR
Técnico em Computação

CARLOS ALEXANDRE DOS SANTOS NOGUEIRA
Chefe do Setor de Infraestrutura e Telecomunicações

15. APROVAÇÃO

Solicitamos aprovação do presente Termo de Referência tendo em vista que o mesmo foi elaborado de forma conveniente e oportuna para atender à demanda do Ministério Público do Estado do Amazonas.

EUDO LIMA DE ASSIS JUNIOR
Diretor de Tecnologia da Informação e Comunicação

Documento assinado eletronicamente por **Carlos Alexandre dos Santos Nogueira**, **Chefe do Setor de Infraestrutura e Telecomunicação - SIET**, em 14/11/2025, às 17:00, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Antovila Frota Bezerra Junior**, **Requisitado**, em 14/11/2025, às 17:01, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Eudo de Lima Assis Júnior**, **Diretor de Tecnologia da Informação e Comunicação (DTIC)**, em 16/11/2025, às 22:31, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2002143** e o código CRC **699016BF**.

DESPACHO Nº 1123.2025.01AJ-SUBADM.2013504.2025.007562

PROCESSO N.º: 2025.007562

ASSUNTO: Contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais do Ministério Público do Estado do Amazonas (MPAM).

INTERESSADO: Diretoria de Tecnologia de Informação e Comunicação (DTIC)

I. DO RELATÓRIO

Trata-se do **Ofício n.º 94.2025.DTIC (1666988)**, de lavra do Ilmo. **Sr. Eudo de Lima Assis Júnior**, **Diretor de Tecnologia de Informação e Comunicação (DTIC)**, por onde são encaminhados o **Estudo Técnico Preliminar (ETP) n.º 7.2025.DTIC (1591885)** e o **Termo de Referência n.º 9.2025.DTIC (1605182),** que tem por objeto a contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup para atender as necessidades institucionais do Ministério Público do Estado do Amazonas (MPAM), **com vigência de 60 (sessenta) meses**.

Após decisão exarada no **Despacho 1018 (1991573)**, de **não solicitar a prorrogação do prazo** para efetivação da adesão à Ata de Registro de Preços nº 19/2025/SEJUSP-DIVCL, objeto do presente processo, e, consequentemente autorizar o prosseguimento da contratação por meio de processo licitatório regular, retornam os autos por meio do Ofício 298 (2009577), por onde a DTIC **submeteu** à aprovação, o Termo de Referência Nº 28.2025.DTIC (2002143) **revisado.**

É o relatório. Decido.

II. DOS FUNDAMENTOS

Cumpre destacar que de acordo com o **art. 6º, inciso XXIII**, da Lei 14.133/2021, o Termo de Referência é o documento necessário para a contratação de bens e serviços.

Nesse contexto, após análise sumária dos elementos constantes no **Termo de Referência n.º 28 (2002143),** bem como dos demais documentos que integram o presente processo, verifica-se, em princípio, o atendimento aos requisitos necessários ao prosseguimento do procedimento de contratação.

Contudo, observa-se que o referido artefato sofreu alteração nos quantitativos estimados, especificamente no **item 11. Especificações Técnicas do Objeto**. Diante disso, faz-se necessário o retorno dos autos ao Setor de Compras e Serviços, a fim de que seja procedida a revisão da pesquisa de preços, garantindo-se a conformidade e a adequação dos valores estimados.

III. DA CONCLUSÃO

Por todo o exposto, com fundamento no art. 26, § 2º, da Lei Complementar nº 011, de 17 de dezembro de 1993, e no art. 4º do Ato nº 076/2013-PGJ, **considerando que o novo Termo de Referência n.º 28 (2002143) atende às exigências legais e regulamentares**, **aprovo** o prosseguimento do procedimento, determinando o **encaminhamento dos autos ao Setor de Compras e Serviços** para que seja revisada a pesquisa de preços, nos termos do art. 23 da Lei nº 14.133/2021, **com vistas à realização do procedimento licitatório**.

Após, sigam os autos as demais unidades do fluxo de contratação.

Cumpra-se.

GABINETE DA SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, Manaus (AM), *data da assinatura eletrônica.*

ANDRÉ VIRGÍLIO BELOTA SEFFAIR

Subprocurador-Geral de Justiça para Assuntos Administrativos

Documento assinado eletronicamente por **André Virgílio Belota Seffair**, **Subprocurador(a)-Geral de Justiça para Assuntos Administrativos**, em 24/11/2025, às 15:54, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2013504** e o código CRC **B5D9E605**.

Departamento: **Setor de Compras e Serviços**

Relatório de Cotação: Plataforma Nutanix

Pesquisa realizada entre 25/11/2025 10:07:54 e 26/11/2025 09:41:11

Relatório gerado no dia 05/12/2025 09:58:48 (IP: 179.48.97.222)

Em conformidade com a Instrução Normativa Nº 65 de 07 de Julho de 2021 (Lei nº 14.133).

Método Matemático Aplicado: Média Aritmética dos preços obtidos - Preço calculado com base na média aritmética de todos os preços selecionados pelo usuário para aquele determinado Item.

Conforme Instrução Normativa Nº 65 de 07 de Julho de 2021 (Lei nº 14.133), no Artigo 3º, "A pesquisa de preços será materializada em documento que conterá: INC V-Método matemático aplicado para a definição do valor estimado."

Item 1: EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9

PREÇOS / PROPOSTAS	QUANTIDADE	PREÇO ESTIMADO	PERCENTUAL	PREÇO EST. CALCULADO	% VALOR GLOBAL	TOTAL
0 / 0	1	R$ 0,00 (un)	-	R$ 0,00	0%	R$ 0,00

Mediana dos Preços Obtidos: R$ 0,00 | Média dos Preços Obtidos: R$ 0,00

Item 2: EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU

PREÇOS / PROPOSTAS	QUANTIDADE	PREÇO ESTIMADO	PERCENTUAL	PREÇO EST. CALCULADO	% VALOR GLOBAL	TOTAL
0 / 0	1	R$ 0,00 (un)	-	R$ 0,00	0%	R$ 0,00

Mediana dos Preços Obtidos: R$ 0,00 | Média dos Preços Obtidos: R$ 0,00

Item 3: SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA

PREÇOS / PROPOSTAS	QUANTIDADE	PREÇO ESTIMADO	PERCENTUAL	PREÇO EST. CALCULADO	% VALOR GLOBAL	TOTAL
0 / 0	1	R$ 0,00 (un)	-	R$ 0,00	0%	R$ 0,00

Mediana dos Preços Obtidos: R$ 0,00 | Média dos Preços Obtidos: R$ 0,00

Item 4: SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU

PREÇOS / PROPOSTAS	QUANTIDADE	PREÇO ESTIMADO	PERCENTUAL	PREÇO EST. CALCULADO	% VALOR GLOBAL	TOTAL
0 / 0	1	R$ 0,00 (un)	-	R$ 0,00	0%	R$ 0,00

Mediana dos Preços Obtidos: R$ 0,00 | Média dos Preços Obtidos: R$ 0,00

Item 5: LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE

PREÇOS / PROPOSTAS	QUANTIDADE	PREÇO ESTIMADO	PERCENTUAL	PREÇO EST. CALCULADO	% VALOR GLOBAL	TOTAL
0 / 0	1	R$ 0,00 (un)	-	R$ 0,00	0%	R$ 0,00

Mediana dos Preços Obtidos: R$ 0,00 | Média dos Preços Obtidos: R$ 0,00

Item 6: SOFTWARE DE BACKUP DE DADOS

PREÇOS / PROPOSTAS	QUANTIDADE	PREÇO ESTIMADO	PERCENTUAL	PREÇO EST. CALCULADO	% VALOR GLOBAL	TOTAL
0 / 0	1	R$ 0,00 (un)	-	R$ 0,00	0%	R$ 0,00

Mediana dos Preços Obtidos: R$ 0,00 | Média dos Preços Obtidos: R$ 0,00

Item 7: EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES

PREÇOS / PROPOSTAS	QUANTIDADE	PREÇO ESTIMADO	PERCENTUAL	PREÇO EST. CALCULADO	% VALOR GLOBAL	TOTAL
0 / 0	1	R$ 0,00 (un)	-	R$ 0,00	0%	R$ 0,00

Mediana dos Preços Obtidos: R$ 0,00 | Média dos Preços Obtidos: R$ 0,00

Item 8: SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES

PREÇOS / PROPOSTAS	QUANTIDADE	PREÇO ESTIMADO	PERCENTUAL	PREÇO EST. CALCULADO	% VALOR GLOBAL	TOTAL
0 / 0	1	R$ 0,00 (un)	-	R$ 0,00	0%	R$ 0,00

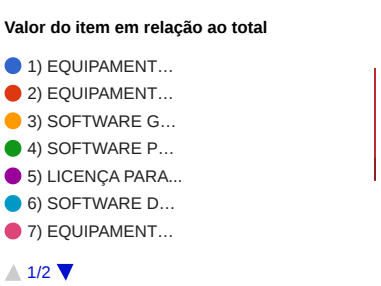
Mediana dos Preços Obtidos: R$ 0,00 | Média dos Preços Obtidos: R$ 0,00

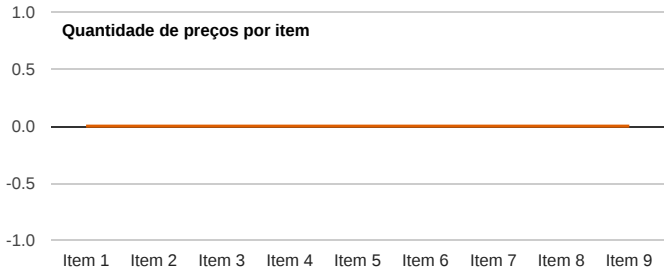
Item 9: SWITCH CORE

PREÇOS / PROPOSTAS	QUANTIDADE	PREÇO ESTIMADO	PERCENTUAL	PREÇO EST. CALCULADO	% VALOR GLOBAL	TOTAL
0 / 0	1	R$ 0,00 (un)	-	R$ 0,00	0%	R$ 0,00

Mediana dos Preços Obtidos: R$ 0,00 | Média dos Preços Obtidos: R$ 0,00

Valor Global: R$ 0,00





Detalhamento dos Itens

Item 1: EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9

Preço Estimado: R$ 0,00 (un) **Percentual:** - **Preço Estimado Calculado:** R$ 0,00 **Média dos Preços Obtidos:** R$ 0,00

Quantidade	Descrição	Observação
1 Unidade	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9	

Item 2: EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU

Preço Estimado: R$ 0,00 (un) **Percentual:** - **Preço Estimado Calculado:** R$ 0,00 **Média dos Preços Obtidos:** R$ 0,00

Quantidade	Descrição	Observação
1 Unidade	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU	

Item 3: SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA

Preço Estimado: R$ 0,00 (un) **Percentual:** - **Preço Estimado Calculado:** R$ 0,00 **Média dos Preços Obtidos:** R$ 0,00

Quantidade	Descrição	Observação
1 Unidade	SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA	

Item 4: SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU

Preço Estimado: R$ 0,00 (un) **Percentual:** - **Preço Estimado Calculado:** R$ 0,00 **Média dos Preços Obtidos:** R$ 0,00

Quantidade	Descrição	Observação
1 Unidade	SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU	

Item 5: LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE

Preço Estimado: R$ 0,00 (un) **Percentual:** - **Preço Estimado Calculado:** R$ 0,00 **Média dos Preços Obtidos:** R$ 0,00

Quantidade	Descrição	Observação
1 Unidade	LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE	

Item 6: SOFTWARE DE BACKUP DE DADOS

Preço Estimado: R$ 0,00 (un) **Percentual:** - **Preço Estimado Calculado:** R$ 0,00 **Média dos Preços Obtidos:** R$ 0,00

Quantidade	Descrição	Observação
1 Unidade	SOFTWARE DE BACKUP DE DADOS	

Item 7: EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES

Preço Estimado: R$ 0,00 (un) **Percentual:** - **Preço Estimado Calculado:** R$ 0,00 **Média dos Preços Obtidos:** R$ 0,00

Quantidade	Descrição	Observação
1 Unidade	EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	

Item 8: SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES

Preço Estimado: R$ 0,00 (un) **Percentual:** - **Preço Estimado Calculado:** R$ 0,00 **Média dos Preços Obtidos:** R$ 0,00

Quantidade	Descrição	Observação
1 Unidade	SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	

Item 9: SWITCH CORE

Preço Estimado: R$ 0,00 (un) **Percentual:** - **Preço Estimado Calculado:** R$ 0,00 **Média dos Preços Obtidos:** R$ 0,00

Quantidade	Descrição	Observação
1 Unidade	SWITCH CORE	

Extrato de fontes utilizadas neste relatório

ATENÇÃO - O Banco de Preços é uma solução tecnológica que atende aos parâmetros de pesquisa dispostos em Leis vigentes, Instruções Normativas, Acórdãos, Regulamentos, Decretos e Portarias. Sendo assim, por reunir diversas fontes governamentais, complementares e sites de domínio amplo, o sistema não é considerado uma fonte e, sim, um meio para que as pesquisas sejam realizadas de forma segura, ágil e eficaz.

Fontes utilizadas nesta cotação:

Outlook

[PGJ/AM] - Datacenter Ministério Público do Amazonas

De Setor de Compras e Servicos <compras@mpam.mp.br>
Data Sex, 28/11/2025 11:20
Cco geilson.melo@addvalue.com.br <geilson.melo@addvalue.com.br>; italopessoa@telequip.com.br <italopessoa@telequip.com.br>; rodrigo.medeiros@approachtech.com.br <rodrigo.medeiros@approachtech.com.br>; alex@cdti.com.br <alex@cdti.com.br>

2 anexos (561 KB)
SEI - 2025.007562.pdf; Modelo de Planilha de formação de preços.docx;

PREZADO FORNECEDOR.

Considerando o PI-2025.007562, que trata da *contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais do Ministério Público do Estado do Amazonas (MPAM);* considerando que propostas de preços já foram encaminhadas anteriormente; e que **houve algumas alterações nas especificações e no quantitativo de alguns itens**, solicitamos o envio de proposta formal de preços com as seguintes observações:

1) A proposta deverá apresentar informações gerais da empresa, tais como: timbre; razão social; CNPJ; endereço, telefones; e-mail; pessoa de contato; dados bancários; data; e assinatura do responsável, bem como os valores unitário e total da contratação.

2) A proposta deverá ter validade mínima de 90 (noventa) dias.

3) O fornecedor deverá observar atentamente as especificações e condições estabelecidas no Termo de Referência em anexo, de forma que a proposta atenda aos requisitos mínimos exigidos.

Pedimos, ainda, que Vossa Senhoria priorize o nosso pleito, encaminhando os arquivos necessários, no máximo, até o dia 01 de dezembro de 2025. Ficamos no aguardo, agradecendo desde já por confirmar o recebimento desta mensagem.

Atenciosamente,

CARLOS EDUARDO ALFAIA DE AZEVEDO
Setor de Compras & Serviços
Ministério Público do Estado do Amazonas
Procuradoria-Geral de Justiça

Telefone: (92) 3655-0763
Whatsapp: (92) 99180-0363
E-mail: compras@mpam.mp.br
CNPJ: 04.153.748/0001-85
Avenida Coronel Teixeira, n. 7995 - Bairro Nova Esperança
CEP: 69037-473 - Manaus/AM
CNPJ: 04.153.748/0001-85

O conteúdo deste e-mail é confidencial e destinado apenas ao destinatário especificado na mensagem. É estritamente proibido compartilhar qualquer parte desta mensagem com terceiros, sem o consentimento por escrito do remetente. Se você recebeu esta mensagem por engano, responda a esta mensagem e prossiga com sua exclusão, para que possamos garantir que tal erro não ocorra no futuro.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

CERTIDÃO Nº 112.2025.SCOMS.2024671.2025.007562

CERTIFICO, para fins de informação a constar nos presentes autos, que, após consulta ao Sistema Banco de Preços adotado por essa Instituição (doc. 2024571), não foram localizados itens com objetos semelhantes que atendessem as especificações constantes do Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562, razão pela qual se procedeu à consulta direta com fornecedores, via lista de fornecedores (doc. 2018636), a fim de estabelecer os respectivos valores estimados, para a contratação em tela mediante licitação.

É a certidão.

Iury Fechine Ramos

Chefe do Setor de Compras e Serviços

Documento assinado eletronicamente por **Iury Fechine Ramos**, **Chefe do Setor de Compras e Serviços - SCOMS**, em 05/12/2025, às 10:06, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2024671** e o código CRC **A7CF2E19**.

Outlook

Re: [PGJ/AM] - Datacenter Ministério Público do Amazonas

De Geilson Melo - Add Value <geilson.melo@addvalue.com.br>
Data Qua, 03/12/2025 10:23
Para Setor de Compras e Servicos <compras@mpam.mp.br>

1 anexo (191 KB)
Modelo de Planilha de formação de preços - Add.pdf;

Prezados, bom dia!

Segue nossa proposta, conforme solicitado.

Atenciosamente,

Geilson Melo
Gerente de Território RJ / ES
+55 21 3900-9833 | +55 21 98493-9385
geilson.melo@addvalue.com.br

ADDVALUE

De: Setor de Compras e Servicos <compras@mpam.mp.br>
Data: sexta-feira, 28 de novembro de 2025 às 12:27
Para:
Assunto: [PGJ/AM] - Datacenter Ministério Público do Amazonas

PREZADO FORNECEDOR.

Considerando o PI-2025.007562, que trata da *contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais do Ministério Público do Estado do Amazonas (MPAM);* considerando que propostas de preços já foram encaminhadas anteriormente; e que **houve algumas alterações nas especificações e no quantitativo de alguns itens**, solicitamos o envio de proposta formal de preços com as seguintes observações:

1) A proposta deverá apresentar informações gerais da empresa, tais como: timbre; razão social; CNPJ; endereço, telefones; e-mail; pessoa de contato; dados bancários; data; e assinatura do responsável, bem como os valores unitário e total da contratação.

2) A proposta deverá ter validade mínima de 90 (noventa) dias.

3) O fornecedor deverá observar atentamente as especificações e condições estabelecidas no Termo de Referência em anexo, de forma que a proposta atenda aos requisitos mínimos exigidos.

Pedimos, ainda, que Vossa Senhoria priorize o nosso pleito, encaminhando os arquivos necessários, no máximo, até o dia 01 de dezembro de 2025. Ficamos no aguardo, agradecendo desde já por confirmar o recebimento desta mensagem.

Atenciosamente,

CARLOS EDUARDO ALFAIA DE AZEVEDO
Setor de Compras & Serviços
Ministério Público do Estado do Amazonas
Procuradoria-Geral de Justiça

Telefone: (92) 3655-0763
Whatsapp: (92) 99180-0363
E-mail: compras@mpam.mp.br
CNPJ: 04.153.748/0001-85
Avenida Coronel Teixeira, n. 7995 - Bairro Nova Esperança
CEP: 69037-473 - Manaus/AM
CNPJ: 04.153.748/0001-85

O conteúdo deste e-mail é confidencial e destinado apenas ao destinatário especificado na mensagem. É estritamente proibido compartilhar qualquer parte desta mensagem com terceiros, sem o consentimento por escrito do remetente. Se você recebeu esta mensagem por engano, responda a esta mensagem e prossiga com sua exclusão, para que possamos garantir que tal erro não ocorra no futuro.

Objeto: Contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais do Ministério Público do Estado do Amazonas (MPAM).

ITEM	DESCRIÇÃO	UND	QTDE	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
01	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9		4	R$ 573.950,00	R$ 2.295.800,00
02	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU		1	R$ 816.070,00	R$ 816.070,00
03	SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX		5	R$ 889.030,00	R$ 4.445.150,00
04	SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU		1	R$ 161.914,00	R$ 161.914,00
05	LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE		50	R$ 9.322,00	R$ 466.100,00
06	SOFTWARE DE BACKUP DE DADOS		1	R$ 2.103.586,00	R$ 2.103.586,00
07	EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES		1	R$ 379.979,00	R$ 379.979,00
08	SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES		1	R$ 1.330.500,00	R$ 1.330.500,00
09	SWITCH CORE		2	R$ 268.030,00	R$ 536.060,00
VALOR TOTAL (R$)					**R$ 12.535.159,00**

A proposta deverá levar em consideração as seguintes observações:

1 - A proposta deverá ser encaminhada em documento com o timbre e informações gerais da empresa, como CNPJ, endereço, contatos, e-mail, dados bancários, e outros dados.

2 - A proposta deverá ter validade mínima de 90 (noventa) dias.

3 - O fornecedor deverá observar atentamente as especificações e condições estabelecidas no TERMO DE REFERÊNCIA Nº 9.2025.DTIC.1605182.2025.007562, em anexo, de forma que a proposta atenda aos requisitos exigidos.

Rio de Janeiro, 03 de dezembro de 2025

Outlook

RES: [PGJ/AM] - Datacenter Ministério Público do Amazonas

De Rosana Vieira <rosana.vieira@approachtech.com.br>
Data Qua, 03/12/2025 11:11
Para Setor de Compras e Servicos <compras@mpam.mp.br>
Cc Rodrigo Medeiros <rodrigo.medeiros@approachtech.com.br>

1 anexo (1.017 KB)
PROPOSTA COMERCIAL - MPAM_03.12.25.pdf;

> Geralmente, você não recebe emails de rosana.vieira@approachtech.com.br. Saiba por que isso é importante

Prezados, Bom dia!

Encaminho anexo proposta comercial conforme solicitado.

Seguimos a disposição!

Atenciosamente,

Rosana Vieira
Coordenadora Comercial

+55 48 996397449
rosana.vieira@approachtech.com.br
approachtech.com.br

approach
Conexões que impulsionam

Aviso de Confidencialidade: Este e-mail e quaisquer arquivos anexos podem conter informações confidenciais e/ou privilegiadas pertencentes à Approach Tecnologia. Se você não é o destinatário pretendido ou recebeu esta mensagem por engano, por favor, notifique imediatamente o remetente e apague-a permanentemente. Qualquer uso não autorizado, divulgação ou distribuição desta comunicação é estritamente proibido. Obrigado.Confidentiality Notice: This e-mail and any attachments may contain confidential and/or privileged information belonging to Approach Tecnologia. If you are not the intended recipient or have received this message in error, please immediately notify the sender and permanently delete it. Any unauthorized use, disclosure, or distribution of this communication is strictly prohibited. Thank you.

De: Setor de Compras e Servicos <compras@mpam.mp.br>
Data: 28 de novembro de 2025 às 12:20:57 BRT
Assunto: [PGJ/AM] - Datacenter Ministério Público do Amazonas

PREZADO FORNECEDOR.

Considerando o PI-2025.007562, que trata da *contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e*

software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais do Ministério Público do Estado do Amazonas (MPAM); considerando que propostas de preços já foram encaminhadas anteriormente; e que **houve algumas alterações nas especificações e no quantitativo de alguns itens**, solicitamos o envio de proposta formal de preços com as seguintes observações:

1) A proposta deverá apresentar informações gerais da empresa, tais como: timbre; razão social; CNPJ; endereço, telefones; e-mail; pessoa de contato; dados bancários; data; e assinatura do responsável, bem como os valores unitário e total da contratação.

2) A proposta deverá ter validade mínima de 90 (noventa) dias.

3) O fornecedor deverá observar atentamente as especificações e condições estabelecidas no Termo de Referência em anexo, de forma que a proposta atenda aos requisitos mínimos exigidos.

Pedimos, ainda, que Vossa Senhoria priorize o nosso pleito, encaminhando os arquivos necessários, no máximo, até o dia 01 de dezembro de 2025. Ficamos no aguardo, agradecendo desde já por confirmar o recebimento desta mensagem.

Atenciosamente,

CARLOS EDUARDO ALFAIA DE AZEVEDO
Setor de Compras & Serviços
Ministério Público do Estado do Amazonas
Procuradoria-Geral de Justiça

Telefone: (92) 3655-0763
Whatsapp: (92) 99180-0363
E-mail: compras@mpam.mp.br
CNPJ: 04.153.748/0001-85
Avenida Coronel Teixeira, n. 7995 - Bairro Nova Esperança
CEP: 69037-473 - Manaus/AM
CNPJ: 04.153.748/0001-85

O conteúdo deste e-mail é confidencial e destinado apenas ao destinatário especificado na mensagem. É estritamente proibido compartilhar qualquer parte desta mensagem com terceiros, sem o consentimento por escrito do remetente. Se você recebeu esta mensagem por engano, responda a esta mensagem e prossiga com sua exclusão, para que possamos garantir que tal erro não ocorra no futuro.

Projeto de: Datacenter

Cliente: **Ministério Público do Amazonas**

3 de dezembro de 2025

Rodrigo Medeiros
Executivo de contas

O QUE RESOLVEMOS

Soluções tecnológicas para a gestão da conectividade, armazenamento de dados e segurança da informação.

Por meio da **compreensão profunda das necessidades dos nossos clientes,** guiada por **profissionais proativos e altamente qualificados,** resultando em uma experiência consultiva personalizada, oferecemos soluções enterprise de ponta a ponta.

Somos propulsores de inovação e performance tecnológica, permitindo que nossos clientes atinjam seu potencial pleno para expandir seus negócios e propósitos, gerando assim, impacto positivo e valor para a economia e sociedade.

1. PROPOSTA COMERCIAL

Proposta Comercial para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais do Ministério Público do Estado do Amazonas (MPAM).

1.1. Itens e valores

ITEM	DESCRIÇÃO	QTDE	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
1	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9	4	R$ 579.768,00	R$ 2.319.072,00
2	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU	1	R$ 824.978,00	R$ 824.978,00
3	SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX	5	R$ 937.101,00	R$ 4.685.505,00
4	SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU	1	R$ 158.080,00	R$ 158.080,00
5	LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE	50	R$ 8.922,00	R$ 446.100,00
6	SOFTWARE DE BACKUP DE DADOS	1	R$ 1.934.224,00	R$ 1.934.224,00
7	EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	1	R$ 404.241,00	R$ 404.241,00
8	SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	1	R$ 1.506.087,00	R$ 1.506.087,00
9	SWITCH CORE	2	R$ 251.987,00	R$ 503.974,00
VALOR TOTAL (R$)				**R$ 12.782.261,00**

1.2. Premissas e observações

- Os itens de hardware e software têm seu preço base em USD, convertidos para R$ pela cotação do dia. Esses valores estão sujeitos às variações cambiais.
- O dimensionamento da solução foi efetuado segundo informações fornecidas pelo contratante.

1.3. Condições comerciais

- **Prazo de entrega:** Em até 120 (cento e vinte) dias após a confirmação do pedido.
- **Validade da proposta:** 90 (noventa) dias**.**

1.4. Confidencialidade

As informações contidas nesta proposta são confidenciais e fornecidas para a finalidade exclusiva de apresentação técnica e comercial da Approach Tecnologia a pedido do cliente, e não deve, de forma alguma, ser utilizada para qualquer outra finalidade.

Atenciosamente,

Rodrigo Medeiros
Executivo de contas

Outlook

Re: [PGJ/AM] - Datacenter Ministério Público do Amazonas

De Ivanilda Tavares <ivanilda@telequip.com.br>
Data Qui, 04/12/2025 10:41
Para Setor de Compras e Servicos <compras@mpam.mp.br>
Cc Italo Pessoa <italopessoa@telequip.com.br>

1 anexo (1 MB)
2025.12.04 - MPAM.pdf;

Geralmente, você não recebe emails de ivanilda@telequip.com.br. Saiba por que isso é importante

Prezado Sr Carlos Eduardo,

Segue em anexo nossa proposta.

Favor confirmar o recebimento.

Atenciosamente,

De: Setor de Compras e Servicos <compras@mpam.mp.br>
Data: 28 de novembro de 2025 às 12:20:49 BRT
Assunto: [PGJ/AM] - Datacenter Ministério Público do Amazonas

PREZADO FORNECEDOR.

Considerando o PI-2025.007562, que trata da *contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais do Ministério Público do Estado do Amazonas (MPAM);* considerando que propostas de preços já foram encaminhadas anteriormente; e que **houve algumas alterações nas especificações e no quantitativo de alguns itens**, solicitamos o envio de proposta formal de preços com as seguintes observações:

1) A proposta deverá apresentar informações gerais da empresa, tais como: timbre; razão social; CNPJ; endereço, telefones; e-mail; pessoa de contato; dados bancários; data; e assinatura do responsável, bem como os valores unitário e total da contratação.

2) A proposta deverá ter validade mínima de 90 (noventa) dias.

3) O fornecedor deverá observar atentamente as especificações e condições estabelecidas no Termo de Referência em anexo, de forma que a proposta atenda aos requisitos mínimos exigidos.

Pedimos, ainda, que Vossa Senhoria priorize o nosso pleito, encaminhando os arquivos necessários, no máximo, até o dia 01 de dezembro de 2025. Ficamos no aguardo, agradecendo desde já por confirmar o recebimento desta mensagem.

Atenciosamente,

CARLOS EDUARDO ALFAIA DE AZEVEDO
Setor de Compras & Serviços
Ministério Público do Estado do Amazonas
Procuradoria-Geral de Justiça

Telefone: (92) 3655-0763
Whatsapp: (92) 99180-0363
E-mail: compras@mpam.mp.br
CNPJ: 04.153.748/0001-85
Avenida Coronel Teixeira, n. 7995 - Bairro Nova Esperança
CEP: 69037-473 - Manaus/AM
CNPJ: 04.153.748/0001-85

O conteúdo deste e-mail é confidencial e destinado apenas ao destinatário especificado na mensagem. É estritamente proibido compartilhar qualquer parte desta mensagem com terceiros, sem o consentimento por escrito do remetente. Se você recebeu esta mensagem por engano, responda a esta mensagem e prossiga com sua exclusão, para que possamos garantir que tal erro não ocorra no futuro.

--
Ivanilda Tavares
Telequip Conectividade
84 3025-1032 / 3234-8151

Ao: Ministério Público do Amazonas

Att.: CARLOS EDUARDO ALFAIA DE AZEVEDO -
Setor de Compras & Serviços

Objeto: Contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais do Ministério Público do Estado do Amazonas (MPAM).

ITEM	DESCRIÇÃO	UN	QTDE	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
01	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9	UN	4	610.470,00	2.441.880,00
02	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU	UN	1	857.780,00	857.780,00
03	SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX	UN	5	801.173,44	4.005.867,20
04	SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU	UN	1	172.763,20	172.763,20
05	LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE	UN	50	9.508,95	475.447,50
06	SOFTWARE DE BACKUP DE DADOS	UN	1	1.978.252,78	1.978.252,78
07	EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	UN	1	337.094,14	337.094,14
08	SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	UN	1	1.378.000,21	1.378.000,21
09	SWITCH CORE	UN	2	266.413,97	532.827,94
				VALOR TOTAL (R$)	**12.179.912,97**

A proposta deverá levar em consideração as seguintes observações:

1 - A proposta deverá ser encaminhada em documento com o timbre e informações gerais da empresa, como CNPJ, endereço, contatos, e-mail, dados bancários, e outros dados.

2 - A proposta deverá ter validade mínima de 90 (noventa) dias.

3 - O fornecedor deverá observar atentamente as especificações e condições estabelecidas no TERMO DE REFERÊNCIA Nº 9.2025.DTIC.1605182.2025.007562, em anexo, de forma que a proposta atenda aos requisitos exigidos.

Natal/RN, 04 de dezembro de 2025

TELEQUIP TELECOMUNICACOES E EQUIPAMENTOS LTDA:70306477000185

Assinado de forma digital por TELEQUIP TELECOMUNICACOES E EQUIPAMENTOS LTDA:70306477000185
Dados: 2025.12.04 11:40:41 -03'00'

Telequip Telecomunicações e Equipamentos Ltda
Francisco Italo Pessoa Alves

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MAPA DEMONSTRATIVO DE PREÇOS Nº 176.2025.SCOMS.2023737.2025.007562

RESUMO DESCRITIVO DO OBJETO
Contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais do Ministério Público do Estado do Amazonas (MPAM).

DADOS GERAIS DA PESQUISA	
Responsável pela pesquisa: Carlos Eduardo Alfaia de Azevedo. **Período da cotação:** 25 de novembro a 04 de dezembro de 2025.	**Critérios estatísticos aplicados:** Foi utilizado o critério da média aritmética simples para definição dos valores estimados da contratação. Os valores unitários foram arredondados para cima, no limite de 2 (duas) casas decimais. Os valores totais foram calculados em função do valor unitário já arredondado.

FONTES DE PREÇO CONSULTADAS			
A	ADD VALUE PARTICIPAÇÕES COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA CNPJ: 10.864.910/0001-76	03.12.2025	doc. 2022384
B	APPROACH TECNOLOGIA LTDA CNPJ: 24.376.542/0001-2	03.12.2025	doc. 2022551
C	TELEQUIP TELECOMUNICAÇÕES E EQUIPAMENTOS LTDA CNPJ: 70.306.477/0001-85	04.12.2025	doc. 2023712

PESQUISA DE MERCADO

ITEM 1 — EQUIPAMENTO HIPERCONVERGENTE - PLATAFORMA NUTANIX G9		UNIDADE	QUANTIDADE
		Unidade	4
FONTES DE PREÇO		**VALOR UNITÁRIO**	**VALOR TOTAL**
A	ADD VALUE PARTICIPAÇÕES COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA	R$ 573.950,00	R$ 2.295.800,00
B	APPROACH TECNOLOGIA LTDA	R$ 579.768,00	R$ 2.319.072,00
C	TELEQUIP TELECOMUNICAÇÕES E EQUIPAMENTOS LTDA	R$ 610.470,00	R$ 2.441.880,00
VALORES MÉDIOS ESTIMADOS PARA O ITEM 1		**R$ 588.062,67**	**R$ 2.352.250,68**

ITEM 2 — EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU		UNIDADE	QUANTIDADE
		Unidade	1
FONTES DE PREÇO		VALOR UNITÁRIO	VALOR TOTAL
A	ADD VALUE PARTICIPAÇÕES COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA	R$ 816.070,00	R$ 816.070,00
B	APPROACH TECNOLOGIA LTDA	R$ 824.978,00	R$ 824.978,00
C	TELEQUIP TELECOMUNICAÇÕES E EQUIPAMENTOS LTDA	R$ 857.780,00	R$ 857.780,00
VALORES MÉDIOS ESTIMADOS PARA O ITEM 2		**R$ 832.942,67**	**R$ 832.942,67**

ITEM 3 — SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX		UNIDADE	QUANTIDADE
		Unidade	5
FONTES DE PREÇO		VALOR UNITÁRIO	VALOR TOTAL
A	ADD VALUE PARTICIPAÇÕES COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA	R$ 889.030,00	R$ 4.445.150,00
B	APPROACH TECNOLOGIA LTDA	R$ 937.101,00	R$ 4.685.505,00
C	TELEQUIP TELECOMUNICAÇÕES E EQUIPAMENTOS LTDA	R$ 801.173,44	R$ 4.005.867,20
VALORES MÉDIOS ESTIMADOS PARA O ITEM 3		**R$ 875.768,15**	**R$ 4.378.840,75**

ITEM 4 — SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU		UNIDADE	QUANTIDADE
		Unidade	1
FONTES DE PREÇO		VALOR UNITÁRIO	VALOR TOTAL
A	ADD VALUE PARTICIPAÇÕES COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA	R$ 161.914,00	R$ 161.914,00
B	APPROACH TECNOLOGIA LTDA	R$ 158.080,00	R$ 158.080,00
C	TELEQUIP TELECOMUNICAÇÕES E EQUIPAMENTOS LTDA	R$ 172.763,20	R$ 172.763,20
VALORES MÉDIOS ESTIMADOS PARA O ITEM 4		**R$ 164.252,40**	**R$ 164.252,40**

ITEM 5 — LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE		UNIDADE	QUANTIDADE
		Unidade	50
FONTES DE PREÇO		VALOR UNITÁRIO	VALOR TOTAL
A	ADD VALUE PARTICIPAÇÕES COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA	R$ 9.322,00	R$ 466.100,00
B	APPROACH TECNOLOGIA LTDA	R$ 8.922,00	R$ 446.100,00

C	TELEQUIP TELECOMUNICAÇÕES E EQUIPAMENTOS LTDA	R$ 9.508,95	R$ 475.447,50
VALORES MÉDIOS ESTIMADOS PARA O ITEM 5		**R$ 9.250,98**	**R$ 462.549,00**

ITEM 6 — SOFTWARE DE BACKUP DE DADOS		**UNIDADE**	**QUANTIDADE**
		Unidade	**1**
FONTES DE PREÇO		**VALOR UNITÁRIO**	**VALOR TOTAL**
A	ADD VALUE PARTICIPAÇÕES COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA	R$ 2.103.586,00	R$ 2.103.586,00
B	APPROACH TECNOLOGIA LTDA	R$ 1.934.224,00	R$ 1.934.224,00
C	TELEQUIP TELECOMUNICAÇÕES E EQUIPAMENTOS LTDA	R$ 1.978.252,78	R$ 1.978.252,78
VALORES MÉDIOS ESTIMADOS PARA O ITEM 6		**R$ 2.005.354,26**	**R$ 2.005.354,26**

ITEM 7 — EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES		**UNIDADE**	**QUANTIDADE**
		Unidade	**1**
FONTES DE PREÇO		**VALOR UNITÁRIO**	**VALOR TOTAL**
A	ADD VALUE PARTICIPAÇÕES COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA	R$ 379.979,00	R$ 379.979,00
B	APPROACH TECNOLOGIA LTDA	R$ 404.241,00	R$ 404.241,00
C	TELEQUIP TELECOMUNICAÇÕES E EQUIPAMENTOS LTDA	R$ 337.094,14	R$ 337.094,14
VALORES MÉDIOS ESTIMADOS PARA O ITEM 7		**R$ 373.771,38**	**R$ 373.771,38**

ITEM 8 — SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES		**UNIDADE**	**QUANTIDADE**
		Unidade	**1**
FONTES DE PREÇO		**VALOR UNITÁRIO**	**VALOR TOTAL**
A	ADD VALUE PARTICIPAÇÕES COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA	R$ 1.330.500,00	R$ 1.330.500,00
B	APPROACH TECNOLOGIA LTDA	R$ 1.506.087,00	R$ 1.506.087,00
C	TELEQUIP TELECOMUNICAÇÕES E EQUIPAMENTOS LTDA	R$ 1.378.000,21	R$ 1.378.000,21
VALORES MÉDIOS ESTIMADOS PARA O ITEM 8		**R$ 1.404.862,40**	**R$ 1.404.862,40**

ITEM 9 — SWITCH CORE		**UNIDADE**	**QUANTIDADE**
		Unidade	**2**
FONTES DE PREÇO		**VALOR UNITÁRIO**	**VALOR TOTAL**
A	ADD VALUE PARTICIPAÇÕES COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA	R$ 268.030,00	R$ 536.060,00

B	APPROACH TECNOLOGIA LTDA	R$ 251.987,00	R$ 503.974,00
C	TELEQUIP TELECOMUNICAÇÕES E EQUIPAMENTOS LTDA	R$ 266.413,97	R$ 532.827,94
VALORES MÉDIOS ESTIMADOS PARA O ITEM 9		**R$ 262.143,66**	**R$ 524.287,32**

Documento assinado eletronicamente por **Iury Fechine Ramos**, **Chefe do Setor de Compras e Serviços - SCOMS**, em 05/12/2025, às 10:12, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2023737** e o código CRC **9B9DDA5F**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

QUADRO-RESUMO DO PROCESSO DE COMPRA Nº 547.2025.SCOMS.2023741.2025.007562

IDENTIFICAÇÃO DO FORNECEDOR

INDEFINIDO
A LICITAR

RESUMO DESCRITIVO DO OBJETO

Contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais do Ministério Público do Estado do Amazonas (MPAM).

DETALHAMENTO DO OBJETO

ITEM	ESPECIFICAÇÃO	UNIDADE	QTD	VALOR UNITÁRIO	VALOR TOTAL
1	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9	Unidade	4	R$ 588.062,67	R$ 2.352.250,68
2	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU	Unidade	1	R$ 832.942,67	R$ 832.942,67
3	SOFTWARE GESTÃO DAPLATAFORMA DE HIPERCONVERGENCIA NUTANIX	Unidade	5	R$ 875.768,15	R$ 4.378.840,75
4	SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU	Unidade	1	R$ 164.252,40	R$ 164.252,40

5	LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE	Unidade	50	R$ 9.250,98	R$ 462.549,00
6	SOFTWARE DE BACKUP DE DADOS	Unidade	1	R$ 2.005.354,26	R$ 2.005.354,26
7	EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	Unidade	1	R$ 373.771,38	R$ 373.771,38
8	SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	Unidade	1	R$ 1.404.862,40	R$ 1.404.862,40
9	SWITCH CORE	Unidade	2	R$ 262.143,66	R$ 524.287,32
VALOR TOTAL DA CONTRATAÇÃO					**R$ 12.499.110,86**

	MODALIDADE SUGERIDA DE CONTRATAÇÃO	FUNDAMENTO LEGAL
	DISPENSA DE LICITAÇÃO	
	INEXIGIBILIDADE DE LICITAÇÃO	
	ADESÃO À ATA DE REGISTRO DE PREÇOS	
	PRORROGAÇÃO DE ATA DE REGISTRO DE PREÇOS	
X	**A LICITAR**	Lei n.º 14.133/2021

INFORMAÇÕES COMPLEMENTARES

— Valores informados conforme a pesquisa de mercado detalhada no Mapa Demonstrativo de Preços Nº 176.2025.SCOMS (doc. 2023737).

— Encaminhe-se à DOF para providências.

Documento assinado eletronicamente por **Iury Fechine Ramos**, **Chefe do Setor de Compras e Serviços - SCOMS**, em 05/12/2025, às 10:12, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2023741** e o código CRC **9D91EF8E**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Av. Coronel Teixeira,nº 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MEMORANDO Nº 28.2025.DOF - ORÇAMENTO.2025202.2025.007562

De: Diretoria de Orçamento e Finanças

Para: Diretoria de Planejamento

Assunto: Contratação para fins de aquisição de uma solução de datacenter.

Com os cumprimentos de estilo, encaminho o presente procedimento para fins de prestação de informação quanto à proposta orçamentária para o exercício de 2026, que atenderá a futura despesa dele resultante, conforme abaixo:

- Programa de Trabalho: 03.091.3234.2536.0001 - Aparelhamento de Unidades Administrativas e Operacionais;

- Natureza de despesa: 4490.52 - Equipamentos e Material Permanente.

Atenciosamente,

MARCOS ANDRÉ ABENSUR
Diretor de Orçamento e Finanças

Documento assinado eletronicamente por **Marcos André Abensur**, **Diretor(a) de Orçamento e Finanças - DOF**, em 05/12/2025, às 16:29, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2025202** e o código CRC **CD21CB1E**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MEMORANDO Nº 397.2025.DPLAN.2026956.2025.007562

Manaus, [data da assinatura eletrônica]

Ao Sr.
MARCOS ANDRÉ ABENSUR
Diretor de Orçamento e Finanças
Nesta

Assunto: Contratação para fins de aquisição de uma solução de datacenter.

Senhor Diretor,

Em atenção ao Memorando Nº 28.2025.DOF - ORÇAMENTO.2025202.2025.007562 a respeito da proposta orçamentária de 2026, com o objetivo de atender a demanda para a aquisição de um datacenter, informamos que o projeto de lei encontra-se em tramitação na Assembleia Legislativa do Amazonas - ALEAM, mas o valor inicialmente previsto para esta aquisição se encontra disponível na ação orçamentaria de nº 2536 - Aparelhamento de Unidades Administrativas e Operacionais, como demonstra o quadro-resumo a seguir:

Programa	Ação Orçamentária		Valor Total Disponível (R$)
	Tipo	Descrição	
3234 - DESENVOLVIMENTO E GARANTIA DA ATUAÇÃO INSTITUCIONAL	Atividades	2536 - Aparelhamento de Unidades Administrativas e Operacionais	8.010.000,00

Adicionalmente informamos que o saldo inicial de R$ 8.010.000,00 pode não ser suficiente para cobrir o valor necessário desta aquisição após o resultado do processo licitatório. Contudo, esta ação orçamentária poderá ser suplementada com recursos disponíveis nas ações orçamentarias a saber:

Programa	Ação Orçamentária		Valor Total Disponível (R$)
	Tipo	Descrição	
3234 - DESENVOLVIMENTO E GARANTIA DA ATUAÇÃO INSTITUCIONAL	Atividades	1208 - Reforma e Ampliação de Unidades Administrativas e Operacionais	8.836.000,00
		1209 - Construção de Unidades Administrativas e Operacionais	20.050.000,00
		1557 - Fortalecimento das Promotorias de Justiça do Interior	7.500.000,00

Respeitosamente,

(assinado eletronicamente)
AFRANIO CORRÊA LIMA JUNIOR
Agente Técnico Economista

(assinado eletronicamente)
JANICE QUEIROZ DE OLIVEIRA
Diretora de Planejamento

Documento assinado eletronicamente por **Janice Queiroz de Oliveira**, **Diretor(a) de Planejamento - DPLAN**, em 10/12/2025, às 11:21, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Afranio Correa Lima Junior**, **Agente Técnico - Economista**, em 10/12/2025, às 11:22, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2026956** e o código CRC **4E2A20C8**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Av. Coronel Teixeira,nº 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

NOTA DE AUTORIZAÇÃO DE DESPESAS / ADJUDICAÇÃO -NAD Nº 512.2025.DOF - ORÇAMENTO.2028015.2025.007562

1 - INFORMAÇÕES DA NOTA DE AUTORIZAÇÃO DE DESPESAS E ADJUDICAÇÃO

Procedimento Interno: 2025.007562 **Processo de Compra: Nº 547.2025.SCOMS.2023741.2025.007562** **Interessado:** Adenilson Roberto de Oliveira Filho, Chefe da Divisão de Controles e Convênios	**Modalidade:** Ordinário **Origem:** Lei n.º 14.133/2021 **Credor:** Indefinido - A licitar

2 - DESCRIÇÃO ORÇAMENTÁRIA

Unidade Orçamentária: 03.101 - Procuradoria-Geral de Justiça do Amazonas **Fonte de Recurso:** 1.500.100 - Recursos não Vinculados de Impostos **Programa de Trabalho:** 03.091.3234.2536.0001 - Aparelhamento de Unidades Administrativas e Operacionais	**Elemento: 4490.52** **-** Equipamentos e Material Permanente **Subelemento: 4490.52.55** **-** TECNOLOGIA DA INFORMAÇÃO

3 - CONTROLE ORÇAMENTÁRIO

SALDO ATUAL	DEDUÇÃO PREVISTA	SALDO APÓS DESPESA
R$ 44.396.000	R$ 12.499.110,86	R$ 31.896.889,14

4 - ESPECIFICAÇÃO DO OBJETO

Contratação de empresa especializada para o ofrnecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atemder as necessidades institucionais do Ministério Público do Estado do Amazonas (MPAM).

ITEM	ESPECIFICAÇÃO	UNIDADE	QTD	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)

1	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9	Unidade	4	R$ 588.062,67	R$ 2.352.250,68
2	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU	Unidade	1	R$ 832.942,67	R$ 832.942,67
3	SOFTWARE GESTÃO DAPLATAFORMA DE HIPERCONVERGENCIA NUTANIX	Unidade	5	R$ 875.768,15	R$ 4.378.840,75
4	SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU	Unidade	1	R$ 164.252,40	R$ 164.252,40
5	LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE	Unidade	50	R$ 9.250,98	R$ 462.549,00
6	SOFTWARE DE BACKUP DE DADOS	Unidade	1	R$ 2.005.354,26	R$ 2.005.354,26
7	EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	Unidade	1	R$ 373.771,38	R$ 373.771,38
8	SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	Unidade	1	R$ 1.404.862,40	R$ 1.404.862,40
9	SWITCH CORE	Unidade	2	R$ 262.143,66	R$ 524.287,32
TOTAL (R$)					R$ 12.499.110,86

OBS: Proposta orçamentária para 2026, conforme memorando 397 (2026956).

5 - CRONOGRAMA DE DESEMBOLSO

JANEIRO	FEVEREIRO	MARÇO	ABRIL	MAIO	JUNHO
R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00
JULHO	**AGOSTO**	**SETEMBRO**	**OUTUBRO**	**NOVEMBRO**	**DEZEMBRO**

R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 12.499.110,86

6 - DESPACHO DO ORDENADOR DE DESPESAS

( ) Encaminhe-se à Divisão de Contratos e Convênios.
( ) Encaminhe-se à Comissão Permanente de Licitação.
(**X**) Autorizo a despesa. Encaminhe-se à Assessoria Jurídica para manifestação acerca da forma da contratação.
( ) Autorizo a despesa. Adjudico em favor da empresa. Empenhe-se.

Documento assinado eletronicamente por **André Virgílio Belota Seffair**, **Subprocurador(a)-Geral de Justiça para Assuntos Administrativos**, em 11/12/2025, às 15:54, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Marcos André Abensur**, **Diretor(a) de Orçamento e Finanças - DOF**, em 11/12/2025, às 16:41, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2028015** e o código CRC **1A98F2AB**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

OFÍCIO Nº 479.2025.CPL.2031552.2025.007562

Manaus, *na data da assinatura eletrônica.*

Ao Senhor

Adenilson Roberto de Oliveira Filho

Chefe da Divisão de Contratos e Convênios - DCCON

Assunto: Encaminhamento dos autos para elaboração de minuta contratual ou instrumento congênere.

Senhor Chefe,

Cumprimentando-o com o presente, informo que tramita nesta Comissão Permanente de Licitação o **Processo SEI n.º 2025.007562,** cujo objeto é a *contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses.*

Na oportunidade, em atenção ao Despacho nº 1123.2025.01AJ-SUBADM.2013504.2025.007562, bem como ao fluxo de processos de compra deste *Parquet*, remeto os presentes autos para análise quanto à necessidade de elaboração de minuta de termo contratual ou instrumento equivalente, especialmente em face do teor do Termo de Referência nº 28.2025.DTIC.2002143.2025.007562**.**

Outrossim, a referida minuta deverá ser submetida ao crivo da Douta Assessoria Jurídica do Ordenador de Despesas, para posterior juntada ao edital do certame a ser publicado.

Por derradeiro, **retornem** os autos a esta Comissão, para prosseguimento regular ao feito.

Atenciosamente,

Sarah Madalena B. Côrtes de Melo
Presidente da Comissão Permanente de Licitação
Ato PGJ n.º 165/2025 - DOMPE, Ed. 3121, de 15.07.2025

Documento assinado eletronicamente por **Sarah Madalena Barbosa Santos Cortes**, **Presidente da Comissão Permanente de Licitação - CPL**, em 16/12/2025, às 09:35, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2031552** e o código CRC **FE09E7BD**.

2025.007562 v5

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Av. Coronel Teixeira,nº 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MINUTA DE CONTRATO ADMINISTRATIVO Nº 68.2025.DCCON - CONTRATOS.2031978.2025.007562

Processo SEI n.º 2025.007562

Licitação ou Contratação Direta n.º _____

Contrato Administrativo n.º _____

Termo de Contrato Administrativo que entre si celebram o **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS** e a empresa _____, visando ao o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais da **CONTRATANTE**.

O **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**, por intermédio de sua **PROCURADORIA-GERAL DE JUSTIÇA**, órgão de sua Administração Superior, com sede na cidade de Manaus, Estado do Amazonas, na Avenida Coronel Teixeira, 7.995 – Nova Esperança, 69.037-473, inscrito no CNPJ (MF) sob o n.º 04.153.748/0001-85, doravante denominada **CONTRATANTE**, neste ato representada por seu Subprocurador-Geral de Justiça para Assuntos Administrativos, o Exmo. Sr. **André Virgílio Belota Seffair**, residente e domiciliado em Manaus/AM, inscito no CPF sob o n.º ***.287.772-**, e a empresa _____, inscrita no CNPJ (MF) sob o n.º _____, com sede na _____, _____, daqui por diante denominada **CONTRATADA**, neste ato representada por _____, inscrito no CPF (MF) sob o n.º _____, tendo em vista o que consta no **Processo n.º 2025.007562**, doravante denominado **PROCESSO**, e em consequência do _____, firmam o presente **TERMO DE CONTRATO ADMINISTRATIVO N.º _____**, nos moldes da Lei n.º 14.133/2021 e mediante as cláusulas a seguir estabelecidas:

CLÁUSULA PRIMEIRA – DO OBJETO:

O objeto deste ajuste consiste no fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais da **CONTRATANTE**.

CLÁUSULA SEGUNDA – DO DETALHAMENTO DO OBJETO:

O objeto deste instrumento compreende a contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais da **CONTRATANTE**.

1. Por tratar-se de solução integrada, em que o funcionamento efetivo e satisfatório depende de cada um dos seus itens em conjunto, como um todo, ou seja, o simples funcionamento de itens separadamente não tem nenhuma funcionalidade, conforme indicado no Estudo Técnico Preliminar (ETP), a contratação terá lote único, organizado conforme tabela a seguir:

ITEM	DESCRIÇÃO	QUANTIDADE
01	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9	4
02	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU	1
03	SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX	5
04	SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU	1
05	LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE	50
06	SOFTWARE DE BACKUP DE DADOS	1
07	EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	1
08	SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	1
09	SWITCH CORE	2

2. Nas especificações técnicas mínimas apresentadas a seguir, os termos "possui", "permite", "suporta" e "é" implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo "ou" implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo "e" implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções citadas.

3. A **CONTRATADA** não poderá oferecer serviço inferior as especificações apresentadas neste Termo, sendo permitido, porém, a oferta de serviço superior as especificações mínimas apresentadas, de acordo com a conveniência da **CONTRATADA** e aprovação da **CONTRATANTE**.

4. Toda documentação gerada durante a prestação dos serviços será de propriedade da **CONTRATANTE**, em virtude de sua elaboração tomar por base informações críticas do funcionamento intrínseco à sua infraestrutura, que afetam diretamente a segurança da **CONTRATANTE**.

5. A **CONTRATADA** deverá guardar inteiro sigilo dos serviços contratados e dos dados processados, bem como de toda e qualquer documentação gerada, reconhecendo serem esses de propriedade e uso exclusivo da **CONTRATANTE**, sendo vedada sua cessão, locação ou venda a terceiros.

6. **CONTRATADA** deverá manter a **CONTRATANTE** atualizada sobre todos os fluxos adotados para a execução das atividades objeto da contratação durante o período contratual, bem como sobre a forma de automatização de quaisquer serviços, documentando todos os procedimentos detalhadamente para que possam servir de base para a continuidade dos serviços independentemente da metodologia que possa ser adotada.

7 . ITEM 01 - EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9

7.1 Características Gerais

7.1.1 A infraestrutura deverá ser composta por appliances Nutanix com integração completa entre hardware e software, armazenamento e rede, entregando uma solução hiperconvergente pronta para operação.

7.1.2 Serão aceitos apenas appliances homologados pela Nutanix para uso com o Nutanix AOS (Acropolis Operating System) e Nutanix AHV (Acropolis Hypervisor) ou outro hipervisor suportado pela plataforma.

7.1.3 Caso necessário, será permitida a entrega de equipamentos ou recursos adicionais para atender aos requisitos mínimos, desde que todos os componentes estejam integrados e certificados pela Nutanix.

7.1.4 É permitida a entrega de múltiplos nós em um único chassi, desde que compatível com a arquitetura Nutanix.

7.1.5 A solução deve incluir a ferramenta Nutanix Prism, em sua ultima versão ou equivalente, que oferece gerenciamento centralizado e interface gráfica para monitoramento, atualizações e operação da infraestrutura, incluindo:

7.1.5.1 Atualização de BIOS, firmware, hipervisor e SDS;

7.1.5.2 Visualização do hardware físico;

7.1.5.3 Diagnóstico, inventário e expansão de nós.

7.1.6 Caso alguma funcionalidade não esteja disponível via Prism ou equivalente para monitoramento ou atualização, a CONTRATADA deverá realizar este serviço de forma remota/on-line ou presencial.

7.1.7 Todas as atualizações devem ser homologadas pela Nutanix e aplicadas conforme as melhores práticas da fabricante. Esta ferramenta deve ser gráfica, com suporte a apresentação de visões do hardware físico dos nós, suporte a troca de drives, com controle do inventário, com ferramenta de diagnóstico e com módulo para a

adição de novos nós.

7.1.8 A arquitetura deve garantir alta disponibilidade (HA) e resiliência a falhas, com suporte a recuperação de desastres (DR).

7.1.9 Os appliances devem permitir expansão modular e não disruptiva dos serviços de rede e aplicações, com detecção automática de novos nós.

7.1.10 Deve centralizar o armazenamento de dados em discos compartilhados, redundantes.

7.1.11 Cada nó deverá conter armazenamento dedicado para o sistema operacional da plataforma.

7.1.12 A solução deve estar preparada para ambientes de virtualização em alta disponibilidade, conforme as práticas recomendadas pela Nutanix.

7.1.13 Deve suportar software de virtualização para consolidação de servidores e recuperação automática em caso de falhas físicas, minimizando o downtime.

7.1.14 A entrega deve ser feita com todos os componentes física e logicamente integrados, sem ponto único de falha, com acesso imediato ao ambiente via sistema de gestão da plataforma após energização e conexão.

7.1.15 A instalação deve ser compatível com racks padrão de 19 polegadas, incluindo todos os acessórios necessários para montagem no ambiente da CONTRATANTE.

7.1.16 O equipamento deve integrar a linha de produtos Nutanix da família “NX”, assegurando total compatibilidade com atual ambiente e possibilidade de expansão das zonas de disponibilidade já estabelecidas, conforme informações disponibilizadas no endereço eletrônico oficial da fabricante: https://www.nutanix.com/products/hardwareplatforms/specsheet?platformProvider=Nutanix.

7.2 Configuração do Nó ou Chassi

7.2.1 Serão admitidas ofertas de chassis que comportam múltiplos servidores (nós/nodes), para o atendimento da especificação técnica.

7.2.2 Cada nó, ou chassi, deverá possuir ventiladores e fontes redundantes para a operação adequada dos equipamentos.

7.2.3 Todas as fontes de alimentação deverão ser acompanhadas de seus respectivos cabos de energia compatíveis.

7.3 Características de Processamento por Nó

7.3.1 Cada servidor deverá possuir, no mínimo, 02 (dois) processadores com arquitetura x86, voltados ao uso em servidores, contendo as seguintes características mínimas:

7.3.1.1 12 (doze) núcleos físicos e 24 (vinte e quatro) threads por processador;

7.3.1.2 Frequência de clock nominal de, no mínimo, 2,4 GHz;

7.3.1.3 Controladora de memória integrada com suporte à tecnologia DDR5 ou superior.

7.3.2 Será admitida a entrega de processadores de geração superior ao modelo originalmente especificado, desde que mantenham no mínimo a mesma quantidade de núcleos e threads, independentemente de demais especificações.

7.4 Especificações de Memória por Nó

7.4.1 Cada servidor deverá ser fornecido com, no mínimo, 1.536 GB (um mil quinhentos e trinta e seis gigabytes) de memória RAM, distribuída uniformemente entre os processadores, utilizando módulos DDR5 ou superior.

7.5 Especificações de Rede por Nó

7.5.1 Cada servidor deverá ser entregue com as seguintes interfaces de rede:

7.5.1.1 Mínimo de 2 (duas) interfaces de 25/10 GbE SFP28, integradas em uma placa de rede;

7.5.1.2 Mínimo de 1 (uma) interface exclusiva de gerenciamento Ethernet 1000Base-T.

7.5.2 A interface de gerenciamento deverá vir acompanhada de cabos UTP categoria 6 (ou superior), com comprimento mínimo de 5 (cinco) metros e conectores RJ-45.

7.6 Especificações de Armazenamento por Nó

7.6.1 Cada servidor deverá ser entregue com a seguinte configuração mínima de discos:

7.6.1.1 04 (quatro) unidades de SSD NVMe, ou SSD SAS/SATA, com capacidade mínima de 3,84 TB por unidade (volumetria bruta);

7.6.1.2 08 (oito) unidades de disco rígido (HDD), com capacidade mínima de 12 TB por unidade (volumetria bruta).

8 . ITEM 02 - EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU

8.1 Características Gerais

8.1.1 A solução deverá ser composta exclusivamente por appliances de nuvem privada, com integração total entre recursos de computação, armazenamento e rede, entregues como infraestrutura unificada.

8.1.2 Serão aceitos apenas appliances homologados para uso com a solução de armazenamento definido por software (Software Defined Storage – SDS) ofertada.

8.1.3 A entrega de equipamentos ou recursos adicionais será aceita, desde que necessária para o atendimento aos requisitos mínimos e que todos os componentes estejam devidamente integrados.

8.1.4 É permitida a entrega de múltiplos nós consolidados em um único chassi modular.

8.1.5 A solução deverá incluir ferramenta unificada de gerenciamento e atualização, com capacidade de monitorar e atualizar BIOS, firmwares, hypervisor e componentes do SDS. Caso não realize todos os procedimentos listados, a CONTRATADA deverá garantir a execução dessas tarefas presencial ou remotamente.

8.1.6 A ferramenta de gestão deverá ser gráfica, com visualização física dos nós, suporte à substituição de drives, inventário automatizado, diagnóstico integrado e capacidade de adicionar novos nós ao cluster.

8.1.7 A arquitetura deverá contemplar alta disponibilidade nativa e recursos para recuperação de desastres (DR), de forma a garantir continuidade dos serviços mesmo em caso de falhas parciais.

8.1.8 Os equipamentos devem possuir arquitetura modular, permitindo expansão de capacidade com inclusão de novos appliances sem interrupção dos serviços.

8.1.9 O armazenamento deverá ser centralizado, com discos compartilhados e redundância nativa.

8.1.10 Cada servidor deverá conter unidade de armazenamento dedicada ao sistema operacional da plataforma e aos softwares de virtualização e processamento gráfico.

8.1.11 A infraestrutura deverá estar preparada para suportar ambientes virtualizados de alta disponibilidade, de acordo com as boas práticas do fabricante da solução.

8.1.12 A solução deverá oferecer suporte a consolidação de servidores e recuperação automática em caso de falhas físicas.

8.1.13 A entrega deverá ocorrer com a solução fisicamente e logicamente pré-integrada, sem ponto único de falha, com acesso imediato à plataforma após energização e conexão física.

8.1.14 A instalação deverá ser compatível com racks padrão de 19", com todos os acessórios de fixação inclusos.

8.1.15 O equipamento deve integrar a linha de produtos Nutanix da família “NX”, assegurando total compatibilidade com atual ambiente e possibilidade de expansão das zonas de disponibilidade já estabelecidas, conforme informações disponibilizadas no endereço eletrônico oficial da fabricante: https://www.nutanix.com/products/hardwareplatforms/specsheet?platformProvider=Nutanix.

8.2 Configuração do Nó ou Chassi

8.2.1 Serão admitidas ofertas de chassis que comportam múltiplos servidores (nós/nodes), para o atendimento da especificação técnica.

8.2.2 Cada nó ou chassi deverá possuir ventiladores e fontes de alimentação redundantes.

8.2.3 Cada fonte deverá ser entregue com seu respectivo cabo de energia.

8.3 Características de Processamento por Nó

8.3.1 Cada servidor deverá possuir, no mínimo, dois processadores com arquitetura x86, dedicados a ambientes de datacenter, com as seguintes características:

8.3.2 12 (doze) núcleos físicos e 24 (vinte e quatro) threads por processador;

8.3.3 Frequência mínima de 2,4 GHz;

8.3.4 Controladora de memória integrada DDR5 ou superior.

8.3.5 A substituição por processadores mais recentes será aceita, desde que observadas as quantidades mínimas de núcleos e threads.

8.4 Especificações de Memória por Nó

8.4.1 - Cada servidor deverá ser entregue com no mínimo 1.024 GB (um mil e vinte e quatro gigabytes) de memória RAM, utilizando módulos DDR5 ou superior, distribuídos de forma equilibrada entre os processadores.

8.5 Especificações de Rede por Nó

8.5.1 Cada servidor deverá conter no mínimo:

8.5.1.1 2 (duas) interfaces de rede 25/10 GbE SFP28;

8.5.1.2 1 (uma) interface de gerenciamento 1000Base-T;

8.5.1.3 A interface de gerenciamento deverá ser acompanhada de cabos UTP Cat-6 ou superior, com 5 metros de comprimento e conectores RJ-45.

8.6 Especificações de Armazenamento por Nó

8.6.1 Cada servidor deverá ser entregue com:

8.6.1.1 2 discos SSD NVMe, SAS ou SATA, com capacidade mínima de 3,84 TB cada (volumetria bruta);

8.6.1.2 4 discos HDD com capacidade mínima de 12 TB cada (volumetria bruta).

8.7 Especificações de Processamento Gráfico e Cálculo Aritmético

8.7.1 Cada servidor deverá conter uma placa gráfica com as seguintes características:

8.7.1.1 48 GB de memória GDDR6 de GPU;

8.7.1.2 Interconexão PCIe Gen4 com largura de banda de 64 GB/s;

8.7.1.3 Suporte a DirectX 12.075, Shader Model 5.175, OpenGL 4.686 e Vulkan 1.186;

8.7.1.4 Compatibilidade com NVIDIA vPC/vApps, NVIDIA RTX Virtual Workstation e NVIDIA Virtual Compute Server;

8.7.1.5 Consumo máximo de 350W.

9 . ITEM 03 – SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX

9.1 Camada de Armazenamento da Solução:

9.1.1 A solução deverá contar com camada de armazenamento compartilhada entre todos os servidores e appliances descritos neste Termo, utilizando tecnologia de armazenamento definido por software (Software Defined Storage – SDS).

9.1.2 A arquitetura de armazenamento deverá ser otimizada para ambientes virtuais, com escalabilidade contínua e elástica, permitindo expansão de capacidade pela adição de novos nós/appliances sem necessidade de licenciamento adicional de virtualização.

9.1.3 Não serão aceitas soluções baseadas em tecnologia RAID para redundância de dados.

9.1.4 A solução deverá suportar as tecnologias de compressão e desduplicação de dados inline, near-line ou pós-processada, com o objetivo de otimização do armazenamento.

9.1.5 A solução deverá prover recursos de QoS (Quality of Service), para controle do volume de I/Os de VMs.

9.1.6 Deverá permitir uso de técnicas de Erasure Coding para otimização de aplicações com baixa sensibilidade à latência de escrita.

9.1.7 A solução deverá permitir a expansão do cluster através da adição de nós/servidores que incrementem tão somente a capacidade de armazenamento, sem a necessidade de emprego de licenças de virtualização nesses nós/servidores;

9.1.8 A substituição de discos defeituosos deverá ocorrer sem impacto nas operações de leitura e escrita das aplicações.

9.1.9 A falha de um nó da solução não poderá comprometer a disponibilidade da camada de armazenamento das VMs.

9.1.10 A criptografia deverá ser aplicada em nível de cluster ou volume, via hardware ou software, com KMS nativo. Caso não possua, será aceita entrega de servidor redundante externo com essa funcionalidade.

9.1.11 A distribuição dos dados deverá ocorrer de forma automática e uniforme dentro do cluster.

9.1.12 A solução deverá permitir criação de cópias no tempo (snapshots) sem movimentação dos dados originais e com redirecionamento de escritas subsequentes.

9.1.13 Deverá suportar clonagem de instâncias virtuais a partir de snapshots, sem movimentação dos dados.

9.1.14 Acesso ao armazenamento deverá ser possível via iSCSI por instâncias físicas ou virtuais externas ao cluster, garantindo suporte a aplicações de alta disponibilidade.

9.2 Tecnologia de Replicação e Proteção de Dados:

9.2.1 Deverá ser fornecida funcionalidade de replicação local realizando clones e snapshots com proteção contínua dos dados da máquina virtual.

9.2.2 A solução deve prover as funcionalidades de Thin Provisioning e Serviços de Cópias de dados.

9.2.3 Deverá permitir a configuração de um grupo ou domínio de proteção de instâncias virtuais, que poderão ser protegidas por cópias point-in-time, bem como replicadas para um cluster remoto.

9.2.4 Deverá permitir a união de máquinas virtuais em um único grupo de proteção.

9.2.5 Deverá proteger, por cópias point-in-time, simultaneamente todas as máquinas virtuais pertencentes ao grupo.

9.2.6 Deverá contemplar, também, a proteção nativa de máquinas virtuais consistentes com aplicações, onde há proteção dos dados em memória a partir da movimentação das operações de escrita para disco, de sistemas operacionais Linux e Windows. Caso a plataforma de nuvem privada não permita executar esta funcionalidade

nativamente, a CONTRATADA deverá atender este requisito compondo com outra solução.

9.2.7 Deverá permitir a configuração de uma entidade capaz de centralizar todo o fluxo do tráfego replicado entre clusters distintos, convergindo assim os recursos para um único ponto focal. Esse recurso centralizado deverá posteriormente redirecionar o tráfego corretamente para os equipamentos específicos do cluster de contingência.

9.2.8 Deverá permitir ajustar o consumo de banda em replicações.

9.2.9 Deverá permitir a existência de frequências distintas de replicação para instâncias virtuais em grupos diferentes.

9.3 Gerenciamento Integrado:

9.3.1 A solução deve oferecer solução de gerenciamento integrado, licenciado para gerenciar inclusive múltiplos clusters.

9.3.2 Monitoração automática e periódica da solução, com o envio de notificações preventivamente em caso de falhas, notificando o suporte do fornecedor a tomar medidas preventivas e acordadas com a CONTRATANTE a fim de evitar tempo de inatividade e impactos na produção.

9.3.3 Deve oferecer portal de acesso do próprio fornecedor para download de atualizações e de softwares agregados.

9.3.4 A ferramenta de gerenciamento, local, deve fornecer um dashboard reportando a utilização dos recursos do cluster como CPU, Memória, Armazenamento, IOPS do cluster, largura de banda do cluster, latência do cluster e informações sobre o virtualizador empregado e os alertas de saúde.

9.3.5 A solução deve fornecer atualização de todos os componentes (Firmware, e softwares de virtualização que fazem parte da solução) em forma de pacote com instalação assistida.

9.3.6 Contemplar as funcionalidades como:

9.3.6.1 Emissão de relatório avançados do ambiente;

9.3.6.2 Personalização da console principal;

9.3.6.3 Planejamento e previsão de capacidade;

9.3.6.4 Detecção de ineficiência de cargas de trabalho e dimensionamento ideal;

9.3.6.5 Planejamento de capacidade ou cargas de trabalho ao longo do tempo;

9.3.6.6 Permitir automação de operações de gerência do ambiente.

9.4 Provisionamento de Containers:

9.4.1 Deverá ser entregue uma plataforma de provisionamento de containers, integrada, a plataforma de virtualização.

9.4.2 A plataforma deverá permitir a criação de múltiplo clusters.

9.4.3 A fabricante da solução deverá, comprovadamente, pertencer a categoria de membro da CNCF (Cloud Native Computing Foundation).

9.4.4 Seleção de sistemas operacionais, bem como suas distintas versões de microcódigo para implementação automática, sendo compatível com sistemas Linux.

9.4.5 Seleção das configurações de rede do cluster de containers ou microserviços.

9.4.6 Seleção do tipo de armazenamento persistente a ser empregado em containers.

9.4.7 Seleção da quantidade de nós dos tipos “Control Plane” e “Workers” que serão implementados simultaneamente.

9.4.8 A plataforma de containers deverá permitir a criação de alertas, facilitando a gestão do cluster.

9.4.9 Deverá ter suporte a implementação de clusters de plataformas de containers, similares a Kubernetes, NCI, baremetal, public cloud.

9.4.10 A plataforma de containers deverá possuir integração para o acesso através de RBAC, permitindo seu uso completo através de acesso administrativo e permitindo seu uso parcial através de acesso controlado aos demais usuários.

9.4.11 Suporte implementação de clusters de plataformas de containers, similares a Kubernetes com suporte a Bring-Your-Own-OS: Rocky Linux, Ubuntu, RHEL e similares.

9.4.12 Permitir a configuração de clusters com alta-disponibilidade para os “Control Plane” nodes, com ou sem balanceador de carga;

9.4.13 Prover armazenamento persistente através de integração com Container Storage Interface (CSI), para armazenamento de blocos e arquivos. Também deverá ser possível configurar armazenamento de arquivos compatível com protocolo Simple Storage Service;

9.4.14 Deverá fornecer um mecanismo de monitoramento que aciona alertas no cluster Kubernetes;

9.4.15 Oferecer as seguintes funcionalidades em ambiente Kubernetes:

9.4.15.1 Gerenciamento de Dados;

9.4.15.2 Proteção e Restauração de Dados;

9.4.15.3 Aceleração da Entrega de Aplicativos;

9.4.15.4 Gerenciamento de Autoatendimento de Aplicativos;

9.4.15.5 Automação e Monitoramento de Infraestrutura;

9.4.15.6 Padronização de Políticas de Governança e Conformidade;

9.4.16 Para a estratégia de criação de cópias dos dados para ambiente de containers Kubernetes, a solução deverá permitir:

9.4.16.1 Fornecimento de software para “worker nodes” Kubernetes, garantindo o suporte unificado e conjunto da solução como um todo;

9.4.16.2 Plataformas de container baseadas em Kubernetes.

9.4.16.3 Permitira realização de copias e armazenamento em repositório externo.

9.4.16.4 Movimentação das imagens de backup para compartilhamentos NFS por meio de solução de armazenamento compatível com protocolo S3, permitindo que o repositório NFS seja utilizado como backend de Object Storage.

9.4.16.5 Capacidade de restaurar o Namespace para seu local original e para um novo Namespace.

9.5 Segurança de Rede:

9.5.1 Suportar microssegmentação para prover controle granular e governança de todo o tráfego de entrada e saída de uma máquina virtual (VM), grupos de máquinas virtuais (VMs) e containers.

9.5.2 Permitir a associação de políticas de rede a VMs e conteiners em vez de segmentos de rede específicos (por exemplo VLANs) ou identificadores (endereços IP ou MAC).

9.5.3 Prover visualização de tráfego e relacionamentos com a descoberta automática dos fluxos entre as máquinas virtuais e containers.

9.5.4 Permitir políticas de segurança centradas na carga de trabalho em vez de uma abordagem centrada na rede, permitindo examinar o tráfego de, e para as VMs, independentemente de como as configurações de rede mudam e onde residem no data center

9.5.5 Políticas aplicadas por categorias de VMs e containers.

9.5.6 Permitir isolamento de conteiners e VMs comprometidas, colocando-a em quarentena.

9.5.7 - Permitir restrição de tráfego entre camadas de aplicação.

9.5.8 Atualização automática de políticas.

9.5.9 Integração com ferramentas de terceiros como IDS/IPS e load balancer.

9.6 Licenciamento do Software de Virtualização:

9.6.1 Entrega do licenciamento completo da plataforma de virtualização, versão mais avançada.

9.6.2 Suporte à criação de VMs com múltiplas interfaces de rede e múltiplas arquiteturas (32/64 bits).

9.6.3 Permitir provisionamento aos principais sistemas operacionais (Windows Server 2022, CentOS 8, Ubuntu 20, RHEL 9) ou superiores.

9.6.4 Alocação dinâmica de recursos (CPU/RAM).

9.6.5 Hypervisor deverá estar instalado em unidade flash dedicada.

9.6.6 Suporte a GPU virtual ou passthrough nativo.

9.6.7 Suporte a BIOS/UEFI, snapshots, exportação OVA.

9.6.8 Deverá permitir o provisionamento de máquinas virtuais, e grupos de máquinas virtuais, em equipamentos específicos com o propósito de respeitar licenciamentos de aplicações. Em caso de falha do equipamento, a máquina virtual não deverá ser migrada para outro equipamento remanescente;

9.6.9 Alta resiliência a falhas de nós/discos.

9.6.10 Armazenamento distribuído e gerenciado via console web.

9.6.11 Deverá permitir a inicialização, a reinicialização, o reset, o desligamento da VM e o desligamento do sistema operacional dela;

9.6.12 Suportar a tecnologia de snapshot nativos do Hypervisor;

9.6.13 Permitir a adição de novos servidores no cluster;

9.6.14 Permitir criar uma área de armazenamento compartilhada, distribuída e otimizada para ambientes virtuais;

9.6.15 Permitir o agrupamento dos volumes lógicos de todos os servidores no cluster provendo uma área de armazenamento comum para o ambiente virtual;

9.6.16 Possuir mecanismo de redundância e proteção de dados nativo que armazena cópias dos dados em diversos discos e hosts do cluster de forma transparente;

9.6.17 Deverá ser fornecido licenciamento do software de virtualização na versão mais completa para todos os servidores do ambiente de armazenamento distribuído.

9.6.18 Deverá contemplar pelo menos 20 (vinte) núcleos de processamento virtuais (vCPU) ou físicos (pCPU) de solução para gestão de base de dados como serviço (DBaaS).

9.6.19 Deverá ser totalmente compatível com a solução ofertada para atendimento aos requisitos deste termo de referência.

9.6.20 Permitir automatizar as tarefas para provisionamento, emprego de correções de software (patching), gerenciamento do ciclo de vida, clonagem, atualização dos dados em bases clonadas (refresh), proteção contínua e recuperação de bases de dados.

9.6.21 Deverá ser compatível pelo menos com Oracle, Microsoft SQL, PostgreSQL, MariaDB, MongoDB e MySQL.

9.6.22 Permitir o uso de uma chave SSH pública para acesso ao servidor de banco de dados com opção através do upload de um arquivo e através da inserção direta da chave em campo de texto.

9.6.23 A solução deverá permitir registrar bancos de dados existentes para emprego de proteção contínua capturando e mantendo snapshots e registros (logs) transacionais da base de dados de origem conforme definições contidas no agendamento.

9.6.24 A mesma tecnologia deverá permitir a clonagem de bases de dados.

9.6.25 Durante a clonagem, a solução deverá permitir a escolha para o administrador utilizar um servidor de banco de dados registrado ou criar um novo servidor.

9.6.26 Permitir que o administrador realize o clone de uma base de dados a partir de um snapshot.

9.6.27 Permitir que o administrador realize o clone de uma base de dados dentro de uma política de proteção contínua, ou seja, clonar uma base de dados em determinado dia, hora, minuto e segundo.

9.6.28 Permitir a definição de agendamento da periodicidade para realizar a atualização (refresh) dos dados da base clonada através do estado atual na base de dados de origem.

9.6.29 Permitir a definição de uma data para remoção ou exclusão do

clone.

9.6.30 Permitir a execução de scripts ou comandos de pré e pós clonagem.

9.6.31 Deverá ser possível definir as políticas de retenção dos snapshots diários, semanais, mensais e trimestrais.

10. ITEM 04 – SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU

10.1 Software para Processamento Gráfico e Cálculo Aritmético:

10.1.1 Permitir a seleção, implantação e gestão de modelos de IA Generativa (LLMs) provenientes da Hugging Face e NVIDIA, bem como a importação de modelos personalizados ou treinados pelo contratante em clusters Kubernetes.

10.1.10 Permitir a criação de um endpoint de inferência e o compartilhamento dele com desenvolvedores para incorporar em seus aplicativos de IA. Permitir gerenciar e validar esses endpoints para garantir que eles estejam configurados corretamente.

10.1.11 Permitir o acesso a um endpoint de inferência por um aplicativo usando chaves de API. O gerenciamento de chaves de API deverá permitir o fornecimento e revogação do acesso à API para garantir controles de segurança de acesso adequados.

10.1.12 Permitir o controle de acesso baseado em função (RBAC), para fornecer permissões de acesso personalizadas aos usuários com base em suas funções atribuídas.

10.1.13 Possuir uma interface de usuário simples e dinâmica que simplifique o processo de implantação.

10.1.14 Possuir um painel dinâmico que permita monitorar a integridade da implantação com ferramentas de monitoramento em tempo real que identifiquem gargalos, rastreiem o desempenho e solucionem problemas.

10.1.15 Suportar a instalação e o funcionamento em estruturas sem qualquer conexão com a Internet (dark-site ou air-gapped).

11. ITEM 05 - LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE

11.1 A solução deverá incluir unidade de subscrição de software para armazenamento de objetos e arquivos, licenciada por terabyte (TB), com suporte técnico durante 60 (sessenta) meses, contemplando ambiente de produção em operação contínua (24x7).

11.2 Caso a solução proposta não ofereça suporte nativo a armazenamento de objetos e arquivos, será permitida a utilização de unidade externa dedicada, desde que esta disponha de todos os componentes, funcionalidades e suporte equivalentes à solução principal.

11.3 O sistema de armazenamento definido (SDS) deverá otimizar dados utilizando tecnologia de erasure coding na camada de capacidade, de modo a garantir eficiência e resiliência no armazenamento de arquivos e objetos.

11.4 A solução deverá permitir a recuperação granular de arquivos pelos usuários, sem necessidade de intervenção do administrador.

11.4.1 Para o protocolo SMB, a restauração deverá ocorrer por meio

da funcionalidade “Versões Prévias” da pasta de destino.

11.4.2 Para o protocolo NFS, a recuperação deverá ser possível pela listagem do subdiretório oculto (snapshot).

11.5 O sistema deverá integrar-se a softwares antivírus de terceiros por meio do protocolo ICAP (Internet Content Adaptation Protocol), possibilitando varredura em tempo real de arquivos compartilhados via SMB sempre que forem abertos, modificados ou encerrados.

11.6 A interface de gerenciamento deverá exibir o estado dos arquivos após a varredura antivírus, incluindo status como limpo, em quarentena ou deletado, além do histórico de eventos correspondentes.

11.7 A interface de gerenciamento deverá também exibir relatórios detalhados contendo a lista de arquivos analisados, ameaças detectadas e arquivos colocados em quarentena.

11.8 A interface de gerenciamento deverá permitir ações diretas sobre os arquivos, incluindo:

11.8.1 Reexecução de varredura (Rescan);

11.8.2 Remoção de arquivos da quarentena;

11.8.3 Exclusão permanente de arquivos em quarentena.

11.9 A solução deverá possibilitar a configuração de ambiente de detecção avançada de intrusão (AIDE), capaz de identificar e corrigir automaticamente desvios na configuração de segurança do servidor de arquivos, sem necessidade de intervenção manual.

11.10 Deverá ser possível configurar políticas de senha forte (strong password) para o acesso à linha de comando (CLI) do servidor de arquivos.

11.11 O sistema deverá suportar configuração de qualidade de serviço (QoS), utilizando valores DSCP para diferenciação de códigos de serviço em rede.

11.12 Deverá suportar o protocolo NFS v4.2, otimizando as operações de entrada/saída (I/O) e reduzindo o consumo de rede.

11.13 A solução deverá contemplar as seguintes funcionalidades para compartilhamento de arquivos via protocolo SMB:

11.14 Autenticação integrada ao Active Directory.

11.15 Enumeração baseada em acesso (ABE), exibindo apenas pastas e arquivos aos quais o usuário possui permissão.

11.16 Assinatura digital de pacotes SMB (SMB Signing), garantindo autenticidade e integridade das transmissões.

11.17 Criptografia em nível de pasta (SMB Encryption), assegurando a confidencialidade dos dados.

11.18 Organização de compartilhamentos em um único espaço de nomes (Single Namespace), suportando ambientes locais ou geograficamente distribuídos, por meio do protocolo DFS-N (DFS Namespaces).

11.19 Suporte à autenticação via Active Directory e LDAP, além de acesso não gerenciado a compartilhamentos NFSv4 (autenticação LDAP) e NFSv3.

11.20 Suporte a acesso multiprotocolo (SMB e NFS) sobre o mesmo compartilhamento, preservando permissões via Windows ACLs e Unix mode bits.

11.21 Suporte a Home Shares por diretório, permitindo o provisionamento automático de pastas pessoais de usuário.

11.22 Suporte à aplicação de cotas de uso do sistema de arquivos, com notificações (soft limit) e bloqueio (hard limit), configuráveis por usuário, grupo ou diretório no momento da criação (Directory Level Quotas).

11.23 O módulo de armazenamento de objetos deverá possuir API REST compatível com AWS S3, apta a lidar com petabytes de dados não estruturados, atendendo casos de uso como backup, retenção de longo prazo e aplicações nativas de nuvem.

11.24 Deverá permitir que os usuários armazenem e gerenciem dados não estruturados em arquitetura de nuvem privada escalável.

11.25 A solução deverá permitir a gestão de objetos via interface gráfica de administração e via API REST compatível com S3, mediante autorização prévia do administrador.

11.26 Suportar integração com serviços de diretório (Microsoft Active Directory e OpenLDAP), possibilitando o controle de acesso a objetos.

11.27 Permitir o compartilhamento de buckets com usuários portadores de chaves de acesso, com delegação de permissões de leitura e escrita conforme o nível definido.

11.28 Exibir a listagem de buckets compartilhados, indicando os respectivos usuários com acesso.

11.29 Permitir o gerenciamento de buckets e objetos por meio de APIs REST compatíveis com a solução de gerenciamento central ou S3, mediante autorização administrativa.

11.30 Suportar o versionamento de múltiplas versões de um mesmo objeto dentro de um bucket.

11.31 Possibilitar a definição de regras de ciclo de vida, como exclusão automática de objetos ou versões após período determinado (dias, meses ou anos).

11.32 Implementar mecanismo de proteção contra exclusão ou alteração de objetos, com base em políticas de retenção WORM (Write-Once-Read-Many).

11.33 Disponibilizar painel de monitoramento de desempenho, apresentando requisições por segundo, taxa de banda (MB/s) e tempo médio de leitura (GET).

11.34 Suportar políticas de cotas de utilização, notificando usuários conforme o consumo de espaço ou número de buckets criados.

11.35 Suportar o envio de notificações em tempo real — como criação, deleção, leitura, gravação ou alteração de permissões — para fins de auditoria e retenção, compatível com servidores syslog ou sistemas equivalentes.

12. ITEM 06 - SOFTWARE DE BACKUP DE DADOS

12.1 Características Gerais do Licenciamento:

12.1.1 Aquisição de 200 (duzentas) licenças pelo período de 05 (cinco) anos ou 60 (sessenta) meses.

12.1.2 Não deverão existir limites quanto ao uso de agentes, conectores, repositórios de armazenamento, hosts físicos e outras

tecnologias agregadas a arquitetura da solução especificada.

12.1.3 Ser a última versão disponível, não será aceita a utilização de versões anteriores para cobrir algum item desse descritivo técnico.

12.1.4 Mostrar na console de gerenciamento a quantidade de licenças adquiridas e utilizadas.

12.1.5 Caso a solução ofertada necessite de algum banco de dados, o mesmo deverá ser fornecido devidamente licenciado sem nenhum custo extra.

12.1.6 A solução deve ser compatível com o Item 07 Equipamento de Armazenamento de Dados de Backup on-premises.

12.2 Cópia e Restauração de Dados:

12.2.1 Permitir o controle da banda utilizada durante a operação de cópia de proteção dos backups.

12.2.2 Ser capaz de realizar cópia de arquivos abertos sem que a consistência deles seja comprometida.

12.2.3 Possuir a opção de priorização de tarefas de proteção com opção de resumo da cópia caso uma atividade de menor prioridade seja colocada em estado de espera por uma tarefa de maior prioridade.

12.2.4 Possuir a funcionalidade de paralelizar a gravação dos dados em dispositivos de armazenamento (funcionalidade conhecida como multiplexação).

12.2.5 Ser capaz de enviar alertas através de e-mail com o objetivo de reportar eventos ocorridos na operação e configuração da solução.

12.2.6 Ser capaz de enviar traps SNMP (Simple Network Management Protocol) com o objetivo de reportar eventos ocorridos na operação da solução.

12.2.7 Possuir a funcionalidade de agendamento automático de tarefas de cópia.

12.2.8 Para um mesmo dado armazenado deve haver a possibilidade de configuração de diferentes períodos de retenção.

12.3 Gerenciamento das Operações de Proteção e Restauração:

12.3.1 Possuir interface única, que seja capaz de gerenciar e executar operações de proteção e recuperação dos sistemas operacionais Windows, Unix e Linux; ambiente de virtualização Acropolis Operating System; aplicações, Microsoft Active Directory e banco de dados Microsoft SQL Server, PostgreSQL e Oracle.

12.3.2 O acesso administrativo ao console do servidor de gerenciamento da solução poderá ser feito através de ferramenta disponibilizada no próprio software (console gráfico) ou através de navegador Web.

12.3.3 Implementar distribuição automática de carga entre os movimentadores de dados, ou seja, os dados oriundos dos clientes de backup deverão ser distribuídos de forma automática entre os servidores de cópia, e em caso de falha de um dos servidores, o cliente automaticamente irá encaminhar seus dados para o outro servidor de cópia ativo. Esta funcionalidade deverá ser nativa do

produto, e não pode ser construída com o uso de soluções baseadas em softwares de cluster de terceiros.

12.3.4 A base de dados para armazenamento do catálogo deverá possuir mecanismo de proteção (backup) das informações armazenadas no catálogo e funcionalidades de recuperação rápida do catálogo em caso de desastre.

12.4 Criptografia dos Dados Protegidos

12.4.1 Implementar criptografia de dados na origem (cliente de backup), de uma forma que seja garantido que o dado que trafegará na rede de modo criptografado.

12.4.2 Deverá implementar no mínimo chaves de criptografia de 128 bits ou 256 bits.

12.5 Desduplicação dos Dados Protegidos

12.5.1 Permitir uso da tecnologia de desduplicação de dados para toda a capacidade licenciada, eliminando blocos repetidos, para cópias e arquivamento em disco e movimentação de dados desduplicados, independentemente do quantitativo de dispositivos de armazenamento que compõem a infraestrutura da CONTRATANTE.

12.5.2 Implementar desduplicação de blocos na origem (client-side desduplication), de forma que o cliente envie apenas novos blocos de dados criados e/ou modificados a partir da última cópia total completa;

12.5.3 Implementar desduplicação de dados nos servidores de armazenamento (target desduplication), de forma que tais servidores tratem adequadamente blocos repetidos enviados pelos clientes, evitando assim o armazenamento de blocos redundantes;

12.5.4 Implementar desduplicação de dados em tarefas de cópia;

12.5.5 Implementar desduplicação e compressão em uma mesma tarefa;

12.5.6 Permitir a restauração granular de arquivos ou sistemas de arquivos a partir de cópias em disco ou fita. Em caso de backup armazenado em disco a recuperação granular poderá ser feito utilizando-se cópias que possam estar desduplicados;

12.6 Alertas e Relatórios da Proteção de Dados

12.6.1 Quantidade de rotinas de backup concluídos nas últimas 24 horas, nos últimos 30 dias e nos últimos 12 meses.

12.6.2 Quantidade de recuperações efetuadas nas últimas 24 horas, nos últimos 30 dias e nos últimos 12 meses.

12.6.3 Resumo de rotinas de backup concluídos com sucesso, com erro ou não concluídos.

12.6.4 Mostrar o total de licenças adquiridas e o total de licenças utilizadas e caso ocorra uma nova aquisição de licenças as novas licenças deverão constar nesse relatório.

12.6.5 Enviar os seguintes alertas via e-mail: rotina de backup finalizada com sucesso, rotina de backup finalizada com erro e rotina de backup com problema.

12.7 Fornecimento de licenciamento do Sistema Operacional

12.7.1 Fornecimento de licenciamento do sistema operacional Microsoft Windows Server Datacenter, baseado em núcleo (core-based licensing , para 48 cores físicos).

12.7.2 As licenças deverão ser entregues em formato eletrônico, acompanhadas de instruções para instalação e ativação, devendo incluir garantia mínima de 60 (sessenta) meses ou suporte técnico equivalente.

12.7.3 O licenciamento deverá ser compatível com servidores físicos e virtuais , observando o licenciamento mínimo exigido pela fabricante.

12.7.4 As licenças fornecidas deverão ser originais, legítimas e adquiridas por meio de canal autorizado da Microsoft, com comprovação documental no momento da entrega.

12.7.5 As licenças deverão ser entregues em formato eletrônico, acompanhadas de instruções para instalação e ativação, incluindo garantia mínima de 60 (sessenta) meses ou suporte técnico equivalente.

12.7.6 O item deverá ser plenamente compatível com a infraestrutura tecnológica do MPAM, em especial com ambientes físicos e virtuais já existentes.

12.7.7 Incluir Software Assurance (SA), garantindo direito a atualizações, suporte técnico estendido e benefícios de mobilidade de licenças durante todo o período contratual.

13. ITEM 07 - EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES

13.1 Características gerais:

13.1.1 Deverá corresponder a um sistema inteligente dedicado ao armazenamento de backups em disco, com funcionalidades integradas de criptografia, compressão, desduplicação e replicação dos dados já desduplicados;

13.12 O equipamento deve estar listado no site oficial do fabricante como um appliance ou sistema de armazenamento de backup em disco, em produção ativa;

13.1.3 O hardware e o software devem ser do mesmo fabricante. Não serão aceitas soluções customizadas especificamente para esta licitação, nem combinações OEM, equipamentos usados, recondicionados, de demonstração ou gateways;

13.1.4 O equipamento deve ser novo, sem uso anterior, pertencente à linha mais recente do fabricante, em produção contínua e sem previsão de fim de suporte (EOSL) nos próximos cinco anos a partir da data de abertura da licitação;

13.1.5 Soluções baseadas exclusivamente em software (appliances virtuais) não serão aceitas;

13.1.6 Deve ser compatível com montagem em racks padrão de 19”, acompanhado de trilhos, cabos, conectores, manuais e todos os itens necessários para instalação, configuração e operação completa;

13.1.7 Para soluções com arquitetura Scale-Out:

13.1.7.1 Deve permitir conexão com outros sistemas do mesmo

fabricante para expansão de desempenho e capacidade;

13.1.7.2 Deve operar em modo ativo-ativo (alta disponibilidade com balanceamento de carga), redirecionando automaticamente os backups em caso de falha de um dos sistemas;

13.1.8 Para soluções com arquitetura Scale-Up:

13.1.8.1 Deve incluir duas controladoras, operando em modo ativo-ativo ou ativo-passivo, garantindo continuidade das operações de backup em caso de falha de uma das controladoras.

13.2 Requisitos de disponibilidade:

13.2.1 Deve possuir tolerância a falhas em componentes como discos, fontes de alimentação e ventiladores;

13.2.2 Deve contar com mecanismos que assegurem a integridade dos dados mesmo em casos de interrupção abrupta ou desligamento acidental;

13.2.3 Deve incluir proteção de cache de escrita para evitar perda de dados em caso de falha de energia;

13.2.4 Deve ser entregue com arranjos RAID-6, RAID-DP ou equivalente, com tolerância a falha de até dois discos e pelo menos um disco hot-spare por grupo RAID;

13.2.5 Os discos devem ser hot-pluggable e hot-swappable, permitindo substituição sem interrupção do sistema;

13.2.6 Deve oferecer monitoramento remoto pelo fabricante, com recursos como Call-Home para detecção proativa de falhas ou pré-falhas.

13.3 - Capacidade, desempenho e conectividade:

13.3.1 Deve oferecer no mínimo 100 (cem) TB de capacidade útil, sem considerar compressão, desduplicação ou espaço reservado ao sistema;

13.4 Para soluções Scale-Out:

13.4.1 Deve atingir taxa mínima de 5 TB/hora (cinco terabytes por hora) para operações de backups, sem considerar desduplicação;

13.4.2 Capacidade de ampliar a solução previamente fornecida, através da interconexão de módulos similares ou não, do mesmo fabricante. Para a expansão, volumes em nuvem, off-site, replicação ou similar para o atendimento a este requisito não serão aceitos, mantendo a característica de desduplicação global da solução.

13.4.3 A criptografia deve ser feita via hardware. Caso seja por software, a taxa de transferência deve ser 30% superior à mínima exigida, considerando apenas a desduplicação.

13.5 Para soluções Scale-Up:

13.5.1 Deve permitir expansão para pelo menos 500 TB (quinhentos terabytes) de capacidade útil, sem considerar compressão ou desduplicação, por meio de gavetas de discos, sem troca ou upgrade das controladoras originais, mantendo a desduplicação global;

13.5.2 Deve atingir taxa mínima de 15 TB/hora (quinze terabytes por hora) para operações de backup, considerando apenas a

desduplicação;

13.5.3 A criptografia deve ser realizada por hardware. Se for por software, a taxa de transferência deve ser 30% superior à exigida, considerando apenas a desduplicação;

13.5.4 Deve incluir no mínimo duas interfaces de rede de 25 Gbps com conectores SFP28 para backup via LAN, fornecidos com o equipamento;

13.5.5 Deve incluir pelo menos duas interfaces de 1 GbE com conectores UTP CAT6 para gerenciamento, também fornecidos;

13.5.6 Deve possuir ao menos uma porta IPMI/iLO/iDRAC ou equivalente;

13.5.7 Interfaces adicionais devem ser fornecidas conforme as melhores práticas do fabricante para garantir o desempenho requerido;

13.5.8 Fornecer a quantidade necessária de discos para atingimento da performance mínima solicitada, ou seja, se a solução requerer mais discos além dos necessários para atender a capacidade solicitada no item 8.3.1, discos adicionais deverão ser fornecidos. Não é obrigatório o licenciamento de capacidade desses discos adicionais

13.5.9 Comprovar a taxa de transferência através da ferramenta de dimensionamento do fabricante da solução, desconsiderando o uso de ferramentas/protocolos de otimizações na origem no seu dimensionamento, caso a solução ofertada não seja fornecida com todos os discos possíveis para sua capacidade total.

14. ITEM 08 - SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES

14.1 Características gerais

14.1.1 Permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, de maneira perpétua, irrestrita e sem necessidade de licenciamentos ou ônus adicionais;

14.1.2 -Possuir licenças na modalidade de uso perpétuo para todo para o completo atendimento das especificações técnicas do equipamento, ou seja, o equipamento deverá continuar a operar normalmente mesmo após o período de manutenção e assistência técnica contratado;

14.1.3 Para soluções com arquitetura Scale-Out:

14.1.3.1 A desduplicação de dados deve ser mantida de forma global em todo o ambiente de armazenamento, independentemente da quantidade de dispositivos interligados;

14.1.4 Para soluções com arquitetura Scale-Up:

14.1.4.1 A desduplicação global deve ser preservada em todo o conjunto de armazenamento.

14.2 Requisitos de compatibilidade:

14.2.1 O software deve ser homologado e plenamente compatível com o software de backup fornecido no ITEM 06 - SOFTWARE DE BACKUP DE DADOS;

14.2.2 Deve permitir leitura e gravação simultâneas via protocolos

CIFS, NFS e OST;

14.2.3 Deve oferecer suporte aos protocolos de monitoramento SNMP e Syslog;

14.2.4 Deve possibilitar que aplicações como Oracle (via RMAN) e Microsoft SQL realizem backups tipo Stream Based (Oracle Stream Backup) e “database dump” diretamente no equipamento, por meio de CIFS e NFS, sem uso de software de backup, evitando o consumo de licenças e sem necessidade de licenciamento por volume (TB) ou por servidor (CPU, Core, Tier). Caso essa funcionalidade exija licenciamento, todos os itens necessários devem ser incluídos na proposta.

14.3 - Funcionalidades operacionais:

14.3.1 Deve permitir a execução simultânea de processos de backup e restore;

14.3.2 Deve dispor de interface de gerenciamento baseada em navegador (WEB);

14.3.3 A desduplicação deve ser global, mesmo com volumes lógicos distintos, identificando dados redundantes entre diferentes fontes de backup e armazenando-os apenas uma vez;

14.3.4 A desduplicação deve ocorrer em conjunto com os processos de backup e restore, sem necessidade de janelas específicas;

14.3.5 Deve incluir mecanismos nativos para verificação da integridade dos dados desduplicados, com capacidade de correção automática em caso de inconsistência, sem uso de scripts externos;

14.3.6 Deve permitir replicação de dados via rede IP (LAN/WAN), de forma assíncrona, entre sistemas compatíveis do mesmo fabricante, utilizando desduplicação para otimizar o uso da banda;

14.3.7 Deve suportar topologias de replicação como 1:1, 1:N, N:1 e o cascateamento de equipamentos;

14.3.8 Deve integrar-se ao Microsoft Active Directory 2012 ou superior, para autenticação e controle de acesso;

14.3.9 Os dados armazenados devem ser criptografados com algoritmos de no mínimo AES128-SHA ou AES256-SHA;

14.3.10 Deve permitir autenticação em dois fatores (2FA), com integração a soluções OTP como Google Authenticator, Microsoft Authenticator ou equivalentes;

14.3.11 Caso a solução exija um sistema OTP específico com licenciamento ou hardware dedicado (ex: Common Access Card /Personal Information Verification cards, sistemas de OTP/tokenização licenciados, etc), todos os componentes necessários devem ser fornecidos para pelo menos 5 usuários;

14.3.12 Deve oferecer recurso de autorização dupla (Dual Auth) para alterações em configurações de proteção contra ransomware;

14.3.13 Deve incluir funcionalidades avançadas de segurança cibernética para proteção contra ransomware, assegurando a integridade dos dados de backup;

14.4 - Deve possuir mecanismo de imutabilidade dos dados:

14.4.1 A proteção deve estar sempre ativa, independente do software de backup, sem necessidade de janelas específicas ou scripts;

14.4.2 A proteção deve ser aplicada imediatamente após a desduplicação dos dados, sem depender de agendamento;

14.4.3 Deve adotar o conceito de air-gap, tornando os dados protegidos invisíveis à rede e inacessíveis por softwares de backup, independentemente do protocolo utilizado.

15. ITEM 09 – SWITCH CORE

15.1 Especificações Físicas

15.1.1 O equipamento deve contar com, no mínimo, 48 portas SFP28 compatíveis com velocidades de 1, 10 e 25 Gigabit Ethernet.

15.1.2 As interfaces devem ser auto-sensíveis, ajustando automaticamente a velocidade conforme o transceiver conectado, sem necessidade de configuração manual.

15.1.3 A altura máxima permitida é de 1 unidade de rack (1 RU).

15.1.4 Deve ser compatível com racks padrão de 19 polegadas, incluindo os kits de fixação apropriados.

15.1.5 As portas SFP28 devem aceitar transceivers dos tipos SFP+ 10GBase-SR, 10GBase-LR, 10GBase-ER, SFP 1000Base-SX, 1000Base-LX, 1000Base-ZX, 1000Base-T e cabos DAC.

15.1.6 Devem ser entregues ao menos 10 cabos DAC 25GbE SFP28 com comprimento mínimo de 3 metros, compatíveis com os appliances do item 1.

15.1.7 O switch deve possuir pelo menos 6 portas QSFP28 de 100GbE, com suporte a velocidades de 40GbE.

15.1.7.1 Deve ser compatível com transceivers 40GBase-SR4 e 40GBase-LR4.

15.1.7.2 Deve aceitar transceivers 100GBase-SR4 e 100GBase-LR4.

15.1.7.3 Deve suportar cabos DAC.

15.1.8 Deve acompanhar pelo menos 1 cabo DAC 100GbE com no mínimo 1 metro de comprimento, para conexão redundante entre switches.

15.1.9 A capacidade da matriz de comutação deve ser de no mínimo 4 Tbps.

15.1.10 O throughput mínimo exigido é de 1,5 Bpps.

15.1.11 O buffer deve ter capacidade mínima de 32 MB.

15.1.12 A latência máxima permitida é de 900 nanosegundos.

15.1.13 Deve suportar ao menos 160.000 endereços MAC.

15.1.14 A tabela ARP deve comportar até 64.000 entradas ou mais.

15.1.15 Deve aceitar jumbo frames com tamanho mínimo de 9000 bytes.

15.1.16 É obrigatória a presença de pelo menos uma porta RJ-45 para gerenciamento fora de banda.

15.1.17 O equipamento deve vir com CPU e memória (RAM e Flash) suficientes para suportar todas as funcionalidades descritas.

15.1.18 Fontes de alimentação internas devem ser redundantes e com ajuste automático para 110/220V.

15.1.19 O sistema de ventilação deve ser redundante, com fluxo de ar configurável (frontal-traseiro ou traseiro-frontal), sendo fornecido com ventiladores de fluxo frontal-traseiro.

15.1.20 Fontes e ventiladores devem ser hot-swappable e redundantes, permitindo substituição sem interrupção.

15.1.21 O equipamento deve ser projetado para ambientes de datacenter, com comutação de pacotes de alto desempenho.

15.2 - Funcionalidades Gerais

15.2.1 LEDs por porta devem indicar status e atividade do link.

15.2.2 A arquitetura da solução deve ser baseada em “spine-leaf”, com VxLAN como plano de dados e BGP EVPN como plano de controle.

15.2.3 Deve possuir porta de console para configuração via CLI, com conector RJ-45 ou RS-232, incluindo cabos e adaptadores necessários.

15.2.4 Gerenciamento via SSHv2 deve ser suportado.

15.2.5 O switch deve ter criptografia FIPS 140-2 validada pelo NIST.

15.2.6 Deve permitir espelhamento de uma ou mais portas para outra porta específica.

15.2.7 Também deve permitir espelhamento para porta remota via tunelamento, mesmo em domínios L2 distintos.

15.2.8 Deve implementar Netflow, sFlow ou tecnologia equivalente.

15.2.9 Gerenciamento via SNMPv3 deve ser possível.

15.2.10 Deve suportar o protocolo Syslog.

15.2.11 Deve implementar NTPv4 ou SNTP.

15.2.12 Autenticação via RADIUS deve ser suportada.

15.2.13 Autenticação via TACACS+ também deve ser suportada.

15.2.14 Controle de acesso por porta (IEEE 802.1x) deve estar presente.

15.2.15 Deve haver controle de broadcast, multicast e unicast por porta.

15.2.16 Deve implementar pelo menos uma fila de saída com prioridade estrita (SP Strict Priority) e divisão de banda ponderada (WRED, WRR ou similar).

15.2.17 Deve classificar, marcar e priorizar tráfego com base em IEEE 802.1p CoS.

15.2.18 Deve classificar, marcar e priorizar tráfego com base em DSCP (Differentiated Services CodePoint), conforme IETF.

15.2.19 Deve permitir classificação de tráfego por IP, portas TCP/UDP e endereços MAC.

15.3 - Virtualização de Switch

15.3.1 Deve permitir agregação de portas multi-chassi com redundância ativa/ativa sem Spanning Tree, usando MLAG, MC-LAG, M-LAG, VLT (Virtual Link Trunking), Multi-Chassis EtherChannel ou equivalentes.

15.3.2 Todos os componentes necessários para alta disponibilidade devem ser fornecidos, incluindo cabos, transceivers e licenças.

15.3.3 Em modo virtualizado, os switches devem operar com processamento local, sem tempo de convergência em caso de falha.

15.4 - Funcionalidades de Camada 2

15.4.1 Suporte a até 4.000 VLANs conforme IEEE 802.1Q.

15.4.2 Implementação de VLAN Trunking conforme IEEE 802.1Q, com controle de VLANs permitidas por tronco.

15.4.3 Suporte a Link Aggregation (LAG) conforme IEEE 802.3ad.

15.4.4 Deve suportar no mínimo 80 grupos LAG com até 16 portas cada.

15.4.5 Implementação dos padrões IEEE 802.1d, 802.1s e 802.1w.

15.4.6 Deve possuir mecanismo de proteção da root bridge do Spanning Tree.

15.4.7 Deve permitir bloqueio de BPDUs em portas em modo fast forwarding, com desativação automática ao recebê-los.

15.4.8 Implementação de LLDP e LLDP-MED para descoberta de vizinhos.

15.4.9 Suporte a DCB com PFC (IEEE 802.1Qbb), ETS (IEEE 802.1Qaz) e DCBx.

15.5 - Funcionalidades de Roteamento

15.5.1 Deve realizar roteamento de camada 3 entre VLANs.

15.5.2 Suporte ao protocolo OSPFv3.

15.5.3 Suporte ao protocolo BGPv4.

15.5.4 Capacidade para no mínimo 106.000 rotas IPv4.

15.5.5 Capacidade para no mínimo 52.000 rotas IPv6.

15.5.6 Operação simultânea com IPv4 e IPv6.

15.5.7 Implementação de VRF ou VRF-Light.

15.5.8 Suporte a roteamento baseado em políticas (PBR).

15.5.9 Implementação do protocolo VRRPv3.

CLÁUSULA TERCEIRA – DA IMPLANTAÇÃO DA SOLUÇÃO E SERVIÇOS CORRELATOS:

A **CONTRATADA** será responsável por toda a instalação e configuração dos equipamentos, firmwares e softwares, incluindo o fornecimento de quaisquer itens adicionais necessários à sua execução.

1. A instalação poderá ser realizada integral ou parcialmente pelo fabricante, devendo a **CONTRATADA** prever esses serviços em sua proposta.
2. A **CONTRATADA** deverá disponibilizar técnicos certificados pelo fabricante,

habilitados a instalar, operar e configurar os equipamentos fornecidos. Caso a instalação seja conduzida diretamente pelo fabricante, essa exigência estará dispensada.

3. A **CONTRATANTE** reserva-se o direito de solicitar a substituição parcial ou total da equipe da **CONTRATADA** durante a fase de implantação, caso seja constatada a ausência de qualificação técnica adequada.

4. Deverá ser apresentado cronograma de implantação e proposta de configuração da solução, ambos sujeitos à aprovação da equipe técnica da **CONTRATANTE**.

5. Ao final da instalação, deverão ser entregues, em meio digital, os manuais e procedimentos utilizados.

6. A instalação deverá incluir, no mínimo:

a) Fixação dos equipamentos em rack padrão 19”;

b) Conectorização elétrica e energização dos equipamentos;

c) Atualização de firmwares de todos os componentes (BIOS, Gerência Out of Band, controladoras HBA, interfaces de rede, discos, etc.);

d) Atualizações e releases disponíveis no site oficial;

e) Registro dos equipamentos e licenças no portal do fabricante.

f) Conectorização das interfaces de rede com os respectivos cabos/conectores;

g) Instalação, atualização e configuração dos componentes conforme boas práticas;

h) Integração dos equipamentos à rede da **CONTRATANTE**;

i) Outras atividades correlatas para garantir a operação da solução no ambiente da **CONTRATANTE**.

7. A aceitação dos itens do objeto contratado no ato da sua entrega ao Ministério Público do Estado do Amazonas será considerada como de caráter provisório. A aceitação definitiva dar-se-á após a instalação e configuração dos itens do objeto e a verificação do atendimento às especificações técnicas constantes deste instrumento.

8. Serão recusados os objetos imprestáveis ou defeituosos, que não atendam as especificações constantes neste termo de referência e/ou que não estejam adequados para uso.

9. Os itens deverão ser instalados, configurados e ativados pela **CONTRATADA** em local indicado pelo DTIC do MPAM.

10. O prazo para conclusão da instalação e configuração dos equipamentos e softwares será de até 30 (trinta) dias, contados a partir da data do recebimento provisório dos mesmos pela DTIC e emissão do termo provisório de recebimento.

11. Os equipamentos e serviços serão aceitos se, e somente se, houver comprovação de que todos os requisitos técnicos especificados neste contrato tenham sido atendidos e os itens se encontre em operação plena. Essa comprovação será feita mediante observação direta das características dos equipamentos, consulta à documentação técnica fornecida e verificação dos serviços de instalação e configurações.

12. Os serviços de instalação, configuração, migração e transferência de conhecimento técnico deverão ser realizados conforme especificado em cada

item.

13. O serviço de instalação e configuração tem a finalidade de garantir que os itens fornecidos estejam operacionais no ambiente de Produção, e de Contingência caso exista.

14. Todos os serviços de instalação, configuração, migração e transferência de conhecimento técnico deverão ser executados de forma presencial, por especialista(s) técnico(s) certificado(s) nos componentes pelo fabricante dos mesmos com a devida apresentação de certificado(s) técnico(s) emitido(s) pelo fabricante do(s) produto(s).

15. Os serviços de instalação, configuração, migração e transferência de conhecimento técnico, deverão ser agendados previamente entre as partes, através de e-mail ou telefone, e deverão ser realizados em dias úteis e em horário de expediente do MPAM.

16. A transferência de conhecimento técnico será feita através de treinamento referente aos componentes do objeto deste instrumento, abrangendo todos os recursos de hardware e software do ambiente, para até 10 (dez) técnicos designados pela **CONTRATANTE**, cobrindo no mínimo os seguintes tópicos:

a) Instalação.

b) Configuração básica e avançada.

c) Operação básica e avançada.

d) Gerenciamento da solução/expansão.

e) Administração.

f) Solução de problemas (troubleshouting).

g) Laboratório prático baseado na solução/expansão adquirida.

17. O treinamento deverá ser realizado nas seguintes condições:

a) Deverá ser ministrado em língua portuguesa do Brasil, de forma presencial;

b) Local: Av. Coronel Teixeira, nº 7.995, Nova Esperança II, CEP. 69037-473, Manaus-AM;

c) Carga horária mínima de 30 (trinta) horas, divididas em, no máximo, 4 (quatro) horas diárias;

d) O conteúdo programático deverá ser aprovado pela DTIC antes da realização de cada treinamento.

18. O material didático e os certificados deverão ser disponibilizados pela **CONTRATADA** com finalidade específica para ministrar o treinamento à DTIC.

19. Ao final do treinamento, os participantes deverão estar aptos a operar e administrar as tecnologias referenciadas neste instrumento.

20. A transferência de conhecimento técnico deverá ocorrer no período correspondente ao recebimento definitivo da expansão, ou em caso de impedimento justificado, em nova data aceita pela fiscalização do contrato.

21. Caberá ainda a **CONTRATADA** a execução de todas as atividades, bem como o fornecimento de todos os materiais necessários e suficientes para a instalação e configuração dos equipamentos fornecidos.

22. O planejamento, instalação, configuração e migração dos equipamentos deverão ser executados por técnicos habilitados e credenciados pelo fabricante.

23. A **CONTRATADA** deverá designar um profissional Técnico Responsável para acompanhar a execução dos serviços desde o planejamento até a implantação da expansão.

24. Antes da implantação dos equipamentos, a equipe técnica da **CONTRATADA** deverá apresentar o cronograma da implantação contendo: o plano de instalação, plano de contingência e prazos máximos para a realização da mudança.

25. A **CONTRATADA** deverá realizar a migração completa do ambiente computacional atualmente em operação para a nova infraestrutura fornecida, incluindo, mas não se limitando a: máquinas virtuais, clusters Kubernetes, bancos de dados, configurações nativas, políticas de segurança, integrações existentes e demais componentes necessários para garantir a continuidade dos serviços. A migração deverá ser executada de forma planejada, segura e sem impacto significativo na disponibilidade dos sistemas, observando as melhores práticas recomendadas pelo fabricante e garantindo a integridade dos dados e das aplicações.

26. A **CONTRATADA** deverá prover PDU´s ou réguas smart adequadas para a devida conecção elétrica necessária dos equipamentos específicados neste contrato.

27. Após a conclusão das atividades de instalação, configuração, migração e pré-operação, deve ser iniciada a fase de operação assistida do objeto contratado.

28. A operação assistida terá duração total de 90 (noventa) dias corridos, sendo 15 (dias) dias corridos de forma presencial, e o restante do período podendo ser de forma remota, de modo a assegurar o auxílio e pronta ação corretiva da **CONTRATADA** necessária em questões relacionadas com a configuração, monitoramento e estabilização da nova solução com o objetivo de garantir o bom funcionamento dos equipamentos e serviços.

29. Durante a fase de operação assistida, a **CONTRATADA** deverá atuar de maneira a mitigar os riscos decorrentes da transição tecnológica da plataforma atualmente existente para a nova solução.

30. As atividades de operação assistida devem ser realizadas somente nas dependências da sede do MPAM em Manaus-AM, em horário de expediente da Procuradoria-Geral, e devem se iniciar logo após a migração tecnológica, testes e ativação dos serviços. Caso seja necessária a consecução de atividades que possam afetar a disponibilidade dos serviços, as atividades de operação assistida podem ser prolongadas após o horário de expediente da Procuradoria-Geral, sem qualquer ônus para o MPAM.

31. O período de operação assistida deve englobar, dentre outras, as seguintes atividades:

a) Monitoramento de funcionamento e da capacidade dos serviços;

b) Identificação e abertura de chamados técnicos para solução de falhas na solução;

c) Resolução de problemas (troubleshooting);

d) Análise da efetividade de regras e configurações;

e) Simulação de abertura de chamados;

f) Instalação de patches;

g) Execução/revisão de procedimentos de backup e restore de

configurações;

h) Geração de relatórios técnicos, administrativos e gerenciais;

CLÁUSULA QUARTA – DA VIGÊNCIA:

O presente contrato tem vigência de **60 (sessenta) meses**, contados da data de publicação do extrato no Diário Oficial do MPAM, nos termos dos arts. 105, caput, e 106, caput, da Lei n.º 14.133/2021, podendo ser prorrogado por comum acordo entre as partes, mediante termo aditivo.

1. A **CONTRATADA** terá o prazo de 5 (cinco) dias úteis para rubricar o contrato ou seus aditivos, contados a partir da data em que ela for notificada dessa providência pela Divisão de Contratos e Convênios (DCCON) da **CONTRATANTE**.

1.1 A assinatura contratual será efetuada por meio do Sistema Eletrônico de Informações (SEI) da **CONTRATANTE**.

1.2 Na hipótese de assinatura de termo aditivo de prorrogação, caso o prazo de expiração da avença for menor que o disposto no item 1 desta cláusula, a **CONTRATADA** deverá rubricar o instrumento até o último dia útil da vigência contratual.

1.3 Se a **CONTRATADA**, regularmente notificada pela DCCON, não assinar o contrato ou seu aditivo no prazo disposto neste item, ela ficará sujeita às penalidades descritas neste instrumento.

2. Consoante o art. 107, da Lei n.º 14.133/2021, o contrato poderá ser prorrogado sucessivas vezes, até o limite de 10 (dez) anos, desde que os preços permaneçam vantajosos para a **CONTRATANTE** e haja suficiência orçamentária.

3. A **CONTRATADA** não possui direito subjetivo à prorrogação contratual.

4. O presente instrumento não poderá ser prorrogado caso a **CONTRATADA** tiver sido penalizada nas sanções de declaração de inidoneidade ou de impedimento de licitar e contratar com a Administração Pública Direta e Indireta do **ESTADO DO AMAZONAS**.

CLÁUSULA QUINTA – DA FUNDAMENTAÇÃO LEGAL DA CONTRATAÇÃO:

O presente contrato foi firmado mediante _____, fundamentando-se no art. _____, da Lei n.º 14.133/2021, e no Ato n.º 008/2024/PGJ, o qual define os procedimentos administrativos para contratação de bens e serviços no âmbito do Ministério Público do Estado do Amazonas, bem como nas demais legislações correlatas, conforme o _____.

CLÁUSULA SEXTA – DO REGIME DE EXECUÇÃO:

Conforme o Termo de Referência n.º 28.2025.DTIC.2002143.2025.007562 e o art. 6º, XXIX, da Lei n.º 14.133/2021, o regime de execução deste contrato é o da **empreitada por preço global**, modalidade em que a contratação do serviço se dá por preço certo e total.

CLÁUSULA SÉTIMA – DOS DOCUMENTOS INTEGRANTES:

Para melhor caracterizar o presente contrato, integram também este instrumento, como se nele estivessem transcritos, obedecidos os termos da legislação sobre

contratos públicos, os seguintes documentos:

1. O Termo de Referência n.º 28.2025.DTIC.2002143.2025.007562;

2. O Edital de Licitação n.º _____;

3. A Proposta Comercial n.º _____ encaminhada pela **CONTRATADA**, no dia _____, contendo os valores unitário e total..

CLÁUSULA OITAVA – DO VALOR:

O valor global e estimado deste contrato é de _____

1. No preço contratado já estão incluídos todos os custos e despesas, tais como: custos diretos e indiretos, tributos incidentes, despesas administrativas, materiais, serviços, encargos sociais, trabalhistas, seguros, frete, embalagens, lucro, e outros necessários ao cumprimento integral do objeto deste instrumento.

CLÁUSULA NONA – DA GESTÃO, FISCALIZAÇÃO E ACOMPANHAMENTO:

O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133/21, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

1. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

2. As comunicações entre a **CONTRATANTE** e a **CONTRATADA** devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

3. A **CONTRATANTE** poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

4. Após a assinatura do contrato ou instrumento equivalente, a **CONTRATANTE** poderá convocar o representante da **CONTRATADA** para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da **CONTRATADA**, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

5. Preposto

5.1 A **CONTRATADA** deverá manter preposto junto à PGJ-AM, aceito pela respectiva **FISCALIZAÇÃO**, durante o período de vigência do contrato, para representá-la administrativamente, sempre que for necessário, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado, o qual deverá ser indicado mediante declaração de que deverá constar o nome completo, nº do CPF e do documento de identidade, além dos dados relacionados à sua qualificação profissional.

5.2 A empresa orientará o seu **PREPOSTO** quanto à necessidade de acatar as orientações da Administração, inclusive quanto ao cumprimento das Normas Internas e de Segurança e Medicina do Trabalho.

5.3. A **CONTRATANTE** poderá recusar, desde que justificadamente, a

indicação ou a manutenção do preposto da empresa, hipótese em que a **CONTRATADA** designará outro para o exercício da atividade.

6. Fiscalização

6.1 A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos, conforme indicação em portaria específica publicada no Diario Oficial do MPAM.

6.2 Compete ao **Gestor da Ata/Contrato,** além de outras atribuições, nos termos da lei:

a) Acompanhar os prazos de execução e de vigência do contrato, conforme as rotinas e procedimentos estabelecidos pelo MPAM, e as cláusulas do contrato ou instrumento equivalente, comunicando à **CONTRATADA** e à unidade competente da Administração eventuais atrasos e encaminhando, em tempo hábil, expediente para a prorrogação do contrato;

b) Coordenar e acompanhar a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração;

c) Acompanhar a manutenção das condições de habilitação da **CONTRATADA**, para fins de empenho de despesa e pagamento, e anotar os problemas que obstam o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais;

d) Comunicar à Autoridade Competente as ocorrências relacionadas à execução do contrato que ultrapassarem a sua competência;

e) Emitir TERMO DE RECEBIMENTO DEFINITIVO, juntamente com a **FISCALIZAÇÃO**, comprovando a avaliação do cumprimento das obrigações assumidas pela **CONTRATADA**;

f) Receber e conferir as faturas/notas fiscais emitidas pela **CONTRATADA**, e encaminhar, devidamente certificadas/atestadas ao setor competente, observando, previamente, se a fatura apresentada pela **CONTRATADA** refere-se ao objeto que foi efetivamente pactuado;

g) Encaminhar o processo à unidade competente para proceder à liquidação da despesa, alertando para a data limite para pagamento das notas fiscais/fatura;

h) Requisitar a prorrogação de contrato, se possível, junto à Autoridade Competente, que deve ser providenciada antes de seu término, reunindo as justificativas necessárias;

i) Elaborar a comunicação à área competente para abertura de nova licitação, antes de findo a prestação de serviços e com antecedência razoável;

j) Cuidar das alterações de interesse da **CONTRATADA**, que deverão ser por ela formalizadas e devidamente fundamentadas, principalmente em se tratando de pedido de reequilíbrio econômico-financeiro ou repactuação, sendo que, no caso de pedido de prorrogação de prazo, deverá ser comprovado o fato impeditivo da

execução, o qual, por sua vez, deverá corresponder àqueles previstos na Lei n. 14.133/21 e alterações, se possível;

k) Esclarecer dúvidas e transmitir instruções à **CONTRATADA**, comunicando alterações de prazos, cronogramas de execução e especificações do projeto, inclusive solicitando ao setor competente da Administração, quando necessário a emissão de parecer técnico;

l) Deflagrar e conduzir os procedimentos de fiscalização à **CONTRATADA**, com base nos termos contratuais, sempre que houver descumprimento de suas cláusulas por culpa da **CONTRATADA**, acionando as instâncias superiores e/ou os órgãos públicos competentes quando o fato exigir;

m) Verificar se a entrega de materiais ou a prestação do serviço está sendo executada em conformidade com o pactuado, no tocante a prazo, especificações, preço e quantidade;

n) Rejeitar equipamentos e serviços que estejam em desacordo com as especificações do objeto contratado;

o) Zelar pelo efetivo cumprimento das obrigações contratuais assumidas e pela qualidade dos produtos fornecidos e dos serviços prestados;

p) Notificar a **CONTRATADA** em qualquer ocorrência desconforme com as cláusulas contratuais, sempre por escrito, com prova de recebimento da notificação (procedimento formal, com prazo);

q) Verificar a regularidade fiscal, trabalhista e previdenciária da contratada para fins de pagamento; e

r) Orientar a **CONTRATADA**, por intermédio do preposto, sobre a correta execução do contrato e, pelo mesmo meio, levar ao seu conhecimento as situações temerárias, recomendando medidas e estabelecendo prazo de resolução.

6.3 Compete ao **Fiscal Técnico**, além de outras atribuições, nos termos da lei:

a) Acompanhar e fiscalizar a execução do contrato nos aspectos técnicos da solução, conforme o respectivo regramento técnico aplicável;

b) Zelar pelo efetivo cumprimento das obrigações contratuais assumidas e pela qualidade dos produtos fornecidos e dos serviços prestados, de modo a assegurar os melhores resultados para a Administração;

c) Ler atentamente o Termo de Contrato e anotar em registro próprio todas as ocorrências relacionadas à sua execução, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados;

d) Esclarecer dúvidas do preposto/representante da **CONTRATADA** que estiverem sob a sua alçada, encaminhando às áreas competentes os problemas que surgirem quando lhe faltar competência;

e) Notificar à **CONTRATADA**, para a correção da execução do contrato, de determinando prazo para a correção, qualquer inexatidão ou irregularidade;

f) Informar ao Gestor do Contrato, em tempo hábil, irregularidades que

possam demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso;

g) Comunicar ao Gestor do Contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual;

h) Avaliar a qualidade dos serviços realizados ou dos itens entregues e justificativas, de acordo com os critérios de aceitação definidos em contrato; e

i) Orientar a **CONTRATADA**, por intermédio do preposto, sobre a correta execução do contrato e, pelo mesmo meio, levar ao seu conhecimento as situações temerárias, recomendando medidas e estabelecendo prazo de resolução.

CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DA CONTRATANTE:

São obrigações da **CONTRATANTE**:

1. Acompanhar e fiscalizar, como lhe aprouver e no seu exclusivo interesse, na forma prevista na Lei n.º 14.133/21, exigindo o cumprimento de todas as obrigações assumidas, de acordo com o contrato e seus anexos.

2. Nomear **GESTOR** e **FISCALIZAÇÃO** técnica e administrativa, para acompanhar e fiscalizar, a execução dos contratos.

3. As ações de fiscalização não excluem nem reduzem a responsabilidade da **CONTRATADA**, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios ou emprego de material inadequado ou de qualidade inferior.

4. Fornecer à **CONTRATADA** as informações necessárias à fiel execução do objeto deste instrumento.

5. Permitir o acesso, acompanhar e fiscalizar a execução do contrato, verificando a conformidade da prestação dos serviços e regular a entrega dos itens, de forma a assegurar o perfeito cumprimento do contrato.

6. Anotar em registro próprio e notificar a **CONTRATADA**, por escrito, a ocorrência de eventuais imperfeições, defeitos de fabricação, e avarias nos itens, fixando prazo para a sua reposição.

7. Rejeitar, no todo ou em parte, serviço ou fornecimento executado em desacordo com o contrato.

8. Efetuar regularmente o pagamento da **CONTRATADA**, dentro dos critérios estabelecidos neste contrato, quanto aos serviços devidamente realizados, por meio de Ordem Bancária, após o atesto das notas fiscais/faturas pelo comitê responsável.

9. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

9.1 A **CONTRATANTE** terá o prazo de 1 (um) mês, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

10. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-

financeiro feitos pela **CONTRATADA** no prazo máximo de 1 (um) mês.

11. A **CONTRATANTE** não responderá por quaisquer compromissos assumidos pela **CONTRATADA** com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da **CONTRATADA**, de seus empregados, prepostos ou subordinados.

CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES DA CONTRATADA:

A **CONTRATADA** deverá cumprir todas as obrigações constantes neste termo de referência, minuta de contrato e seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando:

1. Apresentar, no prazo de até 10 (dez) dias corridos, contados a partir da assinatura do contrato ou do recebimento da Nota de Empenho e da Autorização de Fornecimento de Materiais/Serviços:

1.1 Indicação formal do preposto da **CONTRATADA** apto a representá-la junto à **CONTRATANTE**, que deverá responder pela fiel execução do contrato, designado para acompanhar sua execução e atuar como interlocutor principal junto à **CONTRATANTE**, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

a) A indicação do preposto deverá ser acompanhada de seus dados pessoais, (no mínimo o nome completo e CPF do funcionário da empresa) e dados de contrato, como e-mail, telefone, whatsapp e outros.

1.2 Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste instrumento.

2. Efetuar a entrega do objeto contratado, dentro do prazo e de acordo com as especificações constantes deste contrato, observando as prescrições e as recomendações do fabricante, a legislação estadual ou municipal, se houver, bem como outras normas correlatas, ainda que não estejam explicitamente citadas neste documento e seus anexos.

3. Apresentar, no prazo de até 10 (dez) dias úteis, contados a partir da entrega do objeto, o correspondente TERMO DE GARANTIA E ASSISTÊNCIA TÉCNICA, para os equipamentos/softwares/licenças fornecidos incluindo seus números de série, com o prazo de garantia solicitado nesta avença.

4. Não transferir a outrem, no todo ou em parte, o objeto deste termo, não sendo aceita a transferência de responsabilidade para outras entidades, sejam fabricantes, técnicos, subempreiteiros ou quaisquer outros.

4.1 É vedada a subcontratação total ou parcial do objeto, bem como a cessão ou transferência deste instrumento contratual, no todo ou em parte, incluindo a transferência da execução a terceiros, a qualquer título, sem prejuízo da possibilidade de a **CONTRATADA** contratar atividades-meio acessórias (ex.: frete, seguro, logística), desde que:

I – tais contratações não caracterizem subcontratação do objeto nem delegação de atividades técnicas essenciais; e

II – permaneça a **CONTRATADA** integralmente responsável pela execução, qualidade, prazos, garantias e assistência técnica previstas no Contrato e no Termo de Referência.

5. Comunicar imediatamente à **CONTRATANTE**, formalmente, toda e qualquer anormalidade que dificulte ou impossibilite a execução do objeto deste contrato e prestar os esclarecimentos julgados necessários.

6. Aceitar todas as decisões, métodos de inspeção, verificação e controle, obrigando-se a fornecer todos os dados, elementos e explicações que a **CONTRATANTE** julgar necessário.

6.1 A ação de fiscalização não exonera a **CONTRATADA** de suas responsabilidades contratuais.

7. Manter contato e realizar o planejamento dos serviços com a **CONTRATANTE** de forma a executar quaisquer tarefas ou ajustes inerentes ao objeto contratado.

8. Acatar as observações feitas pela **FISCALIZAÇÃO** da **CONTRATANTE** quanto à execução dos serviços.

9. Atender prontamente quaisquer orientações e exigências da equipe de **FISCALIZAÇÃO** do contrato ou autoridade superior (art. 137, II, da Lei n.º 14.133/21, e prestar todo esclarecimento ou informação por eles solicitados, inerentes à execução do objeto contratual;

9.1 A **CONTRATADA** deverá responder por escrito, no prazo máximo de até 2 (dois) dias consecutivos, a quaisquer comunicações e/ou esclarecimentos requisitados pela **CONTRATANTE**, pertinentes à execução do contrato e que venham a ser solicitados pelo MPAM.

10. A **CONTRATADA** deverá responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com Código de Defesa do Consumidor, Lei nº 8.078/90, e às demais normas pertinentes.

11. Apresentar justificativa por escrito, devidamente comprovada, nos casos de ocorrência de fato superveniente, excepcional ou imprevisível, estranho à vontade das partes, e de impedimento de execução por fato ou ato de terceiro reconhecido pela **CONTRATANTE** em documento contemporâneo a sua ocorrência, quando não puder cumprir os prazos estipulados para a execução, total ou parcial, do objeto deste contrato.

11.1 Nos casos de eventual atraso na entrega do objeto, comunicar à **CONTRATANTE**, antes de expirar tal prazo, quaisquer problemas que impossibilitem o cumprimento do prazo previsto, com a devida comprovação.

12. Substituir, reparar, corrigir, remover, refazer ou reconstituir, às suas expensas, no todo ou em parte, no prazo fixado pela **FISCALIZAÇÃO**, os itens que não atendam às especificações exigidas e foram rejeitados, os que se verifiquem imperfeições, vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.

13. Responsabilizar-se por falhas na execução dos serviços que venham a se tornar aparentes em data posterior à sua entrega, ainda que tenha havido aceitação deles.

14. Responsabilizar-se pela garantia e assistência técnica *on-site* dos itens, caso o fabricante e/ou assistência técnica autorizada por este não puder fazê-lo ou se recusar.

15. Manter, durante toda a execução do contrato, todas as condições de habilitação e qualificação exigidas na respectiva licitação, em compatibilidade com as obrigações assumidas.

16. Responder pela idoneidade moral e técnica dos seus empregados, sendo única, integral e exclusivamente responsável, em qualquer caso, por todos os danos e prejuízos, de qualquer natureza, causados, direta ou indiretamente, à **CONTRATANTE** ou a terceiros, provenientes da execução dos serviços objeto deste contrato, quaisquer que tenham sido as medidas preventivas adotadas, respondendo por si e seus procuradores.

17. Responsabilizar-se por obter todas as franquias, licenças, aprovações e demais exigências de órgãos competentes, inclusive responsabilizando-se por todos os ônus decorrentes.

18. A inobservância das especificações constantes deste instrumento implicará a não aceitação parcial ou total dos serviços, devendo a **CONTRATADA** refazer as partes recusadas sem direito a indenização

19. Cumprir as normas de proteção ao trabalho, inclusive aquelas relativas à segurança e à saúde no trabalho;

20. Não submeter os trabalhadores a condições degradantes de trabalho, jornadas exaustivas, servidão por dívida ou trabalhos forçados;

21. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos de idade, exceto na condição de aprendiz para os maiores de quatorze anos de idade, observada a legislação pertinente;

22. Não submeter o menor de dezoito anos de idade:

22.1 à realização de trabalho noturno;

22.2 à realização de trabalho em condições perigosas e insalubres; nem

22.3 à realização de atividades constantes na Lista de Piores Formas de Trabalho Infantil, aprovada pelo Decreto Federal n.º 6.481, de 12 de junho de 2008;

23. Receber e dar o tratamento adequado a denúncias de discriminação, violência e assédio no ambiente de trabalho;

24. Rubricar o contrato ou seus aditivos no prazo de 5 (cinco) dias úteis, contados a partir da notificação enviada pela DCCON.

CLÁUSULA DÉCIMA SEGUNDA – DA MATRIZ DE ALOCAÇÃO DE RISCOS:

1. Disposições gerais.

1.1. Para os fins desta Cláusula entende-se por risco todo evento futuro, incerto e alheio à vontade das partes, capaz de gerar impacto relevante no prazo, no custo ou na qualidade da execução contratual.

1.2. A alocação de riscos observa o art. 22 da Lei n.º 14.133/2021, de modo a atribuir-lhes, sempre que possível, à parte que detenha melhor capacidade de gerenciá-los ou mitigá-los, assegurando o equilíbrio econômico-financeiro do ajuste.

1.3. Sempre que caracterizado caso fortuito ou força maior, devidamente comprovado, aplicar-se-ão as regras desta Matriz, sem prejuízo das demais disposições legais pertinentes.

2. Riscos atribuídos exclusivamente à CONTRATANTE:

Evento	**Abrangência / Limite**	**Medida de mitigação ou compensação**

Evento	Abrangência / Limite	Medida de mitigação ou compensação
2.1 Alterações unilaterais do objeto ou das quantidades (art. 124, inciso I, da Lei n.º 14.133/2021).	Até os limites legais	Reequilíbrio mediante reajuste de preço, de prazo ou ambos, a pedido do CONTRATADO, nos termos da Cláusula Vigésima.
2.2 Caso fortuito ou força maior **externo** à cadeia de suprimentos do CONTRATADO (greves gerais, calamidade natural que impeça recebimento / instalação).	—	Suspensão de prazos e, se for o caso, recomposição de custos diretos comprovados.
2.3 Atraso de pagamento por fato imputável à Administração.	> 30 (dias) após vencimento	Incidência de atualização financeira (art. 92, inciso V, da Lei n.º 14.133/2021) e possibilidade de paralisação justificada (art. 137, § 3.º, inciso II, da Lei n.º 14.133/2021).
2.4 Falhas de infraestrutura, logística interna ou compatibilidade de sistemas sob gestão do MPAM.	—	Ajuste de cronograma sem ônus ao CONTRATADO; despesas adicionais cobertas pelo CONTRATANTE.
2.5 Contingenciamento ou indisponibilidade orçamentária superveniente.	—	Aplicação dos arts. 137, § 3.º, inciso II, e 138, § 2.º, da Lei n.º 14.133/2021, com suspensão ou rescisão e pagamento de indenizações cabíveis.

3. Riscos atribuídos exclusivamente à CONTRATADA:

Evento	Abrangência / Limite	Medida de mitigação ou compensação
3.1 Execução inadequada, atraso ou descumprimento de prazos sem causa justificada.	—	Aplicação de penalidades contratuais (arts. 155 e 156 da Lei n.º 14.133/2021) e obrigação de corrigir/repactuar às suas expensas.
3.2 Falha de fornecimento de materiais, insumos ou mão de obra.	—	Substituição ou suplementação imediata, sem ônus à CONTRATANTE.

Evento	Abrangência / Limite	Medida de mitigação ou compensação
3.3 Não conformidade dos equipamentos às especificações ou às amostras aprovadas.	—	Rejeição, substituição e aplicação de multas previstas.
3.4 Ausência ou insuficiência da garantia técnica **on-site** prevista.	—	Multa específica e extensão proporcional do período de garantia.
3.5 Danos causados por transporte ou armazenagem sob responsabilidade do fornecedor.	—	Reparação integral e sem custo para a CONTRATANTE.

4. Riscos COMPARTILHADOS:

4.1 São considerados riscos compartilhados aqueles que, pela própria natureza, escapam do controle exclusivo de uma das partes e cuja ocorrência possa comprometer a equação econômico-financeira do contrato.

Evento	Critério de compartilhamento	Forma de compensação
4.1.1 Alterações legais, normativas ou tributárias não previstas na data da proposta que onerem ou desonerem o objeto.	Cada parte arca com o impacto em até **5%** (cinco por cento) do valor atualizado do contrato; excedente será objeto de reequilíbrio conforme Cláusula Vigésima.	Ajuste de preços ou de escopo, conforme art. 124 da Lei n.º 14.133/2021.
4.1.2 Oscilação inflacionária ou cambial extraordinária, com variação acumulada superior a **10 %** do IPCA.	Impacto até **10 %** suportado pela parte contratada; excedente sujeito a reequilíbrio.	Reajuste ou repactuação após comprovação documental.
4.1.3 Situações de emergência pública ou calamidade que exijam alteração de cronograma.	Prorrogação automática dos prazos equivalente ao período de paralisação.	Eventuais custos diretos adicionais divididos meio a meio, mediante apresentação de planilha analítica.
4.1.4 Oscilações severas de mercado em componentes de manutenção (variação > 15 % do índice ICEI-TI).	Excedente dividido em partes iguais, mediante laudo de mercado independente.	Repactuação de preços de manutenção.

4.2 A superveniência de novos riscos não contemplados será tratada pelos mesmos critérios de alocação (capacidade de controle e gestão), mediante aditivo específico ou termo de apostilamento, observado o procedimento da Cláusula Vigésima.

5. Revisões e atualização da Matriz:

5.1 Ocorrendo fatos supervenientes relevantes, a presente Matriz poderá ser revista por aditivo específico, preservados os princípios da legalidade, da eficiência e do equilíbrio econômico-financeiro.

CLÁUSULA DÉCIMA TERCEIRA – DA GARANTIA TÉCNICA:

Todos os equipamentos e softwares utilizados no fornecimento do objeto deverão estar cobertos por suporte, garantia e assistência técnica do fabricante, durante toda a vigência do contrato.

1. A garantia dos hardwares deverá ser na modalidade on-site no Datacenter da **CONTRATADA**.

2. A **CONTRATADA** é a única responsável pelos equipamentos e softwares disponibilizados na prestação dos serviços fornecidos à **CONTRATANTE**, mesmo que tenham sido adquiridos de terceiros.

3. A **CONTRATADA** responderá pela reparação dos danos causados por defeitos relativos ao serviço prestado, conforme descrição e exigências deste instrumento. Por isso, deve prezar pela qualidade e eficiência, garantindo que o serviço e as soluções definitivas fornecidas não causem problemas adicionais àqueles apresentados pela **CONTRATANTE**, quando do recebimento de alertas ou da abertura dos chamados de suporte técnico.

4. Serviços de Suporte Técnico e Manutenção

4.1 Os equipamentos deverão possuir garantia de 60 (sessenta) meses, com suporte 24x7 e prazo de envio de peças até o próximo dia útil após abertura do chamado.

4.2 A **CONTRATANTE** poderá acionar diretamente o suporte do fabricante, sem necessidade de autorização prévia da **CONTRATADA**. Não haverá limitação quanto à quantidade de chamados, seja para dúvidas, configurações ou problemas relacionados a hardware e software.

4.3 Chamados poderão ser abertos via telefone 0800, portal web ou e-mail.

4.4 O atendimento telefônico inicial deverá ser realizado em português.

4.5 A contratada deverá garantir acesso completo ao portal do fabricante, incluindo base de conhecimento, atualizações de software e documentação.

4.6 Durante a vigência do suporte, todas as atualizações de firmware e software deverão ser fornecidas sem ônus à **CONTRATANTE**.

4.7 A contratada deverá apresentar os códigos de serviço (SKU, part number) referentes à garantia do fabricante, com os equipamentos devidamente registrados em nome da contratante.

4.8 É de responsabilidade da contratada garantir a compatibilidade técnica entre todos os componentes da solução durante toda a vigência contratual.

CLÁUSULA DÉCIMA QUARTA – DO ACORDO DE NÍVEL DE SERVIÇO (SLA):

Os chamados de suporte técnico serão classificados conforme o nível de severidade,

com base no impacto causado no ambiente computacional da **CONTRATANTE**, conforme as tabelas a seguir:

1. Impacto:

Nível	**Descrição do Impacto**
1	Serviços totalmente indisponíveis
2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos
3	Acesso aos aplicativos

2. Níveis de Severidade:

Modalidade	**Prazo**	**Níveis de Severidade**		
		1	**2**	**3**
Remoto	Início do Atendimento	1 hora	4 horas	8 horas
	Solução do Contorno	8 horas	12 horas	24 horas

3. Quando for necessário atendimento presencial, a **CONTRATADA** deverá disponibilizar técnicos para resolver os problemas no local. Preferencialmente, essas atividades devem ser previamente acordadas entre as partes, exceto em casos de severidade máxima ou evidente indisponibilidade da infraestrutura da **CONTRATANTE**.

4. O início do atendimento será considerado a partir da abertura do chamado técnico.

5. O atendimento será considerado encerrado quando a solução estiver disponível e funcionando perfeitamente no local de instalação.

6. Durante toda a vigência do contrato, a **CONTRATANTE** poderá abrir chamados ilimitados para suporte técnico.

7. A **CONTRATADA** será integralmente responsável por quaisquer danos ou prejuízos causados ao patrimônio da **CONTRATANTE** ou de terceiros, decorrentes de ações ou omissões de seus colaboradores durante a execução dos serviços solicitados.

8. Qualquer atividade relacionada a configurações, ajustes ou parametrizações após a implantação deverá ser precedida da abertura de um chamado técnico.

9. Caso a atividade seja realizada de forma proativa, a **CONTRATADA** deverá comunicar à **CONTRATANTE**, via e-mail, justificando a execução antecipada.

10. Se alguma atividade exigir a interrupção da solução, a **CONTRATANTE** deverá ser imediatamente notificada para autorizar ou reagendar a execução.

11. Atualizações que impliquem indisponibilidade do ambiente devem ser previamente agendadas com a equipe técnica da **CONTRATANTE**.

12. A **CONTRATADA** deverá manter uma Central de Atendimento em português (Brasil), operando 24 horas por dia, 7 dias por semana, durante todo o ano

(24x7x365), para abertura de chamados e demais comunicações.

13. A **CONTRATANTE** poderá solicitar serviços específicos por meio dos seguintes canais de comunicação:

a) E-mail;

b) Telefone 0800;

c) Sistema de Chamados Web.

14. O serviço será considerado concluído somente após a confirmação da área técnica da **CONTRATANTE** quanto à sua execução satisfatória.

15. O encerramento de solicitações técnicas dependerá da anuência de ambas as partes: **CONTRATADA** e **CONTRATANTE**.

16. A **CONTRATADA** manterá um cadastro com os nomes das pessoas indicadas pela **CONTRATANTE** autorizadas a abrir e encerrar chamados.

17. O prazo para encerramento do atendimento não poderá ultrapassar os limites estabelecidos para cada nível de criticidade.

18. Considera-se suporte técnico as atividades que requerem acompanhamento por parte de um técnico da **CONTRATANTE**.

19. Quando for necessário atendimento local, o cronograma de execução deverá ser acordado entre as partes.

20. A **CONTRATADA** deverá iniciar o atendimento conforme os prazos definidos para cada nível de criticidade.

21. A manutenção corretiva inclui os serviços necessários para restaurar o funcionamento adequado dos equipamentos, com fornecimento de peças conforme especificações do fabricante, em caso de falhas ou defeitos de hardware.

22. A **CONTRATADA** deverá realizar os serviços de manutenção com ferramentas próprias e técnicos especializados, devidamente identificados.

23. O suporte técnico compreende ações para restabelecer o funcionamento correto das soluções contratadas, incluindo configuração, habilitação, implementação, manutenção e colocação em produção de funcionalidades.

24. Caso seja necessária a atualização de firmware, a **CONTRATADA** deverá fornecer o pacote de software e realizar a atualização.

25. Considerando que a resolução de problemas de software pode envolver o desenvolvimento de patches, admite-se a adoção de soluções de contorno (workaround) até a implementação da solução definitiva.

26. O período para solução de ocorrências de software será contado entre a formalização e o encerramento efetivo da ocorrência, seja com solução definitiva ou provisória.

27. Para ocorrências de hardware não resolvidas dentro do prazo, a **CONTRATADA** deverá substituir o equipamento ou módulo defeituoso em até 72 (setenta e duas) horas úteis. Após a substituição, deverá ser entregue um documento com as descrições e números de série dos equipamentos substituídos e novos.

28. A substituição definitiva de hardware deverá ser feita com equipamento novo, original, recomendado pelo fabricante, com configuração igual ou superior à do substituído.

29. Durante a substituição, a **CONTRATADA** deverá entregar documento

contendo a descrição e número de série do equipamento defeituoso e do novo equipamento.

30. O prazo para solução de ocorrências de hardware será contado entre a formalização e o encerramento efetivo da ocorrência. Quando houver substituição, o encerramento será considerado apenas após o novo equipamento entrar em operação.

31. Para cálculo do tempo de atendimento, serão desconsiderados os períodos em que a **CONTRATANTE** estiver responsável por ações necessárias à análise e solução da ocorrência.

32. Não haverá limitação quanto ao número de técnicos da **CONTRATANTE** autorizados a abrir chamados, desde que previamente registrados como pontos de contato.

33. Durante o período de garantia, a **CONTRATADA** deverá fornecer todas as atualizações de software (versões, releases, patches), firmware ou microcódigos dos hardwares cobertos pela manutenção, sem custo adicional.

CLÁUSULA DÉCIMA QUINTA – DO RECEBIMENTO E DOS PRAZOS DE ENTREGA:

1. Da Entrega

1.1 Do prazo

1.1.1 A **CONTRATADA** deverá em, **no máximo, 60 (sessenta) dias corridos**, contados a partir da assinatura do contrato, finalizar a entrega de todos os itens do objeto especificado, com funcionamento e funcionalidades da solução de Datacenter completamente operacionais, totalmente ativadas e disponíveis na estrutura da **CONTRATADA**, conforme descritas neste contrato.

1.1.2 O prazo para entrega do objeto especificado poderá ser prorrogado mediante apresentação pela **CONTRATADA**, antes do fim do prazo especificado, de solicitação formal e fundamentada, condicionado à aceitação pela **CONTRATANTE**, que decidirá pela prorrogação do prazo ou aplicação das penalidades previstas em contrato.

1.2 Das condições de fornecimento

1.2.1 A **CONTRATADA** será responsável pelo transporte dos produtos, desde o local de sua fabricação/embalagem, conforme o caso, até o local de entrega, na sede da PROCURADORIA GERAL DE JUSTIÇA, a qual ocorrerá em dias úteis, no horário das 14h às 17h, no seguinte endereço:

Av. Coronel Teixeira, nº 7.995, Nova Esperança II
CEP. 69037-473, Manaus-AM

1.2.2 A entrega dos produtos deverá ser previamente agendada com o SETOR DE PATRIMÔNIO E MATERIAL – SPAT pelo telefone (92) 3655-0767.

1.2.3 Os produtos deverão ser entregues em perfeitas condições, conforme a quantidade e especificações pactuadas, observando o

Edital, a Proposta da **CONTRATADA** e este contrato devendo, também, ser acondicionado adequadamente, em seu invólucro original, que deverão ser entregues devidamente acompanhados da respectiva nota fiscal, na qual constarão os valores discriminados dos itens que integram o conjunto, assim como as indicações referentes a: marca, modelo, procedência e prazo de garantia ou validade.

1.2.4 Os produtos devem estar em plena fabricação, não sendo aceitos aqueles com avisos de end-of-sale, end-of-support ou end-of-life emitidos pelo fabricante.

2. Do recebimento provisório e definitivo

2.1 O recebimento dos produtos será conduzido por uma COMISSÃO especialmente designada para essa finalidade. Essa comissão será composta por, no mínimo, três servidores ou empregados públicos, em conformidade com o disposto no Art. 117, §1º e Art. 140, inciso II da Lei n.º 14.133/21, conforme estabelecido neste subitem.

2.2 O RECEBIMENTO PROVISÓRIO será realizado pelo SETOR DE PATRIMÔNIO E MATERIAL - SPAT no ato da entrega da totalidade dos produtos empenhados, devidamente acompanhados da nota fiscal. Constitui-se de uma inspeção quantitativa, para posterior verificação de sua conformidade com as especificações do Termo de Referência e do Contrato.

a) O RECEBIMENTO PROVISÓRIO não constitui aceitação do objeto.

2.3 O RECEBIMENTO DEFINITIVO será realizado por FISCAL TÉCNICO ou COMISSÃO especialmente designada, no prazo máximo de 30 (trinta) dias, a contar do recebimento provisório, para verificação da conformidade dos equipamentos com as condições, especificações e obrigações contratuais.

a) É condição para RECEBIMENTO DEFINITIVO o fornecimento do TERMO DE GARANTIA E ASSISTÊNCIA TÉCNICA, informando que os referidos produtos estão cobertos por garantia de fábrica, de acordo com as exigências constantes neste instrumento;

b) O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais;

c) Uma vez constatado o cumprimento das obrigações de fornecimento, o TERMO DE RECEBIMENTO DEFINITIVO será emitido, que consistirá na declaração formal de que os itens fornecidos atendem aos requisitos estabelecidos no contrato, comprovando o atendimento das exigências contratuais.

2.4 Para avaliação da adequação às exigências contratuais e qualidade, o FISCAL TÉCNICO ou COMISSÃO submeterá os equipamentos recebidos a testes de aceitação, para aferição da boa execução do objeto contratado, após o qual, emitirá um relatório completo dos testes efetuados, devidamente assinado. Os testes serão constituídos das seguintes fases:

a) Abertura das embalagens;

b) Comprovação de que o equipamento/solução atende às especificações mínimas exigidas ou superiores oferecidas;

c) Testes funcionais de configuração e desempenho dos produtos.

2.5 Os itens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste instrumento, seus Anexos e na proposta, sem prejuízo da aplicação das penalidades, cabendo à **CONTRATADA** o dever de substituir os itens que não estejam de acordo com as especificações, observando-se o disposto no Art. 140, §1º da Lei n.º 14.133/21.

2.6 O RECEBIMENTO PROVISÓRIO ou DEFINITIVO do objeto não exclui a responsabilidade civil a ele relativa, nem a ético-profissional, pela perfeita execução do objeto deste termo.

2.7 As não conformidades e desvios de qualidade observados serão descritos em relatório, e não serão recebidos definitivamente, devendo a pendência ser completamente sanada pela **CONTRATADA**, em no máximo 15 (quinze) dias consecutivos, contados da notificação da **CONTRATANTE**.

2.8 Se, a qualquer tempo, vier a ser constatado que o material fornecido o foi em desacordo com as especificações e, em decorrência desse fato, observar-se qualquer tipo de dano ao equipamento onde está sendo utilizado, o reparo do equipamento ou, se for o caso, a sua substituição, será de inteira responsabilidade da **CONTRATADA**, nos termos da lei pertinente.

CLÁUSULA DÉCIMA SEXTA – DAS CONDIÇÕES DE PAGAMENTO:

O pagamento devido à **CONTRATADA** será creditado em conta-corrente, por meio de ordem bancária, efetuado mediante apresentação de nota fiscal/fatura, que será atestada pela **FISCALIZAÇÃO** deste contrato.

1. O pagamento será realizado à **CONTRATADA** de forma integral e condicionado ao marco da emissão do Termo de Recebimento Definitivo do objeto, assinado por ambas as partes.

2. Nos termos do art. 139, caput, e do art. 140, ambos do Ato n.º 008/2024/PGJ, os prazos para a **CONTRATANTE** liquidar e pagar são de:

2.1 até 10 (dez) dias úteis para a liquidação da despesa, a contar do recebimento da nota fiscal ou do instrumento de cobrança equivalente pela **CONTRATANTE**;

2.2 até 10 (dez) dias úteis para o pagamento, contados da liquidação da desepesa.

3. O requerimento de pagamento deverá ser encaminhado aos endereços eletrônicos protocolo@mpam.mp.br e dtic@mpam.mp.br, acompanhado da respectiva nota fiscal/fatura dos produtos, emitidas em conformidade com o Protocolo ICMS 42/2009 (NF-e), deverá estar devidamente discriminada, em nome da **PROCURADORIA-GERAL DE JUSTIÇA**, CNPJ n.º 04.153.748/0001-85, e acompanhada da seguinte documentação:

3.1 Certidão Negativa de Débitos para com a Fazenda Federal, Estadual e Municipal do domicílio ou sede da empresa, ou outra equivalente, na forma da lei.

3.2 Certidão Negativa de Débitos à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS.

3.3 Certidão Negativa de Débitos trabalhistas.

3.4 Requerimento solicitando o pagamento, em duas vias, constando o número da Nota de Empenho e deste contrato.

3.5 Recibo em duas vias.

4. Nenhum pagamento será efetuado à **CONTRATADA** enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência.

4.1 Na hipótese de a **CONTRATADA** não ter executado completamente o objeto, ou tê-lo realizado de maneira insatisfatória, conforme relatório da **FISCALIZAÇÃO**, o pagamento será feito de maneira proprocional e apenas pelos serviços efetivamente prestados.

4.2 Em qualquer dos casos deste item, a **CONTRATANTE** poderá reter os pagamentos devidos à **CONTRATADA** até que as pendências sejam resolvidas.

5. Se, quando da efetivação do pagamento, os documentos comprobatórios de situação regular, apresentados em atendimento às exigências de habilitação, estiverem com a validade expirada, o pagamento ficará retido até a apresentação de novos documentos dentro do prazo de validade.

6. Qualquer atraso ocorrido na apresentação da nota fiscal/fatura, ou dos documentos exigidos como condição de pagamento por parte da **CONTRATADA**, importará em prorrogação automática do prazo de vencimento da obrigação da **CONTRATANTE,** não sendo devido à **CONTRATADA** o pagamento de multa e juros moratórios.

7. Nenhum pagamento isentará a **CONTRATADA** das responsabilidades atinentes ao produto, tampouco implicará a aprovação definitiva da entrega, total ou parcialmente.

8.Nos casos de eventuais atrasos de pagamento, desde que a **CONTRATADA** não tenha concorrido de alguma forma para tanto, fica convencionado que os encargos moratórios devidos pela **CONTRATANTE**, entre a data de vencimento e a do dia do efetivo pagamento da nota fiscal/fatura, a serem incluídos na fatura do mês seguinte ao da ocorrência, serão calculados por meio da aplicação da seguinte fórmula:

EM = I x N x VP, onde:

EM = encargos moratórios

N = número de dias entre a data prevista para o pagamento e a do efetivo pagamento

VP = valor da parcela em atraso

I = índice de compensação financeira = 0,00016438, assim apurado:

I = i ÷ 365 = (6÷100) ÷ 365 = 0,00016438

Onde i = taxa percentual anual no valor de 6%.

CLÁUSULA DÉCIMA SÉTIMA – DA DOTAÇÃO ORÇAMENTÁRIA:

As despesas oriundas deste contrato correrão à conta da seguinte dotação orçamentária:

Unidade Gestora: 003101 – Procuradoria Geral de Justiça; **Unidade Orçamentária:** 03101 – Procuradoria Geral de Justiça; **Programa de Trabalho**: 03.122.0001.2001.0001 – Administração da Unidade; **Fonte**: – ; **Natureza da Despesa:** – , tendo sido emitida pela **CONTRATANTE**, em _____, a Nota de Empenho n.º _____, no valor global de **R$ _____**.

CLÁUSULA DÉCIMA OITAVA – DAS SANÇÕES ADMINISTRATIVAS:

Nos termos dos art. 155 da Lei n.º 14.133/2021, a **CONTRATADA** será responsabilizada administrativamente na forma desta cláusula.

1. São condutas passíveis de sanção administrativa:

1.1 Dar causa à inexecução parcial do contrato;

1.2 Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

1.3 Dar causa à inexecução total do contrato;

1.4 Deixar de entregar a documentação exigida para o certame;

1.5 Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

1.6 Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

1.7 Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

1.8 Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

1.9 Fraudar a licitação ou praticar ato fraudulento na execução do contrato;

1.10 Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

1.11 Praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

1.12 Praticar ato lesivo previsto no art. 5º da Lei n.º 12.846/2013.

2. Pela inexecução total ou parcial do compromisso assumido, a **CONTRATANTE** poderá aplicar à **CONTRATADA** as seguintes sanções:

2.1 Advertência, que será aplicada exclusivamente à conduta descrita no subitem 1.1 desta cláusula, quando não se justificar imposição de penalidade mais grave;

2.2 Multas, que serão aplicadas por qualquer das infrações descritas no item 1 desta cláusula, nos percentuais estabelecidos na Cláusula Décima Nona deste contrato;

2.3 Impedimento de licitar e contratar com a Administração Pública Direta e Indireta do **ESTADO DO AMAZONAS**, em decorrência das infrações previstas nos subitens 1.2, 1.3, 1.4, 1.5, 1.6 e 1.7 desta cláusula, pelo prazo máximo de 3 (três) anos, havendo possibilidade de reabilitação da **CONTRATADA** após o decurso de 1 (um) ano;

2.4 Declaração de inidoneidade para licitar ou contratar com toda a Administração Pública brasileira, em virtude das condutas descritas nos subitens 1.8, 1.9, 1.10, 1.11 e 1.12 desta cláusula, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a **CONTRATADA** ressarcir a **CONTRATANTE** pelos prejuízos resultantes e após decorrido o prazo de 3 (três) anos;

3. As sanções serão aplicadas pela **CONTRATANTE** em procedimento apuratório que assegure à **CONTRATADA** as garantias do contraditório e da ampla defesa, com os recursos a eles inerentes.

3.1 Compete à Comissão Permanente de Licitação (CPL) da **CONTRATANTE** instruir os procedimentos apuratórios de que trata este item.

4. Cabe ao (à) **SUBPROCURADOR(A)-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS** a aplicação das sançoes descritas nos subitens 2.1, 2.2 e 2.3 desta cláusula.

4.1 Da decisão do (a) **SUBPROCURADOR(A)-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS** cabe recurso dirigido a este, no prazo de 15 (quinze) dias úteis, contado da data da intimação.

4.2 Se o (a) **SUBPROCURADOR(A)-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS** não reconsiderar a decisão em 5 (cinco) dias úteis, encaminhar-la-á ao (à) **PROCURADOR(A)-GERAL DE JUSTIÇA.**

5. Compete ao (à) **PROCURADOR(A)-GERAL DE JUSTIÇA** a aplicação da sanção disposta no subitem 2.4 desta cláusula.

5.1 Da decisão do (a) **PROCURADOR(A)-GERAL DE JUSTIÇA** caberá apenas pedido de reconsideração, que deverá ser apresentado no prazo de 15 (quinze) dias úteis.

6. As penalidades serão obrigatoriamente registradas no Sistema de Cadastro Único de Fornecedores - SICAF.

7. A sanção do subitem 2.2 desta cláusula pode ser aplicada isolada ou conjuntamente com as dos subitens 2.1, 2.3 e 2.4.

8. A aplicação das penalidades previstas nesta cláusula não exclui nem atenua a obrigação de a **CONTRATADA** reparar integralmente os danos causados à **CONTRATANTE**.

CLÁUSULA DÉCIMA NONA – DAS MULTAS:

As multas a que se refere o subitem 2.2 da Cláusula Décima Oitava serão impostas nas seguintes hipóteses:

Item	Penalidade	Sanção	Limite
1	Atraso injustificado na entrega do objeto contratado, ou pelo não cumprimento dos prazos estabelecidos no Edital	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor total da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **C O N T R A T A D A** às sanções correlatas.

Item	Penalidade	Sanção	Limite
2	Atraso injustificado na regularização pertinente quando da recusa do objeto fornecido, na fase de **RECEBIMENTO**.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor total da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **C O N T R A T A D A** às sanções correlatas.
3	Recusa em substituir o produto defeituoso, que vier a ser rejeitado, ou que na execução dos serviços de garantia e assistência técnica, apontem a necessidade de troca;	Multa de mora diária de **1% (um por cento)** sobre o valor da Nota de Empenho	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **C O N T R A T A D A** às sanções correlatas.
4	Deixar de utilizar peças, componentes ou insumos originais ou certificados pelo fabricante, novos e de primeiro uso.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho. Por ocorrência	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **C O N T R A T A D A** às sanções correlatas.

Item	Penalidade	Sanção	Limite
5	Atraso injustificado para efetiva recolocação do produto em seu pleno estado de funcionamento, conforme condições de GARANTIA E ASSISTÊNCIA TÉCNICA deste Termo.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **C O N T R A T A D A** às sanções correlatas.
6	Deixar de fornecer equipamento backup nos casos em que não for possível recuperar os produtos dentro dos prazos de atendimento previstos.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **C O N T R A T A D A** às sanções correlatas.
7	Atraso injustificado para a substituição de determinado item (equipamento, serviço, software, licença), no atendimento de chamado de garantia e assistência técnica.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da CONTRATADA às sanções correlatas.

Item	Penalidade	Sanção	Limite
8	Atraso injustificado para a análise e correção dos itens (equipamento, serviço, software, licença), no atendimento de chamado de garantia e assistência técnica.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 10º (décimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 11.º (décimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **C O N T R A T A D A** às sanções correlatas.
9	Atraso injustificado para o fornecimento do TERMO DE GARANTIA E ASSISTÊNCIA TÉCNICA.	Multa de mora diária de **0,3% (três décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 10º (décimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 11.º (décimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **C O N T R A T A D A** às sanções correlatas.
10	Atraso injustificado na resposta aos pedidos de esclarecimentos de ordem técnica.	Multa de mora diária de **0,2% (dois décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 10º (décimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 11.º (décimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **C O N T R A T A D A** às sanções correlatas.
11	Deixar de cumprir qualquer outra obrigação não prevista neste contrato	Multa de mora diária de **1% (um por cento)** sobre o valor da Nota de Empenho	Limitada a sua aplicação até **15% (quinze por cento)**.

Item	Penalidade	Sanção	Limite
12	Quando, sem justificativa aceita pela **CONTRATANTE**, o vencedor não providenciar o devido cadastramento junto ao Sistema de Administração Financeira e Contabilidade – Cadastramento de Credores da SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ-AM, na forma prevista no Edital.	Multa de **2,5% (dois inteiros e cinco décimos por cento)** sobre o valor total da proposta.	Não se aplica.
13	Inexecução parcial do objeto contratado.	Multa de até **0,5% (cinco décimos por cento)** até **30% (trinta por cento)** sobre o valor da Nota de Empenho, sem prejuízo das demais sanções previstas.	Não se aplica.
14	Inexecução total do objeto.	Multa de até **5% (cinco por cento)** até **30% (trinta por cento**) sobre o valor total do contrato, sem prejuízo das demais sanções previstas.	Não se aplica.

1. Serão descontados dos pagamentos porventura devidos à **CONTRATADA** as importâncias alusivas a multas, ou efetuar sua cobrança mediante inscrição na dívida ativa do Estado, ou por qualquer outra forma prevista em lei.

2. Caso a **CONTRATANTE** determine, a multa deverá ser recolhida no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

3. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a **CONTRATANTE** poderá cobrar o valor remanescente judicialmente.

CLÁUSULA VIGÉSIMA – DO REAJUSTAMENTO DE PREÇOS:

Nos termos do art. 92, §§ 3º e 4°, I, da Lei n.º 14.133/2021, os preços inicialmente contratados poderão ser reajustados, por requerimento da **CONTRATADA**, desde

que observado o interregno mínimo de 12 (doze) meses, de acordo com a variação do Índice de Custo da Tecnologia da Informação (ICTI), computado pelo Instituto de Pesquisa Econômica Aplicada (Ipea), ou outro que venha substituí-lo, na forma e periodicidade regulamentadas.

1. Caberá à **CONTRATADA** efetuar os cálculos relativos ao reajustamento OU repactuação e demais documentos comprobatórios, submetendo-os à apreciação da **FISCALIZAÇÃO**.

2. O interregno mínimo de 12 (doze) meses para o primeiro reajustamento será contado a partir da data do orçamento estimado pela **CONTRATANTE**, que corresponderá à da assinatura do Quadro-Resumo de Compras, ocorrida em _____.

3. Nos reajustes subsequentes ao primeiro, o interregno de 12 (doze) meses será contado a partir da data de início dos efeitos financeiros do último reajustamento ocorrido.

4. O prazo para a **FISCALIZAÇÃO** responder ao pedido de reajustamento será de 1 (um) mês, contado do recebimento do pedido.

5. Conforme o art. 136, I, da Lei n.º 14.133/2021, o reajustamento poderá ser efetuado por simples apostila, salvo se coincidir com a porrogação contratual, hipótese em que deverá ser formalizado por termo aditivo.

6. Caso a **CONTRATADA** não requeira tempestivamente o reajustamento e prorrogue o contrato sem pleiteá-lo, ocorrerá a preclusão do direito.

7. A **CONTRATANTE** poderá restabelecer o equilíbrio econômico-financeiro do ajuste em seu favor, visando à adequação dos preços contratuais, quando se verificar que houve redução dos preços dos serviços no mercado, observando-se o disposto no art. 124 da Lei n.º 14.133/2021.

8. A **FISCALIZAÇÃO** poderá solicitar à **CONTRATADA**, durante a vigência deste contrato, a revisão dos preços e dos percentuais de desconto contratados quando o contrato mostrar-se desvantajoso para a Administração.

9. Nos termos do art. 124, II, "d", da Lei n.º 14.133/2021, ainda que não decorrido o interregno mínimo de 1 (um) ano a que se refere o item 2 desta cláusula, a **CONTRATADA** poderá pleitear à **FISCALIZAÇÃO** o reequilíbrio econômico-financeiro inicial do contrato em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução do contrato tal como pactuado, respeitada, em qualquer caso, a repartição objetiva de risco estabelecida no contrato.

CLÁUSULA VIGÉSIMA PRIMEIRA – DA ALTERAÇÃO DO CONTRATO:

Nos termos dos arts. 124 e seguintes da Lei n.º 14.133/2021, o presente contrato pode ser alterado pelas partes, mediante termo aditivo.

1. A **CONTRATADA** é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

2. As supressões e acréscimos resultantes de acordo celebrado entre a **CONTRATADA** e a **CONTRATANTE** poderão exceder os limites estipulados no item anterior.

3. Nos termos do art. 136 da Lei n.º 14.133/2021, registros que não caracterizam alteração do contrato poderão ser formalizados por simples

apostila.

CLÁUSULA VIGÉSIMA SEGUNDA – DA EXTINÇÃO DO CONTRATO:

O contrato se extingue quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

1. A extinção do contrato por vencimento do prazo não exonerará a **CONTRATADA** de suas responsabilidades contratuais nem das sanções que porventura lhe forem aplicadas.

1.1 A extinção a que alude este item não prejudicará o andamento de procedimento apuratório em face da **CONTRATADA**.

2. O contrato pode ser extinto antes do prazo nele fixado, sem ônus para a **CONTRATANTE**, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

2.1 A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação do contratado pelo contratante nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia.

2.2 Caso a notificação da não continuidade do contrato de que trata este item ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

3. O contrato pode ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no art. 137 da Lei n.º 14.133/21, bem como consensualmente, assegurados o contraditório e a ampla defesa.

3.1 Nessas hipóteses, aplicam-se os arts. 138 e 139 da mesma Lei.

3.2 A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a rescisão se não restringir sua capacidade de concluir o contrato.

3.3 Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

4. O termo de rescisão, sempre que possível, será precedido de:

4.1 Indenizações e multas.

4.2 Relação dos pagamentos já efetuados e ainda devidos;

4.3 Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos.

5. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório, nos termos do art. 131, caput, da Lei n.º 14.133/2021.

CLÁUSULA VIGÉSIMA TERCEIRA – DA RESERVA DE CARGOS:

Nos termos do art. 92, XVII, da Lei n.º 14.133/2021, a **CONTRATADA**, durante toda a vigência contratual, cumprirá a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz.

CLÁUSULA VIGÉSIMA QUARTA – DA PUBLICAÇÃO:

O presente contrato será publicado no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei n.º 14.133, de 2021, e sob a forma de extrato, no Diário Oficial Eletrônico do Ministério Público do Estado do Amazonas, após a sua assinatura, correndo as despesas por conta da **CONTRATANTE**, nos termos do art. 88, §2º, XV, do Ato n.º 008/2024/PGJ.

1. O contrato em sua íntegra será publicado no sítio oficial do Ministério Público do Estado do Amazonas, por meio do Portal da Transparência, nos termos do art. 91, caput, da Lei n.º 14.133/2021, e do art. 5º, II, da Resolução n.º 86/2012, do Conselho Nacional do Ministério Público - CNMP.

CLÁUSULA VIGÉSIMA QUINTA – DAS NORMAS APLICÁVEIS:

A **CONTRATADA** declara conhecer todas as normas abaixo e concorda em sujeitar-se às estipulações, sistemas de penalidades e demais regras delas constantes, mesmo que não expressamente transcritas no presente instrumento:

1. Lei n.º 14.133/2021 – Licitações e Contratos;

2. Lei n.º 10.406/2002 – Código Civil Brasileiro;

3. Lei n.º 8.078/1990 – Código de Defesa do Consumidor;

4. Decreto Federal n.º 6.481/2008 – Lista de Piores Formas de Trabalho Infantil;

5. Resolução n.º 37/2009, do Conselho Nacional do Ministério Público – CNMP;

6. Instrução Normativa n.º 5/2017, do Ministério do Planejamento, Desenvolvimento e Gestão, de forma subsidiária;

7. Ato n.º 008/2024/PGJ – Procedimentos Administrativos de Contratação de Bens e Serviços no Âmbito do Ministério Público do Estado do Amazonas; e

8. Demais legislações correlatas, de forma suplementar, à luz das normas específicas vigentes.

CLÁUSULA VIGÉSIMA SEXTA – DAS DISPOSIÇÕES FINAIS E DOS CASOS OMISSOS:

A **CONTRATADA**, em cumprimento à Resolução n.º 37/2009 do Conselho Nacional do Ministério Público e ao art. 48, parágrafo único, da Lei n.º 14.133/2021, declara que não possui cônjuge, companheira ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do Ministério Público do Estado do Amazonas.

1. A **CONTRATADA** e seus representantes legais apresentaram neste ato os documentos comprobatórios de suas condições jurídico-pessoais indispensáveis à lavratura do presente, inclusive a Certificação de Regularidade dos órgãos fiscais previdenciários públicos, a que estiver vinculada.

2. Os casos omissos neste contrato serão resolvidos pela Administração Superior da **CONTRATANTE***,* baseados na legislação vigente.

CLÁUSULA VIGÉSIMA SÉTIMA – DO FORO CONTRATUAL:

As questões decorrentes da execução deste instrumento, que não possam ser dirimidas administrativamente, serão processadas e julgadas na justiça estadual, no

foro de Manaus/AM, com expressa renúncia da **CONTRATADA** a qualquer outro que tenha ou venha a ter, por mais privilegiado que seja.

E, por estarem de acordo, foi o presente termo de contrato, depois de lido e anuído, assinado digitalmente pelas partes e por duas testemunhas.

Manaus, data da última assinatura eletrônica das partes.

(assinado eletronicamente)
ANDRÉ VIRGÍLIO BELOTA SEFFAIR
Subprocurador-Geral de Justiça para Assuntos Administrativos
Ministério Público do Estado do Amazonas

(assinado eletronicamente)
_____
Representante Legal da Contratada
Empresa _____

Documento assinado eletronicamente por **Adenilson Roberto de Oliveira Filho**, **Chefe da Divisão de Contratos e Convênios - DCCON**, em 17/12/2025, às 09:19, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2031978** e o código CRC **BCDBF304**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Av. Coronel Teixeira,nº 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MEMORANDO Nº 458.2025.DCCON - CONTRATOS.2032266.2025.007562

Manaus, [data da assinatura eletrônica].

À Senhora
SARAH MADALENA BARBOSA CORTES DE MELO
Presidente da Comissão Permanente de Licitação - CPL

Assunto: Encaminha a Minuta de Contrato Administrativo n.º 68.2025.DCCON - CONTRATOS.2031978.2025.007562 (2031978).

Senhora Presidente,

Em cumprimento ao Ofício n.º 479.2025.CPL.2031552.2025.007562 (2031552), esta Divisão de Contratos e Convênios (DCCON) remete o esboço contratual em epígrafe, cujo objeto é o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, observando o novel Termo de Referência n.º 28.2025.DTIC.2002143.2025.007562 (2002143)

Atenciosamente,

[*assinado eletronicamente*]
ADENILSON ROBERTO DE OLIVEIRA FILHO
Chefe da Divisão de Contratos e Convênios
Ministério Público do Estado do Amazonas

Documento assinado eletronicamente por **Adenilson Roberto de Oliveira Filho**, **Chefe da Divisão de Contratos e Convênios - DCCON**, em 17/12/2025, às 09:19, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2032266** e o código CRC **DABD3009**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Av. Coronel Teixeira,nº 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MINUTA DE CONTRATO ADMINISTRATIVO Nº 69.2025.DCCON - CONTRATOS.2033432.2025.007562

Processo SEI n.º 2025.007562

Licitação ou Contratação Direta n.º _____

Contrato Administrativo n.º _____

Termo de Contrato Administrativo que entre si celebram o **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS** e a empresa _____, visando ao o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais da **CONTRATANTE**.

O **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**, por intermédio de sua **PROCURADORIA-GERAL DE JUSTIÇA**, órgão de sua Administração Superior, com sede na cidade de Manaus, Estado do Amazonas, na Avenida Coronel Teixeira, 7.995 – Nova Esperança, 69.037-473, inscrito no CNPJ (MF) sob o n.º 04.153.748/0001-85, doravante denominada **CONTRATANTE**, neste ato representada por seu Subprocurador-Geral de Justiça para Assuntos Administrativos, o Exmo. Sr. **André Virgílio Belota Seffair**, residente e domiciliado em Manaus/AM, inscito no CPF sob o n.º ***.287.772-**, e a empresa _____, inscrita no CNPJ (MF) sob o n.º _____, com sede na _____, _____, daqui por diante denominada **CONTRATADA**, neste ato representada por _____, inscrito no CPF (MF) sob o n.º _____, tendo em vista o que consta no **Processo n.º 2025.007562**, doravante denominado **PROCESSO**, e em consequência do _____, firmam o presente **TERMO DE CONTRATO ADMINISTRATIVO N.º _____**, nos moldes da Lei n.º 14.133/2021 e mediante as cláusulas a seguir estabelecidas:

CLÁUSULA PRIMEIRA – DO OBJETO:

O objeto deste ajuste consiste no fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais da **CONTRATANTE**.

CLÁUSULA SEGUNDA – DO DETALHAMENTO DO OBJETO:

O objeto deste instrumento compreende a contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais da **CONTRATANTE**.

1. Por tratar-se de solução integrada, em que o funcionamento efetivo e satisfatório depende de cada um dos seus itens em conjunto, como um todo, ou seja, o simples funcionamento de itens separadamente não tem nenhuma funcionalidade, conforme indicado no Estudo Técnico Preliminar (ETP), a contratação terá lote único, organizado conforme tabela a seguir:

ITEM	DESCRIÇÃO	QUANTIDADE
01	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9	4
02	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU	1
03	SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX	5
04	SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU	1
05	LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE	50
06	SOFTWARE DE BACKUP DE DADOS	1
07	EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	1
08	SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	1
09	SWITCH CORE	2

2. Nas especificações técnicas mínimas apresentadas a seguir, os termos "possui", "permite", "suporta" e "é" implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo "ou" implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo "e" implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções citadas.

3. A **CONTRATADA** não poderá oferecer serviço inferior as especificações apresentadas neste Termo, sendo permitido, porém, a oferta de serviço superior as especificações mínimas apresentadas, de acordo com a conveniência da **CONTRATADA** e aprovação da **CONTRATANTE**.

4. Toda documentação gerada durante a prestação dos serviços será de propriedade da **CONTRATANTE**, em virtude de sua elaboração tomar por base informações críticas do funcionamento intrínseco à sua infraestrutura, que afetam diretamente a segurança da **CONTRATANTE**.

5. A **CONTRATADA** deverá guardar inteiro sigilo dos serviços contratados e dos dados processados, bem como de toda e qualquer documentação gerada, reconhecendo serem esses de propriedade e uso exclusivo da **CONTRATANTE**, sendo vedada sua cessão, locação ou venda a terceiros.

6. **CONTRATADA** deverá manter a **CONTRATANTE** atualizada sobre todos os fluxos adotados para a execução das atividades objeto da contratação durante o período contratual, bem como sobre a forma de automatização de quaisquer serviços, documentando todos os procedimentos detalhadamente para que possam servir de base para a continuidade dos serviços independentemente da metodologia que possa ser adotada.

7 . ITEM 01 - EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9

7.1 Características Gerais

7.1.1 A infraestrutura deverá ser composta por appliances Nutanix com integração completa entre hardware e software, armazenamento e rede, entregando uma solução hiperconvergente pronta para operação.

7.1.2 Serão aceitos apenas appliances homologados pela Nutanix para uso com o Nutanix AOS (Acropolis Operating System) e Nutanix AHV (Acropolis Hypervisor) ou outro hipervisor suportado pela plataforma.

7.1.3 Caso necessário, será permitida a entrega de equipamentos ou recursos adicionais para atender aos requisitos mínimos, desde que todos os componentes estejam integrados e certificados pela Nutanix.

7.1.4 É permitida a entrega de múltiplos nós em um único chassi, desde que compatível com a arquitetura Nutanix.

7.1.5 A solução deve incluir a ferramenta Nutanix Prism, em sua ultima versão ou equivalente, que oferece gerenciamento centralizado e interface gráfica para monitoramento, atualizações e operação da infraestrutura, incluindo:

7.1.5.1 Atualização de BIOS, firmware, hipervisor e SDS;

7.1.5.2 Visualização do hardware físico;

7.1.5.3 Diagnóstico, inventário e expansão de nós.

7.1.6 Caso alguma funcionalidade não esteja disponível via Prism ou equivalente para monitoramento ou atualização, a CONTRATADA deverá realizar este serviço de forma remota/on-line ou presencial.

7.1.7 Todas as atualizações devem ser homologadas pela Nutanix e aplicadas conforme as melhores práticas da fabricante. Esta ferramenta deve ser gráfica, com suporte a apresentação de visões do hardware físico dos nós, suporte a troca de drives, com controle do inventário, com ferramenta de diagnóstico e com módulo para a

adição de novos nós.

7.1.8 A arquitetura deve garantir alta disponibilidade (HA) e resiliência a falhas, com suporte a recuperação de desastres (DR).

7.1.9 Os appliances devem permitir expansão modular e não disruptiva dos serviços de rede e aplicações, com detecção automática de novos nós.

7.1.10 Deve centralizar o armazenamento de dados em discos compartilhados, redundantes.

7.1.11 Cada nó deverá conter armazenamento dedicado para o sistema operacional da plataforma.

7.1.12 A solução deve estar preparada para ambientes de virtualização em alta disponibilidade, conforme as práticas recomendadas pela Nutanix.

7.1.13 Deve suportar software de virtualização para consolidação de servidores e recuperação automática em caso de falhas físicas, minimizando o downtime.

7.1.14 A entrega deve ser feita com todos os componentes física e logicamente integrados, sem ponto único de falha, com acesso imediato ao ambiente via sistema de gestão da plataforma após energização e conexão.

7.1.15 A instalação deve ser compatível com racks padrão de 19 polegadas, incluindo todos os acessórios necessários para montagem no ambiente da CONTRATANTE.

7.1.16 O equipamento deve integrar a linha de produtos Nutanix da família “NX”, assegurando total compatibilidade com atual ambiente e possibilidade de expansão das zonas de disponibilidade já estabelecidas, conforme informações disponibilizadas no endereço eletrônico oficial da fabricante: https://www.nutanix.com/products/hardwareplatforms/specsheet?platformProvider=Nutanix.

7.2 Configuração do Nó ou Chassi

7.2.1 Serão admitidas ofertas de chassis que comportam múltiplos servidores (nós/nodes), para o atendimento da especificação técnica.

7.2.2 Cada nó, ou chassi, deverá possuir ventiladores e fontes redundantes para a operação adequada dos equipamentos.

7.2.3 Todas as fontes de alimentação deverão ser acompanhadas de seus respectivos cabos de energia compatíveis.

7.3 Características de Processamento por Nó

7.3.1 Cada servidor deverá possuir, no mínimo, 02 (dois) processadores com arquitetura x86, voltados ao uso em servidores, contendo as seguintes características mínimas:

7.3.1.1 12 (doze) núcleos físicos e 24 (vinte e quatro) threads por processador;

7.3.1.2 Frequência de clock nominal de, no mínimo, 2,4 GHz;

7.3.1.3 Controladora de memória integrada com suporte à tecnologia DDR5 ou superior.

7.3.2 Será admitida a entrega de processadores de geração superior ao modelo originalmente especificado, desde que mantenham no mínimo a mesma quantidade de núcleos e threads, independentemente de demais especificações.

7.4 Especificações de Memória por Nó

7.4.1 Cada servidor deverá ser fornecido com, no mínimo, 1.536 GB (um mil quinhentos e trinta e seis gigabytes) de memória RAM, distribuída uniformemente entre os processadores, utilizando módulos DDR5 ou superior.

7.5 Especificações de Rede por Nó

7.5.1 Cada servidor deverá ser entregue com as seguintes interfaces de rede:

7.5.1.1 Mínimo de 2 (duas) interfaces de 25/10 GbE SFP28, integradas em uma placa de rede;

7.5.1.2 Mínimo de 1 (uma) interface exclusiva de gerenciamento Ethernet 1000Base-T.

7.5.2 A interface de gerenciamento deverá vir acompanhada de cabos UTP categoria 6 (ou superior), com comprimento mínimo de 5 (cinco) metros e conectores RJ-45.

7.6 Especificações de Armazenamento por Nó

7.6.1 Cada servidor deverá ser entregue com a seguinte configuração mínima de discos:

7.6.1.1 04 (quatro) unidades de SSD NVMe, ou SSD SAS/SATA, com capacidade mínima de 3,84 TB por unidade (volumetria bruta);

7.6.1.2 08 (oito) unidades de disco rígido (HDD), com capacidade mínima de 12 TB por unidade (volumetria bruta).

8 . ITEM 02 - EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU

8.1 Características Gerais

8.1.1 A solução deverá ser composta exclusivamente por appliances de nuvem privada, com integração total entre recursos de computação, armazenamento e rede, entregues como infraestrutura unificada.

8.1.2 Serão aceitos apenas appliances homologados para uso com a solução de armazenamento definido por software (Software Defined Storage – SDS) ofertada.

8.1.3 A entrega de equipamentos ou recursos adicionais será aceita, desde que necessária para o atendimento aos requisitos mínimos e que todos os componentes estejam devidamente integrados.

8.1.4 É permitida a entrega de múltiplos nós consolidados em um único chassi modular.

8.1.5 A solução deverá incluir ferramenta unificada de gerenciamento e atualização, com capacidade de monitorar e atualizar BIOS, firmwares, hypervisor e componentes do SDS. Caso não realize todos os procedimentos listados, a CONTRATADA deverá garantir a execução dessas tarefas presencial ou remotamente.

8.1.6 A ferramenta de gestão deverá ser gráfica, com visualização física dos nós, suporte à substituição de drives, inventário automatizado, diagnóstico integrado e capacidade de adicionar novos nós ao cluster.

8.1.7 A arquitetura deverá contemplar alta disponibilidade nativa e recursos para recuperação de desastres (DR), de forma a garantir continuidade dos serviços mesmo em caso de falhas parciais.

8.1.8 Os equipamentos devem possuir arquitetura modular, permitindo expansão de capacidade com inclusão de novos appliances sem interrupção dos serviços.

8.1.9 O armazenamento deverá ser centralizado, com discos compartilhados e redundância nativa.

8.1.10 Cada servidor deverá conter unidade de armazenamento dedicada ao sistema operacional da plataforma e aos softwares de virtualização e processamento gráfico.

8.1.11 A infraestrutura deverá estar preparada para suportar ambientes virtualizados de alta disponibilidade, de acordo com as boas práticas do fabricante da solução.

8.1.12 A solução deverá oferecer suporte a consolidação de servidores e recuperação automática em caso de falhas físicas.

8.1.13 A entrega deverá ocorrer com a solução fisicamente e logicamente pré-integrada, sem ponto único de falha, com acesso imediato à plataforma após energização e conexão física.

8.1.14 A instalação deverá ser compatível com racks padrão de 19", com todos os acessórios de fixação inclusos.

8.1.15 O equipamento deve integrar a linha de produtos Nutanix da família “NX”, assegurando total compatibilidade com atual ambiente e possibilidade de expansão das zonas de disponibilidade já estabelecidas, conforme informações disponibilizadas no endereço eletrônico oficial da fabricante: https://www.nutanix.com/products/hardwareplatforms/specsheet?platformProvider=Nutanix.

8.2 Configuração do Nó ou Chassi

8.2.1 Serão admitidas ofertas de chassis que comportam múltiplos servidores (nós/nodes), para o atendimento da especificação técnica.

8.2.2 Cada nó ou chassi deverá possuir ventiladores e fontes de alimentação redundantes.

8.2.3 Cada fonte deverá ser entregue com seu respectivo cabo de energia.

8.3 Características de Processamento por Nó

8.3.1 Cada servidor deverá possuir, no mínimo, dois processadores com arquitetura x86, dedicados a ambientes de datacenter, com as seguintes características:

8.3.2 12 (doze) núcleos físicos e 24 (vinte e quatro) threads por processador;

8.3.3 Frequência mínima de 2,4 GHz;

8.3.4 Controladora de memória integrada DDR5 ou superior.

8.3.5 A substituição por processadores mais recentes será aceita, desde que observadas as quantidades mínimas de núcleos e threads.

8.4 Especificações de Memória por Nó

8.4.1 - Cada servidor deverá ser entregue com no mínimo 1.024 GB (um mil e vinte e quatro gigabytes) de memória RAM, utilizando módulos DDR5 ou superior, distribuídos de forma equilibrada entre os processadores.

8.5 Especificações de Rede por Nó

8.5.1 Cada servidor deverá conter no mínimo:

8.5.1.1 2 (duas) interfaces de rede 25/10 GbE SFP28;

8.5.1.2 1 (uma) interface de gerenciamento 1000Base-T;

8.5.1.3 A interface de gerenciamento deverá ser acompanhada de cabos UTP Cat-6 ou superior, com 5 metros de comprimento e conectores RJ-45.

8.6 Especificações de Armazenamento por Nó

8.6.1 Cada servidor deverá ser entregue com:

8.6.1.1 2 discos SSD NVMe, SAS ou SATA, com capacidade mínima de 3,84 TB cada (volumetria bruta);

8.6.1.2 4 discos HDD com capacidade mínima de 12 TB cada (volumetria bruta).

8.7 Especificações de Processamento Gráfico e Cálculo Aritmético

8.7.1 Cada servidor deverá conter uma placa gráfica com as seguintes características:

8.7.1.1 48 GB de memória GDDR6 de GPU;

8.7.1.2 Interconexão PCIe Gen4 com largura de banda de 64 GB/s;

8.7.1.3 Suporte a DirectX 12.075, Shader Model 5.175, OpenGL 4.686 e Vulkan 1.186;

8.7.1.4 Compatibilidade com NVIDIA vPC/vApps, NVIDIA RTX Virtual Workstation e NVIDIA Virtual Compute Server;

8.7.1.5 Consumo máximo de 350W.

9 . ITEM 03 – SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX

9.1 Camada de Armazenamento da Solução:

9.1.1 A solução deverá contar com camada de armazenamento compartilhada entre todos os servidores e appliances descritos neste Termo, utilizando tecnologia de armazenamento definido por software (Software Defined Storage – SDS).

9.1.2 A arquitetura de armazenamento deverá ser otimizada para ambientes virtuais, com escalabilidade contínua e elástica, permitindo expansão de capacidade pela adição de novos nós/appliances sem necessidade de licenciamento adicional de virtualização.

9.1.3 Não serão aceitas soluções baseadas em tecnologia RAID para redundância de dados.

9.1.4 A solução deverá suportar as tecnologias de compressão e desduplicação de dados inline, near-line ou pós-processada, com o objetivo de otimização do armazenamento.

9.1.5 A solução deverá prover recursos de QoS (Quality of Service), para controle do volume de I/Os de VMs.

9.1.6 Deverá permitir uso de técnicas de Erasure Coding para otimização de aplicações com baixa sensibilidade à latência de escrita.

9.1.7 A solução deverá permitir a expansão do cluster através da adição de nós/servidores que incrementem tão somente a capacidade de armazenamento, sem a necessidade de emprego de licenças de virtualização nesses nós/servidores;

9.1.8 A substituição de discos defeituosos deverá ocorrer sem impacto nas operações de leitura e escrita das aplicações.

9.1.9 A falha de um nó da solução não poderá comprometer a disponibilidade da camada de armazenamento das VMs.

9.1.10 A criptografia deverá ser aplicada em nível de cluster ou volume, via hardware ou software, com KMS nativo. Caso não possua, será aceita entrega de servidor redundante externo com essa funcionalidade.

9.1.11 A distribuição dos dados deverá ocorrer de forma automática e uniforme dentro do cluster.

9.1.12 A solução deverá permitir criação de cópias no tempo (snapshots) sem movimentação dos dados originais e com redirecionamento de escritas subsequentes.

9.1.13 Deverá suportar clonagem de instâncias virtuais a partir de snapshots, sem movimentação dos dados.

9.1.14 Acesso ao armazenamento deverá ser possível via iSCSI por instâncias físicas ou virtuais externas ao cluster, garantindo suporte a aplicações de alta disponibilidade.

9.2 Tecnologia de Replicação e Proteção de Dados:

9.2.1 Deverá ser fornecida funcionalidade de replicação local realizando clones e snapshots com proteção contínua dos dados da máquina virtual.

9.2.2 A solução deve prover as funcionalidades de Thin Provisioning e Serviços de Cópias de dados.

9.2.3 Deverá permitir a configuração de um grupo ou domínio de proteção de instâncias virtuais, que poderão ser protegidas por cópias point-in-time, bem como replicadas para um cluster remoto.

9.2.4 Deverá permitir a união de máquinas virtuais em um único grupo de proteção.

9.2.5 Deverá proteger, por cópias point-in-time, simultaneamente todas as máquinas virtuais pertencentes ao grupo.

9.2.6 Deverá contemplar, também, a proteção nativa de máquinas virtuais consistentes com aplicações, onde há proteção dos dados em memória a partir da movimentação das operações de escrita para disco, de sistemas operacionais Linux e Windows. Caso a plataforma de nuvem privada não permita executar esta funcionalidade

nativamente, a CONTRATADA deverá atender este requisito compondo com outra solução.

9.2.7 Deverá permitir a configuração de uma entidade capaz de centralizar todo o fluxo do tráfego replicado entre clusters distintos, convergindo assim os recursos para um único ponto focal. Esse recurso centralizado deverá posteriormente redirecionar o tráfego corretamente para os equipamentos específicos do cluster de contingência.

9.2.8 Deverá permitir ajustar o consumo de banda em replicações.

9.2.9 Deverá permitir a existência de frequências distintas de replicação para instâncias virtuais em grupos diferentes.

9.3 Gerenciamento Integrado:

9.3.1 A solução deve oferecer solução de gerenciamento integrado, licenciado para gerenciar inclusive múltiplos clusters.

9.3.2 Monitoração automática e periódica da solução, com o envio de notificações preventivamente em caso de falhas, notificando o suporte do fornecedor a tomar medidas preventivas e acordadas com a CONTRATANTE a fim de evitar tempo de inatividade e impactos na produção.

9.3.3 Deve oferecer portal de acesso do próprio fornecedor para download de atualizações e de softwares agregados.

9.3.4 A ferramenta de gerenciamento, local, deve fornecer um dashboard reportando a utilização dos recursos do cluster como CPU, Memória, Armazenamento, IOPS do cluster, largura de banda do cluster, latência do cluster e informações sobre o virtualizador empregado e os alertas de saúde.

9.3.5 A solução deve fornecer atualização de todos os componentes (Firmware, e softwares de virtualização que fazem parte da solução) em forma de pacote com instalação assistida.

9.3.6 Contemplar as funcionalidades como:

9.3.6.1 Emissão de relatório avançados do ambiente;

9.3.6.2 Personalização da console principal;

9.3.6.3 Planejamento e previsão de capacidade;

9.3.6.4 Detecção de ineficiência de cargas de trabalho e dimensionamento ideal;

9.3.6.5 Planejamento de capacidade ou cargas de trabalho ao longo do tempo;

9.3.6.6 Permitir automação de operações de gerência do ambiente.

9.4 Provisionamento de Containers:

9.4.1 Deverá ser entregue uma plataforma de provisionamento de containers, integrada, a plataforma de virtualização.

9.4.2 A plataforma deverá permitir a criação de múltiplo clusters.

9.4.3 A fabricante da solução deverá, comprovadamente, pertencer a categoria de membro da CNCF (Cloud Native Computing Foundation).

9.4.4 Seleção de sistemas operacionais, bem como suas distintas versões de microcódigo para implementação automática, sendo compatível com sistemas Linux.

9.4.5 Seleção das configurações de rede do cluster de containers ou microserviços.

9.4.6 Seleção do tipo de armazenamento persistente a ser empregado em containers.

9.4.7 Seleção da quantidade de nós dos tipos “Control Plane” e “Workers” que serão implementados simultaneamente.

9.4.8 A plataforma de containers deverá permitir a criação de alertas, facilitando a gestão do cluster.

9.4.9 Deverá ter suporte a implementação de clusters de plataformas de containers, similares a Kubernetes, NCI, baremetal, public cloud.

9.4.10 A plataforma de containers deverá possuir integração para o acesso através de RBAC, permitindo seu uso completo através de acesso administrativo e permitindo seu uso parcial através de acesso controlado aos demais usuários.

9.4.11 Suporte implementação de clusters de plataformas de containers, similares a Kubernetes com suporte a Bring-Your-Own-OS: Rocky Linux, Ubuntu, RHEL e similares.

9.4.12 Permitir a configuração de clusters com alta-disponibilidade para os “Control Plane” nodes, com ou sem balanceador de carga;

9.4.13 Prover armazenamento persistente através de integração com Container Storage Interface (CSI), para armazenamento de blocos e arquivos. Também deverá ser possível configurar armazenamento de arquivos compatível com protocolo Simple Storage Service;

9.4.14 Deverá fornecer um mecanismo de monitoramento que aciona alertas no cluster Kubernetes;

9.4.15 Oferecer as seguintes funcionalidades em ambiente Kubernetes:

9.4.15.1 Gerenciamento de Dados;

9.4.15.2 Proteção e Restauração de Dados;

9.4.15.3 Aceleração da Entrega de Aplicativos;

9.4.15.4 Gerenciamento de Autoatendimento de Aplicativos;

9.4.15.5 Automação e Monitoramento de Infraestrutura;

9.4.15.6 Padronização de Políticas de Governança e Conformidade;

9.4.16 Para a estratégia de criação de cópias dos dados para ambiente de containers Kubernetes, a solução deverá permitir:

9.4.16.1 Fornecimento de software para “worker nodes” Kubernetes, garantindo o suporte unificado e conjunto da solução como um todo;

9.4.16.2 Plataformas de container baseadas em Kubernetes.

9.4.16.3 Permitira realização de copias e armazenamento em repositório externo.

9.4.16.4 Movimentação das imagens de backup para compartilhamentos NFS por meio de solução de armazenamento compatível com protocolo S3, permitindo que o repositório NFS seja utilizado como backend de Object Storage.

9.4.16.5 Capacidade de restaurar o Namespace para seu local original e para um novo Namespace.

9.5 Segurança de Rede:

9.5.1 Suportar microssegmentação para prover controle granular e governança de todo o tráfego de entrada e saída de uma máquina virtual (VM), grupos de máquinas virtuais (VMs) e containers.

9.5.2 Permitir a associação de políticas de rede a VMs e conteiners em vez de segmentos de rede específicos (por exemplo VLANs) ou identificadores (endereços IP ou MAC).

9.5.3 Prover visualização de tráfego e relacionamentos com a descoberta automática dos fluxos entre as máquinas virtuais e containers.

9.5.4 Permitir políticas de segurança centradas na carga de trabalho em vez de uma abordagem centrada na rede, permitindo examinar o tráfego de, e para as VMs, independentemente de como as configurações de rede mudam e onde residem no data center

9.5.5 Políticas aplicadas por categorias de VMs e containers.

9.5.6 Permitir isolamento de conteiners e VMs comprometidas, colocando-a em quarentena.

9.5.7 - Permitir restrição de tráfego entre camadas de aplicação.

9.5.8 Atualização automática de políticas.

9.5.9 Integração com ferramentas de terceiros como IDS/IPS e load balancer.

9.6 Licenciamento do Software de Virtualização:

9.6.1 Entrega do licenciamento completo da plataforma de virtualização, versão mais avançada.

9.6.2 Suporte à criação de VMs com múltiplas interfaces de rede e múltiplas arquiteturas (32/64 bits).

9.6.3 Permitir provisionamento aos principais sistemas operacionais (Windows Server 2022, CentOS 8, Ubuntu 20, RHEL 9) ou superiores.

9.6.4 Alocação dinâmica de recursos (CPU/RAM).

9.6.5 Hypervisor deverá estar instalado em unidade flash dedicada.

9.6.6 Suporte a GPU virtual ou passthrough nativo.

9.6.7 Suporte a BIOS/UEFI, snapshots, exportação OVA.

9.6.8 Deverá permitir o provisionamento de máquinas virtuais, e grupos de máquinas virtuais, em equipamentos específicos com o propósito de respeitar licenciamentos de aplicações. Em caso de falha do equipamento, a máquina virtual não deverá ser migrada para outro equipamento remanescente;

9.6.9 Alta resiliência a falhas de nós/discos.

9.6.10 Armazenamento distribuído e gerenciado via console web.

9.6.11 Deverá permitir a inicialização, a reinicialização, o reset, o desligamento da VM e o desligamento do sistema operacional dela;

9.6.12 Suportar a tecnologia de snapshot nativos do Hypervisor;

9.6.13 Permitir a adição de novos servidores no cluster;

9.6.14 Permitir criar uma área de armazenamento compartilhada, distribuída e otimizada para ambientes virtuais;

9.6.15 Permitir o agrupamento dos volumes lógicos de todos os servidores no cluster provendo uma área de armazenamento comum para o ambiente virtual;

9.6.16 Possuir mecanismo de redundância e proteção de dados nativo que armazena cópias dos dados em diversos discos e hosts do cluster de forma transparente;

9.6.17 Deverá ser fornecido licenciamento do software de virtualização na versão mais completa para todos os servidores do ambiente de armazenamento distribuído.

9.6.18 Deverá contemplar pelo menos 20 (vinte) núcleos de processamento virtuais (vCPU) ou físicos (pCPU) de solução para gestão de base de dados como serviço (DBaaS).

9.6.19 Deverá ser totalmente compatível com a solução ofertada para atendimento aos requisitos deste termo de referência.

9.6.20 Permitir automatizar as tarefas para provisionamento, emprego de correções de software (patching), gerenciamento do ciclo de vida, clonagem, atualização dos dados em bases clonadas (refresh), proteção contínua e recuperação de bases de dados.

9.6.21 Deverá ser compatível pelo menos com Oracle, Microsoft SQL, PostgreSQL, MariaDB, MongoDB e MySQL.

9.6.22 Permitir o uso de uma chave SSH pública para acesso ao servidor de banco de dados com opção através do upload de um arquivo e através da inserção direta da chave em campo de texto.

9.6.23 A solução deverá permitir registrar bancos de dados existentes para emprego de proteção contínua capturando e mantendo snapshots e registros (logs) transacionais da base de dados de origem conforme definições contidas no agendamento.

9.6.24 A mesma tecnologia deverá permitir a clonagem de bases de dados.

9.6.25 Durante a clonagem, a solução deverá permitir a escolha para o administrador utilizar um servidor de banco de dados registrado ou criar um novo servidor.

9.6.26 Permitir que o administrador realize o clone de uma base de dados a partir de um snapshot.

9.6.27 Permitir que o administrador realize o clone de uma base de dados dentro de uma política de proteção contínua, ou seja, clonar uma base de dados em determinado dia, hora, minuto e segundo.

9.6.28 Permitir a definição de agendamento da periodicidade para realizar a atualização (refresh) dos dados da base clonada através do estado atual na base de dados de origem.

9.6.29 Permitir a definição de uma data para remoção ou exclusão do

clone.

9.6.30 Permitir a execução de scripts ou comandos de pré e pós clonagem.

9.6.31 Deverá ser possível definir as políticas de retenção dos snapshots diários, semanais, mensais e trimestrais.

10. ITEM 04 – SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU

10.1 Software para Processamento Gráfico e Cálculo Aritmético:

10.1.1 Permitir a seleção, implantação e gestão de modelos de IA Generativa (LLMs) provenientes da Hugging Face e NVIDIA, bem como a importação de modelos personalizados ou treinados pelo contratante em clusters Kubernetes.

10.1.10 Permitir a criação de um endpoint de inferência e o compartilhamento dele com desenvolvedores para incorporar em seus aplicativos de IA. Permitir gerenciar e validar esses endpoints para garantir que eles estejam configurados corretamente.

10.1.11 Permitir o acesso a um endpoint de inferência por um aplicativo usando chaves de API. O gerenciamento de chaves de API deverá permitir o fornecimento e revogação do acesso à API para garantir controles de segurança de acesso adequados.

10.1.12 Permitir o controle de acesso baseado em função (RBAC), para fornecer permissões de acesso personalizadas aos usuários com base em suas funções atribuídas.

10.1.13 Possuir uma interface de usuário simples e dinâmica que simplifique o processo de implantação.

10.1.14 Possuir um painel dinâmico que permita monitorar a integridade da implantação com ferramentas de monitoramento em tempo real que identifiquem gargalos, rastreiem o desempenho e solucionem problemas.

10.1.15 Suportar a instalação e o funcionamento em estruturas sem qualquer conexão com a Internet (dark-site ou air-gapped).

11. ITEM 05 - LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE

11.1 A solução deverá incluir unidade de subscrição de software para armazenamento de objetos e arquivos, licenciada por terabyte (TB), com suporte técnico durante 60 (sessenta) meses, contemplando ambiente de produção em operação contínua (24x7).

11.2 Caso a solução proposta não ofereça suporte nativo a armazenamento de objetos e arquivos, será permitida a utilização de unidade externa dedicada, desde que esta disponha de todos os componentes, funcionalidades e suporte equivalentes à solução principal.

11.3 O sistema de armazenamento definido (SDS) deverá otimizar dados utilizando tecnologia de erasure coding na camada de capacidade, de modo a garantir eficiência e resiliência no armazenamento de arquivos e objetos.

11.4 A solução deverá permitir a recuperação granular de arquivos pelos usuários, sem necessidade de intervenção do administrador.

11.4.1 Para o protocolo SMB, a restauração deverá ocorrer por meio

da funcionalidade “Versões Prévias” da pasta de destino.

11.4.2 Para o protocolo NFS, a recuperação deverá ser possível pela listagem do subdiretório oculto (snapshot).

11.5 O sistema deverá integrar-se a softwares antivírus de terceiros por meio do protocolo ICAP (Internet Content Adaptation Protocol), possibilitando varredura em tempo real de arquivos compartilhados via SMB sempre que forem abertos, modificados ou encerrados.

11.6 A interface de gerenciamento deverá exibir o estado dos arquivos após a varredura antivírus, incluindo status como limpo, em quarentena ou deletado, além do histórico de eventos correspondentes.

11.7 A interface de gerenciamento deverá também exibir relatórios detalhados contendo a lista de arquivos analisados, ameaças detectadas e arquivos colocados em quarentena.

11.8 A interface de gerenciamento deverá permitir ações diretas sobre os arquivos, incluindo:

11.8.1 Reexecução de varredura (Rescan);

11.8.2 Remoção de arquivos da quarentena;

11.8.3 Exclusão permanente de arquivos em quarentena.

11.9 A solução deverá possibilitar a configuração de ambiente de detecção avançada de intrusão (AIDE), capaz de identificar e corrigir automaticamente desvios na configuração de segurança do servidor de arquivos, sem necessidade de intervenção manual.

11.10 Deverá ser possível configurar políticas de senha forte (strong password) para o acesso à linha de comando (CLI) do servidor de arquivos.

11.11 O sistema deverá suportar configuração de qualidade de serviço (QoS), utilizando valores DSCP para diferenciação de códigos de serviço em rede.

11.12 Deverá suportar o protocolo NFS v4.2, otimizando as operações de entrada/saída (I/O) e reduzindo o consumo de rede.

11.13 A solução deverá contemplar as seguintes funcionalidades para compartilhamento de arquivos via protocolo SMB:

11.14 Autenticação integrada ao Active Directory.

11.15 Enumeração baseada em acesso (ABE), exibindo apenas pastas e arquivos aos quais o usuário possui permissão.

11.16 Assinatura digital de pacotes SMB (SMB Signing), garantindo autenticidade e integridade das transmissões.

11.17 Criptografia em nível de pasta (SMB Encryption), assegurando a confidencialidade dos dados.

11.18 Organização de compartilhamentos em um único espaço de nomes (Single Namespace), suportando ambientes locais ou geograficamente distribuídos, por meio do protocolo DFS-N (DFS Namespaces).

11.19 Suporte à autenticação via Active Directory e LDAP, além de acesso não gerenciado a compartilhamentos NFSv4 (autenticação LDAP) e NFSv3.

11.20 Suporte a acesso multiprotocolo (SMB e NFS) sobre o mesmo compartilhamento, preservando permissões via Windows ACLs e Unix mode bits.

11.21 Suporte a Home Shares por diretório, permitindo o provisionamento automático de pastas pessoais de usuário.

11.22 Suporte à aplicação de cotas de uso do sistema de arquivos, com notificações (soft limit) e bloqueio (hard limit), configuráveis por usuário, grupo ou diretório no momento da criação (Directory Level Quotas).

11.23 O módulo de armazenamento de objetos deverá possuir API REST compatível com AWS S3, apta a lidar com petabytes de dados não estruturados, atendendo casos de uso como backup, retenção de longo prazo e aplicações nativas de nuvem.

11.24 Deverá permitir que os usuários armazenem e gerenciem dados não estruturados em arquitetura de nuvem privada escalável.

11.25 A solução deverá permitir a gestão de objetos via interface gráfica de administração e via API REST compatível com S3, mediante autorização prévia do administrador.

11.26 Suportar integração com serviços de diretório (Microsoft Active Directory e OpenLDAP), possibilitando o controle de acesso a objetos.

11.27 Permitir o compartilhamento de buckets com usuários portadores de chaves de acesso, com delegação de permissões de leitura e escrita conforme o nível definido.

11.28 Exibir a listagem de buckets compartilhados, indicando os respectivos usuários com acesso.

11.29 Permitir o gerenciamento de buckets e objetos por meio de APIs REST compatíveis com a solução de gerenciamento central ou S3, mediante autorização administrativa.

11.30 Suportar o versionamento de múltiplas versões de um mesmo objeto dentro de um bucket.

11.31 Possibilitar a definição de regras de ciclo de vida, como exclusão automática de objetos ou versões após período determinado (dias, meses ou anos).

11.32 Implementar mecanismo de proteção contra exclusão ou alteração de objetos, com base em políticas de retenção WORM (Write-Once-Read-Many).

11.33 Disponibilizar painel de monitoramento de desempenho, apresentando requisições por segundo, taxa de banda (MB/s) e tempo médio de leitura (GET).

11.34 Suportar políticas de cotas de utilização, notificando usuários conforme o consumo de espaço ou número de buckets criados.

11.35 Suportar o envio de notificações em tempo real — como criação, deleção, leitura, gravação ou alteração de permissões — para fins de auditoria e retenção, compatível com servidores syslog ou sistemas equivalentes.

12. ITEM 06 - SOFTWARE DE BACKUP DE DADOS

12.1 Características Gerais do Licenciamento:

12.1.1 Aquisição de 200 (duzentas) licenças pelo período de 05 (cinco) anos ou 60 (sessenta) meses.

12.1.2 Não deverão existir limites quanto ao uso de agentes, conectores, repositórios de armazenamento, hosts físicos e outras

tecnologias agregadas a arquitetura da solução especificada.

12.1.3 Ser a última versão disponível, não será aceita a utilização de versões anteriores para cobrir algum item desse descritivo técnico.

12.1.4 Mostrar na console de gerenciamento a quantidade de licenças adquiridas e utilizadas.

12.1.5 Caso a solução ofertada necessite de algum banco de dados, o mesmo deverá ser fornecido devidamente licenciado sem nenhum custo extra.

12.1.6 A solução deve ser compatível com o Item 07 Equipamento de Armazenamento de Dados de Backup on-premises.

12.2 Cópia e Restauração de Dados:

12.2.1 Permitir o controle da banda utilizada durante a operação de cópia de proteção dos backups.

12.2.2 Ser capaz de realizar cópia de arquivos abertos sem que a consistência deles seja comprometida.

12.2.3 Possuir a opção de priorização de tarefas de proteção com opção de resumo da cópia caso uma atividade de menor prioridade seja colocada em estado de espera por uma tarefa de maior prioridade.

12.2.4 Possuir a funcionalidade de paralelizar a gravação dos dados em dispositivos de armazenamento (funcionalidade conhecida como multiplexação).

12.2.5 Ser capaz de enviar alertas através de e-mail com o objetivo de reportar eventos ocorridos na operação e configuração da solução.

12.2.6 Ser capaz de enviar traps SNMP (Simple Network Management Protocol) com o objetivo de reportar eventos ocorridos na operação da solução.

12.2.7 Possuir a funcionalidade de agendamento automático de tarefas de cópia.

12.2.8 Para um mesmo dado armazenado deve haver a possibilidade de configuração de diferentes períodos de retenção.

12.3 Gerenciamento das Operações de Proteção e Restauração:

12.3.1 Possuir interface única, que seja capaz de gerenciar e executar operações de proteção e recuperação dos sistemas operacionais Windows, Unix e Linux; ambiente de virtualização Acropolis Operating System; aplicações, Microsoft Active Directory e banco de dados Microsoft SQL Server, PostgreSQL e Oracle.

12.3.2 O acesso administrativo ao console do servidor de gerenciamento da solução poderá ser feito através de ferramenta disponibilizada no próprio software (console gráfico) ou através de navegador Web.

12.3.3 Implementar distribuição automática de carga entre os movimentadores de dados, ou seja, os dados oriundos dos clientes de backup deverão ser distribuídos de forma automática entre os servidores de cópia, e em caso de falha de um dos servidores, o cliente automaticamente irá encaminhar seus dados para o outro servidor de cópia ativo. Esta funcionalidade deverá ser nativa do

produto, e não pode ser construída com o uso de soluções baseadas em softwares de cluster de terceiros.

12.3.4 A base de dados para armazenamento do catálogo deverá possuir mecanismo de proteção (backup) das informações armazenadas no catálogo e funcionalidades de recuperação rápida do catálogo em caso de desastre.

12.4 Criptografia dos Dados Protegidos

12.4.1 Implementar criptografia de dados na origem (cliente de backup), de uma forma que seja garantido que o dado que trafegará na rede de modo criptografado.

12.4.2 Deverá implementar no mínimo chaves de criptografia de 128 bits ou 256 bits.

12.5 Desduplicação dos Dados Protegidos

12.5.1 Permitir uso da tecnologia de desduplicação de dados para toda a capacidade licenciada, eliminando blocos repetidos, para cópias e arquivamento em disco e movimentação de dados desduplicados, independentemente do quantitativo de dispositivos de armazenamento que compõem a infraestrutura da CONTRATANTE.

12.5.2 Implementar desduplicação de blocos na origem (client-side desduplication), de forma que o cliente envie apenas novos blocos de dados criados e/ou modificados a partir da última cópia total completa;

12.5.3 Implementar desduplicação de dados nos servidores de armazenamento (target desduplication), de forma que tais servidores tratem adequadamente blocos repetidos enviados pelos clientes, evitando assim o armazenamento de blocos redundantes;

12.5.4 Implementar desduplicação de dados em tarefas de cópia;

12.5.5 Implementar desduplicação e compressão em uma mesma tarefa;

12.5.6 Permitir a restauração granular de arquivos ou sistemas de arquivos a partir de cópias em disco ou fita. Em caso de backup armazenado em disco a recuperação granular poderá ser feito utilizando-se cópias que possam estar desduplicados;

12.6 Alertas e Relatórios da Proteção de Dados

12.6.1 Quantidade de rotinas de backup concluídos nas últimas 24 horas, nos últimos 30 dias e nos últimos 12 meses.

12.6.2 Quantidade de recuperações efetuadas nas últimas 24 horas, nos últimos 30 dias e nos últimos 12 meses.

12.6.3 Resumo de rotinas de backup concluídos com sucesso, com erro ou não concluídos.

12.6.4 Mostrar o total de licenças adquiridas e o total de licenças utilizadas e caso ocorra uma nova aquisição de licenças as novas licenças deverão constar nesse relatório.

12.6.5 Enviar os seguintes alertas via e-mail: rotina de backup finalizada com sucesso, rotina de backup finalizada com erro e rotina de backup com problema.

12.7 Fornecimento de licenciamento do Sistema Operacional

12.7.1 Fornecimento de licenciamento do sistema operacional Microsoft Windows Server Datacenter, baseado em núcleo (core-based licensing , para 48 cores físicos).

12.7.2 As licenças deverão ser entregues em formato eletrônico, acompanhadas de instruções para instalação e ativação, devendo incluir garantia mínima de 60 (sessenta) meses ou suporte técnico equivalente.

12.7.3 O licenciamento deverá ser compatível com servidores físicos e virtuais , observando o licenciamento mínimo exigido pela fabricante.

12.7.4 As licenças fornecidas deverão ser originais, legítimas e adquiridas por meio de canal autorizado da Microsoft, com comprovação documental no momento da entrega.

12.7.5 As licenças deverão ser entregues em formato eletrônico, acompanhadas de instruções para instalação e ativação, incluindo garantia mínima de 60 (sessenta) meses ou suporte técnico equivalente.

12.7.6 O item deverá ser plenamente compatível com a infraestrutura tecnológica do MPAM, em especial com ambientes físicos e virtuais já existentes.

12.7.7 Incluir Software Assurance (SA), garantindo direito a atualizações, suporte técnico estendido e benefícios de mobilidade de licenças durante todo o período contratual.

13. ITEM 07 - EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES

13.1 Características gerais:

13.1.1 Deverá corresponder a um sistema inteligente dedicado ao armazenamento de backups em disco, com funcionalidades integradas de criptografia, compressão, desduplicação e replicação dos dados já desduplicados;

13.12 O equipamento deve estar listado no site oficial do fabricante como um appliance ou sistema de armazenamento de backup em disco, em produção ativa;

13.1.3 O hardware e o software devem ser do mesmo fabricante. Não serão aceitas soluções customizadas especificamente para esta licitação, nem combinações OEM, equipamentos usados, recondicionados, de demonstração ou gateways;

13.1.4 O equipamento deve ser novo, sem uso anterior, pertencente à linha mais recente do fabricante, em produção contínua e sem previsão de fim de suporte (EOSL) nos próximos cinco anos a partir da data de abertura da licitação;

13.1.5 Soluções baseadas exclusivamente em software (appliances virtuais) não serão aceitas;

13.1.6 Deve ser compatível com montagem em racks padrão de 19”, acompanhado de trilhos, cabos, conectores, manuais e todos os itens necessários para instalação, configuração e operação completa;

13.1.7 Para soluções com arquitetura Scale-Out:

13.1.7.1 Deve permitir conexão com outros sistemas do mesmo

fabricante para expansão de desempenho e capacidade;

13.1.7.2 Deve operar em modo ativo-ativo (alta disponibilidade com balanceamento de carga), redirecionando automaticamente os backups em caso de falha de um dos sistemas;

13.1.8 Para soluções com arquitetura Scale-Up:

13.1.8.1 Deve incluir duas controladoras, operando em modo ativo-ativo ou ativo-passivo, garantindo continuidade das operações de backup em caso de falha de uma das controladoras.

13.2 Requisitos de disponibilidade:

13.2.1 Deve possuir tolerância a falhas em componentes como discos, fontes de alimentação e ventiladores;

13.2.2 Deve contar com mecanismos que assegurem a integridade dos dados mesmo em casos de interrupção abrupta ou desligamento acidental;

13.2.3 Deve incluir proteção de cache de escrita para evitar perda de dados em caso de falha de energia;

13.2.4 Deve ser entregue com arranjos RAID-6, RAID-DP ou equivalente, com tolerância a falha de até dois discos e pelo menos um disco hot-spare por grupo RAID;

13.2.5 Os discos devem ser hot-pluggable e hot-swappable, permitindo substituição sem interrupção do sistema;

13.2.6 Deve oferecer monitoramento remoto pelo fabricante, com recursos como Call-Home para detecção proativa de falhas ou pré-falhas.

13.3 - Capacidade, desempenho e conectividade:

13.3.1 Deve oferecer no mínimo 100 (cem) TB de capacidade útil, sem considerar compressão, desduplicação ou espaço reservado ao sistema;

13.4 Para soluções Scale-Out:

13.4.1 Deve atingir taxa mínima de 5 TB/hora (cinco terabytes por hora) para operações de backups, sem considerar desduplicação;

13.4.2 Capacidade de ampliar a solução previamente fornecida, através da interconexão de módulos similares ou não, do mesmo fabricante. Para a expansão, volumes em nuvem, off-site, replicação ou similar para o atendimento a este requisito não serão aceitos, mantendo a característica de desduplicação global da solução.

13.4.3 A criptografia deve ser feita via hardware. Caso seja por software, a taxa de transferência deve ser 30% superior à mínima exigida, considerando apenas a desduplicação.

13.5 Para soluções Scale-Up:

13.5.1 Deve permitir expansão para pelo menos 500 TB (quinhentos terabytes) de capacidade útil, sem considerar compressão ou desduplicação, por meio de gavetas de discos, sem troca ou upgrade das controladoras originais, mantendo a desduplicação global;

13.5.2 Deve atingir taxa mínima de 15 TB/hora (quinze terabytes por hora) para operações de backup, considerando apenas a

desduplicação;

13.5.3 A criptografia deve ser realizada por hardware. Se for por software, a taxa de transferência deve ser 30% superior à exigida, considerando apenas a desduplicação;

13.5.4 Deve incluir no mínimo duas interfaces de rede de 25 Gbps com conectores SFP28 para backup via LAN, fornecidos com o equipamento;

13.5.5 Deve incluir pelo menos duas interfaces de 1 GbE com conectores UTP CAT6 para gerenciamento, também fornecidos;

13.5.6 Deve possuir ao menos uma porta IPMI/iLO/iDRAC ou equivalente;

13.5.7 Interfaces adicionais devem ser fornecidas conforme as melhores práticas do fabricante para garantir o desempenho requerido;

13.5.8 Fornecer a quantidade necessária de discos para atingimento da performance mínima solicitada, ou seja, se a solução requerer mais discos além dos necessários para atender a capacidade solicitada no item 8.3.1, discos adicionais deverão ser fornecidos. Não é obrigatório o licenciamento de capacidade desses discos adicionais

13.5.9 Comprovar a taxa de transferência através da ferramenta de dimensionamento do fabricante da solução, desconsiderando o uso de ferramentas/protocolos de otimizações na origem no seu dimensionamento, caso a solução ofertada não seja fornecida com todos os discos possíveis para sua capacidade total.

14. ITEM 08 - SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES

14.1 Características gerais

14.1.1 Permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, de maneira perpétua, irrestrita e sem necessidade de licenciamentos ou ônus adicionais;

14.1.2 -Possuir licenças na modalidade de uso perpétuo para todo para o completo atendimento das especificações técnicas do equipamento, ou seja, o equipamento deverá continuar a operar normalmente mesmo após o período de manutenção e assistência técnica contratado;

14.1.3 Para soluções com arquitetura Scale-Out:

14.1.3.1 A desduplicação de dados deve ser mantida de forma global em todo o ambiente de armazenamento, independentemente da quantidade de dispositivos interligados;

14.1.4 Para soluções com arquitetura Scale-Up:

14.1.4.1 A desduplicação global deve ser preservada em todo o conjunto de armazenamento.

14.2 Requisitos de compatibilidade:

14.2.1 O software deve ser homologado e plenamente compatível com o software de backup fornecido no ITEM 06 - SOFTWARE DE BACKUP DE DADOS;

14.2.2 Deve permitir leitura e gravação simultâneas via protocolos

CIFS, NFS e OST;

14.2.3 Deve oferecer suporte aos protocolos de monitoramento SNMP e Syslog;

14.2.4 Deve possibilitar que aplicações como Oracle (via RMAN) e Microsoft SQL realizem backups tipo Stream Based (Oracle Stream Backup) e “database dump” diretamente no equipamento, por meio de CIFS e NFS, sem uso de software de backup, evitando o consumo de licenças e sem necessidade de licenciamento por volume (TB) ou por servidor (CPU, Core, Tier). Caso essa funcionalidade exija licenciamento, todos os itens necessários devem ser incluídos na proposta.

14.3 - Funcionalidades operacionais:

14.3.1 Deve permitir a execução simultânea de processos de backup e restore;

14.3.2 Deve dispor de interface de gerenciamento baseada em navegador (WEB);

14.3.3 A desduplicação deve ser global, mesmo com volumes lógicos distintos, identificando dados redundantes entre diferentes fontes de backup e armazenando-os apenas uma vez;

14.3.4 A desduplicação deve ocorrer em conjunto com os processos de backup e restore, sem necessidade de janelas específicas;

14.3.5 Deve incluir mecanismos nativos para verificação da integridade dos dados desduplicados, com capacidade de correção automática em caso de inconsistência, sem uso de scripts externos;

14.3.6 Deve permitir replicação de dados via rede IP (LAN/WAN), de forma assíncrona, entre sistemas compatíveis do mesmo fabricante, utilizando desduplicação para otimizar o uso da banda;

14.3.7 Deve suportar topologias de replicação como 1:1, 1:N, N:1 e o cascateamento de equipamentos;

14.3.8 Deve integrar-se ao Microsoft Active Directory 2012 ou superior, para autenticação e controle de acesso;

14.3.9 Os dados armazenados devem ser criptografados com algoritmos de no mínimo AES128-SHA ou AES256-SHA;

14.3.10 Deve permitir autenticação em dois fatores (2FA), com integração a soluções OTP como Google Authenticator, Microsoft Authenticator ou equivalentes;

14.3.11 Caso a solução exija um sistema OTP específico com licenciamento ou hardware dedicado (ex: Common Access Card /Personal Information Verification cards, sistemas de OTP/tokenização licenciados, etc), todos os componentes necessários devem ser fornecidos para pelo menos 5 usuários;

14.3.12 Deve oferecer recurso de autorização dupla (Dual Auth) para alterações em configurações de proteção contra ransomware;

14.3.13 Deve incluir funcionalidades avançadas de segurança cibernética para proteção contra ransomware, assegurando a integridade dos dados de backup;

14.4 - Deve possuir mecanismo de imutabilidade dos dados:

14.4.1 A proteção deve estar sempre ativa, independente do software de backup, sem necessidade de janelas específicas ou scripts;

14.4.2 A proteção deve ser aplicada imediatamente após a desduplicação dos dados, sem depender de agendamento;

14.4.3 Deve adotar o conceito de air-gap, tornando os dados protegidos invisíveis à rede e inacessíveis por softwares de backup, independentemente do protocolo utilizado.

15. ITEM 09 – SWITCH CORE

15.1 Especificações Físicas

15.1.1 O equipamento deve contar com, no mínimo, 48 portas SFP28 compatíveis com velocidades de 1, 10 e 25 Gigabit Ethernet.

15.1.2 As interfaces devem ser auto-sensíveis, ajustando automaticamente a velocidade conforme o transceiver conectado, sem necessidade de configuração manual.

15.1.3 A altura máxima permitida é de 1 unidade de rack (1 RU).

15.1.4 Deve ser compatível com racks padrão de 19 polegadas, incluindo os kits de fixação apropriados.

15.1.5 As portas SFP28 devem aceitar transceivers dos tipos SFP+ 10GBase-SR, 10GBase-LR, 10GBase-ER, SFP 1000Base-SX, 1000Base-LX, 1000Base-ZX, 1000Base-T e cabos DAC.

15.1.6 Devem ser entregues ao menos 10 cabos DAC 25GbE SFP28 com comprimento mínimo de 3 metros, compatíveis com os appliances do item 1.

15.1.7 O switch deve possuir pelo menos 6 portas QSFP28 de 100GbE, com suporte a velocidades de 40GbE.

15.1.7.1 Deve ser compatível com transceivers 40GBase-SR4 e 40GBase-LR4.

15.1.7.2 Deve aceitar transceivers 100GBase-SR4 e 100GBase-LR4.

15.1.7.3 Deve suportar cabos DAC.

15.1.8 Deve acompanhar pelo menos 1 cabo DAC 100GbE com no mínimo 1 metro de comprimento, para conexão redundante entre switches.

15.1.9 A capacidade da matriz de comutação deve ser de no mínimo 4 Tbps.

15.1.10 O throughput mínimo exigido é de 1,5 Bpps.

15.1.11 O buffer deve ter capacidade mínima de 32 MB.

15.1.12 A latência máxima permitida é de 900 nanosegundos.

15.1.13 Deve suportar ao menos 160.000 endereços MAC.

15.1.14 A tabela ARP deve comportar até 64.000 entradas ou mais.

15.1.15 Deve aceitar jumbo frames com tamanho mínimo de 9000 bytes.

15.1.16 É obrigatória a presença de pelo menos uma porta RJ-45 para gerenciamento fora de banda.

15.1.17 O equipamento deve vir com CPU e memória (RAM e Flash) suficientes para suportar todas as funcionalidades descritas.

15.1.18 Fontes de alimentação internas devem ser redundantes e com ajuste automático para 110/220V.

15.1.19 O sistema de ventilação deve ser redundante, com fluxo de ar configurável (frontal-traseiro ou traseiro-frontal), sendo fornecido com ventiladores de fluxo frontal-traseiro.

15.1.20 Fontes e ventiladores devem ser hot-swappable e redundantes, permitindo substituição sem interrupção.

15.1.21 O equipamento deve ser projetado para ambientes de datacenter, com comutação de pacotes de alto desempenho.

15.2 - Funcionalidades Gerais

15.2.1 LEDs por porta devem indicar status e atividade do link.

15.2.2 A arquitetura da solução deve ser baseada em “spine-leaf”, com VxLAN como plano de dados e BGP EVPN como plano de controle.

15.2.3 Deve possuir porta de console para configuração via CLI, com conector RJ-45 ou RS-232, incluindo cabos e adaptadores necessários.

15.2.4 Gerenciamento via SSHv2 deve ser suportado.

15.2.5 O switch deve ter criptografia FIPS 140-2 validada pelo NIST.

15.2.6 Deve permitir espelhamento de uma ou mais portas para outra porta específica.

15.2.7 Também deve permitir espelhamento para porta remota via tunelamento, mesmo em domínios L2 distintos.

15.2.8 Deve implementar Netflow, sFlow ou tecnologia equivalente.

15.2.9 Gerenciamento via SNMPv3 deve ser possível.

15.2.10 Deve suportar o protocolo Syslog.

15.2.11 Deve implementar NTPv4 ou SNTP.

15.2.12 Autenticação via RADIUS deve ser suportada.

15.2.13 Autenticação via TACACS+ também deve ser suportada.

15.2.14 Controle de acesso por porta (IEEE 802.1x) deve estar presente.

15.2.15 Deve haver controle de broadcast, multicast e unicast por porta.

15.2.16 Deve implementar pelo menos uma fila de saída com prioridade estrita (SP Strict Priority) e divisão de banda ponderada (WRED, WRR ou similar).

15.2.17 Deve classificar, marcar e priorizar tráfego com base em IEEE 802.1p CoS.

15.2.18 Deve classificar, marcar e priorizar tráfego com base em DSCP (Differentiated Services CodePoint), conforme IETF.

15.2.19 Deve permitir classificação de tráfego por IP, portas TCP/UDP e endereços MAC.

15.3 - Virtualização de Switch

15.3.1 Deve permitir agregação de portas multi-chassi com redundância ativa/ativa sem Spanning Tree, usando MLAG, MC-LAG, M-LAG, VLT (Virtual Link Trunking), Multi-Chassis EtherChannel ou equivalentes.

15.3.2 Todos os componentes necessários para alta disponibilidade devem ser fornecidos, incluindo cabos, transceivers e licenças.

15.3.3 Em modo virtualizado, os switches devem operar com processamento local, sem tempo de convergência em caso de falha.

15.4 - Funcionalidades de Camada 2

15.4.1 Suporte a até 4.000 VLANs conforme IEEE 802.1Q.

15.4.2 Implementação de VLAN Trunking conforme IEEE 802.1Q, com controle de VLANs permitidas por tronco.

15.4.3 Suporte a Link Aggregation (LAG) conforme IEEE 802.3ad.

15.4.4 Deve suportar no mínimo 80 grupos LAG com até 16 portas cada.

15.4.5 Implementação dos padrões IEEE 802.1d, 802.1s e 802.1w.

15.4.6 Deve possuir mecanismo de proteção da root bridge do Spanning Tree.

15.4.7 Deve permitir bloqueio de BPDUs em portas em modo fast forwarding, com desativação automática ao recebê-los.

15.4.8 Implementação de LLDP e LLDP-MED para descoberta de vizinhos.

15.4.9 Suporte a DCB com PFC (IEEE 802.1Qbb), ETS (IEEE 802.1Qaz) e DCBx.

15.5 - Funcionalidades de Roteamento

15.5.1 Deve realizar roteamento de camada 3 entre VLANs.

15.5.2 Suporte ao protocolo OSPFv3.

15.5.3 Suporte ao protocolo BGPv4.

15.5.4 Capacidade para no mínimo 106.000 rotas IPv4.

15.5.5 Capacidade para no mínimo 52.000 rotas IPv6.

15.5.6 Operação simultânea com IPv4 e IPv6.

15.5.7 Implementação de VRF ou VRF-Light.

15.5.8 Suporte a roteamento baseado em políticas (PBR).

15.5.9 Implementação do protocolo VRRPv3.

CLÁUSULA TERCEIRA – DA IMPLANTAÇÃO DA SOLUÇÃO E SERVIÇOS CORRELATOS:

A **CONTRATADA** será responsável por toda a instalação e configuração dos equipamentos, firmwares e softwares, incluindo o fornecimento de quaisquer itens adicionais necessários à sua execução.

1. A instalação poderá ser realizada integral ou parcialmente pelo fabricante, devendo a **CONTRATADA** prever esses serviços em sua proposta.
2. A **CONTRATADA** deverá disponibilizar técnicos certificados pelo fabricante,

habilitados a instalar, operar e configurar os equipamentos fornecidos. Caso a instalação seja conduzida diretamente pelo fabricante, essa exigência estará dispensada.

3. A **CONTRATANTE** reserva-se o direito de solicitar a substituição parcial ou total da equipe da **CONTRATADA** durante a fase de implantação, caso seja constatada a ausência de qualificação técnica adequada.

4. Deverá ser apresentado cronograma de implantação e proposta de configuração da solução, ambos sujeitos à aprovação da equipe técnica da **CONTRATANTE**.

5. Ao final da instalação, deverão ser entregues, em meio digital, os manuais e procedimentos utilizados.

6. A instalação deverá incluir, no mínimo:

a) Fixação dos equipamentos em rack padrão 19”;

b) Conectorização elétrica e energização dos equipamentos;

c) Atualização de firmwares de todos os componentes (BIOS, Gerência Out of Band, controladoras HBA, interfaces de rede, discos, etc.);

d) Atualizações e releases disponíveis no site oficial;

e) Registro dos equipamentos e licenças no portal do fabricante.

f) Conectorização das interfaces de rede com os respectivos cabos/conectores;

g) Instalação, atualização e configuração dos componentes conforme boas práticas;

h) Integração dos equipamentos à rede da **CONTRATANTE**;

i) Outras atividades correlatas para garantir a operação da solução no ambiente da **CONTRATANTE**.

7. A aceitação dos itens do objeto contratado no ato da sua entrega ao Ministério Público do Estado do Amazonas será considerada como de caráter provisório. A aceitação definitiva dar-se-á após a instalação e configuração dos itens do objeto e a verificação do atendimento às especificações técnicas constantes deste instrumento.

8. Serão recusados os objetos imprestáveis ou defeituosos, que não atendam as especificações constantes neste termo de referência e/ou que não estejam adequados para uso.

9. Os itens deverão ser instalados, configurados e ativados pela **CONTRATADA** em local indicado pelo DTIC do MPAM.

10. O prazo para conclusão da instalação e configuração dos equipamentos e softwares será de até 30 (trinta) dias, contados a partir da data do recebimento provisório dos mesmos pela DTIC e emissão do termo provisório de recebimento.

11. Os equipamentos e serviços serão aceitos se, e somente se, houver comprovação de que todos os requisitos técnicos especificados neste contrato tenham sido atendidos e os itens se encontre em operação plena. Essa comprovação será feita mediante observação direta das características dos equipamentos, consulta à documentação técnica fornecida e verificação dos serviços de instalação e configurações.

12. Os serviços de instalação, configuração, migração e transferência de conhecimento técnico deverão ser realizados conforme especificado em cada

item.

13. O serviço de instalação e configuração tem a finalidade de garantir que os itens fornecidos estejam operacionais no ambiente de Produção, e de Contingência caso exista.

14. Todos os serviços de instalação, configuração, migração e transferência de conhecimento técnico deverão ser executados de forma presencial, por especialista(s) técnico(s) certificado(s) nos componentes pelo fabricante dos mesmos com a devida apresentação de certificado(s) técnico(s) emitido(s) pelo fabricante do(s) produto(s).

15. Os serviços de instalação, configuração, migração e transferência de conhecimento técnico, deverão ser agendados previamente entre as partes, através de e-mail ou telefone, e deverão ser realizados em dias úteis e em horário de expediente do MPAM.

16. A transferência de conhecimento técnico será feita através de treinamento referente aos componentes do objeto deste instrumento, abrangendo todos os recursos de hardware e software do ambiente, para até 10 (dez) técnicos designados pela **CONTRATANTE**, cobrindo no mínimo os seguintes tópicos:

a) Instalação.

b) Configuração básica e avançada.

c) Operação básica e avançada.

d) Gerenciamento da solução/expansão.

e) Administração.

f) Solução de problemas (troubleshouting).

g) Laboratório prático baseado na solução/expansão adquirida.

17. O treinamento deverá ser realizado nas seguintes condições:

a) Deverá ser ministrado em língua portuguesa do Brasil, de forma presencial;

b) Local: Av. Coronel Teixeira, nº 7.995, Nova Esperança II, CEP. 69037-473, Manaus-AM;

c) Carga horária mínima de 30 (trinta) horas, divididas em, no máximo, 4 (quatro) horas diárias;

d) O conteúdo programático deverá ser aprovado pela DTIC antes da realização de cada treinamento.

18. O material didático e os certificados deverão ser disponibilizados pela **CONTRATADA** com finalidade específica para ministrar o treinamento à DTIC.

19. Ao final do treinamento, os participantes deverão estar aptos a operar e administrar as tecnologias referenciadas neste instrumento.

20. A transferência de conhecimento técnico deverá ocorrer no período correspondente ao recebimento definitivo da expansão, ou em caso de impedimento justificado, em nova data aceita pela fiscalização do contrato.

21. Caberá ainda a **CONTRATADA** a execução de todas as atividades, bem como o fornecimento de todos os materiais necessários e suficientes para a instalação e configuração dos equipamentos fornecidos.

22. O planejamento, instalação, configuração e migração dos equipamentos deverão ser executados por técnicos habilitados e credenciados pelo fabricante.

23. A **CONTRATADA** deverá designar um profissional Técnico Responsável para acompanhar a execução dos serviços desde o planejamento até a implantação da expansão.

24. Antes da implantação dos equipamentos, a equipe técnica da **CONTRATADA** deverá apresentar o cronograma da implantação contendo: o plano de instalação, plano de contingência e prazos máximos para a realização da mudança.

25. A **CONTRATADA** deverá realizar a migração completa do ambiente computacional atualmente em operação para a nova infraestrutura fornecida, incluindo, mas não se limitando a: máquinas virtuais, clusters Kubernetes, bancos de dados, configurações nativas, políticas de segurança, integrações existentes e demais componentes necessários para garantir a continuidade dos serviços. A migração deverá ser executada de forma planejada, segura e sem impacto significativo na disponibilidade dos sistemas, observando as melhores práticas recomendadas pelo fabricante e garantindo a integridade dos dados e das aplicações.

26. A **CONTRATADA** deverá prover PDU´s ou réguas smart adequadas para a devida conecção elétrica necessária dos equipamentos específicados neste contrato.

27. Após a conclusão das atividades de instalação, configuração, migração e pré-operação, deve ser iniciada a fase de operação assistida do objeto contratado.

28. A operação assistida terá duração total de 90 (noventa) dias corridos, sendo 15 (dias) dias corridos de forma presencial, e o restante do período podendo ser de forma remota, de modo a assegurar o auxílio e pronta ação corretiva da **CONTRATADA** necessária em questões relacionadas com a configuração, monitoramento e estabilização da nova solução com o objetivo de garantir o bom funcionamento dos equipamentos e serviços.

29. Durante a fase de operação assistida, a **CONTRATADA** deverá atuar de maneira a mitigar os riscos decorrentes da transição tecnológica da plataforma atualmente existente para a nova solução.

30. As atividades de operação assistida devem ser realizadas somente nas dependências da sede do MPAM em Manaus-AM, em horário de expediente da Procuradoria-Geral, e devem se iniciar logo após a migração tecnológica, testes e ativação dos serviços. Caso seja necessária a consecução de atividades que possam afetar a disponibilidade dos serviços, as atividades de operação assistida podem ser prolongadas após o horário de expediente da Procuradoria-Geral, sem qualquer ônus para o MPAM.

31. O período de operação assistida deve englobar, dentre outras, as seguintes atividades:

a) Monitoramento de funcionamento e da capacidade dos serviços;

b) Identificação e abertura de chamados técnicos para solução de falhas na solução;

c) Resolução de problemas (troubleshooting);

d) Análise da efetividade de regras e configurações;

e) Simulação de abertura de chamados;

f) Instalação de patches;

g) Execução/revisão de procedimentos de backup e restore de

configurações;

h) Geração de relatórios técnicos, administrativos e gerenciais;

CLÁUSULA QUARTA – DA VIGÊNCIA:

O presente contrato tem vigência de **60 (sessenta) meses**, contados da data de publicação do extrato no Diário Oficial do MPAM, nos termos dos art. 105, caput, e 106, caput, da Lei n.º 14.133/2021.

1. A **CONTRATADA** terá o prazo de 5 (cinco) dias úteis para rubricar o contrato ou seus aditivos, contados a partir da data em que ela for notificada dessa providência pela Divisão de Contratos e Convênios (DCCON) da **CONTRATANTE**.

1.1 A assinatura contratual será efetuada por meio do Sistema Eletrônico de Informações (SEI) da **CONTRATANTE**.

1.2 Na hipótese de assinatura de termo aditivo de prorrogação, caso o prazo de expiração da avença for menor que o disposto no item 1 desta cláusula, a **CONTRATADA** deverá rubricar o instrumento até o último dia útil da vigência contratual.

1.3 Se a **CONTRATADA**, regularmente notificada pela DCCON, não assinar o contrato ou seu aditivo no prazo disposto neste item, ela ficará sujeita às penalidades descritas neste instrumento.

2. Consoante o art. 107, da Lei n.º 14.133/2021, o contrato poderá ser prorrogado sucessivas vezes, até o limite de 10 (dez) anos, desde que os preços permaneçam vantajosos para a **CONTRATANTE** e haja suficiência orçamentária.

3. A **CONTRATADA** não possui direito subjetivo à prorrogação contratual.

CLÁUSULA QUINTA – DA FUNDAMENTAÇÃO LEGAL DA CONTRATAÇÃO:

O presente contrato foi firmado mediante _____, fundamentando-se no art. _____, da Lei n.º 14.133/2021, e no Ato n.º 008/2024/PGJ, o qual define os procedimentos administrativos para contratação de bens e serviços no âmbito do Ministério Público do Estado do Amazonas, bem como nas demais legislações correlatas, conforme o _____.

CLÁUSULA SEXTA – DO REGIME DE EXECUÇÃO:

Conforme o Termo de Referência n.º 28.2025.DTIC.2002143.2025.007562 e o art. 6º, XXIX, da Lei n.º 14.133/2021, o regime de execução deste contrato é o da **empreitada por preço global**, modalidade em que a contratação do serviço se dá por preço certo e total.

CLÁUSULA SÉTIMA – DOS DOCUMENTOS INTEGRANTES:

Para melhor caracterizar o presente contrato, integram também este instrumento, como se nele estivessem transcritos, obedecidos os termos da legislação sobre contratos públicos, os seguintes documentos:

1. O Termo de Referência n.º 28.2025.DTIC.2002143.2025.007562;

2. O Edital de Licitação n.º _____;

3. A Proposta Comercial n.º _____ encaminhada pela **CONTRATADA**, no dia

_____, contendo os valores unitário e total..

CLÁUSULA OITAVA – DO VALOR:

O valor global e estimado deste contrato é de _____

1. No preço contratado já estão incluídos todos os custos e despesas, tais como: custos diretos e indiretos, tributos incidentes, despesas administrativas, materiais, serviços, encargos sociais, trabalhistas, seguros, frete, embalagens, lucro, e outros necessários ao cumprimento integral do objeto deste instrumento.

CLÁUSULA NONA – DA GESTÃO, FISCALIZAÇÃO E ACOMPANHAMENTO:

O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133/21, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

1. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

2. As comunicações entre a **CONTRATANTE** e a **CONTRATADA** devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

3. A **CONTRATANTE** poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

4. Após a assinatura do contrato ou instrumento equivalente, a **CONTRATANTE** poderá convocar o representante da **CONTRATADA** para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da **CONTRATADA**, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

5. Preposto

5.1 A **CONTRATADA** deverá manter preposto junto à PGJ-AM, aceito pela respectiva **FISCALIZAÇÃO**, durante o período de vigência do contrato, para representá-la administrativamente, sempre que for necessário, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado, o qual deverá ser indicado mediante declaração de que deverá constar o nome completo, nº do CPF e do documento de identidade, além dos dados relacionados à sua qualificação profissional.

5.2 A empresa orientará o seu **PREPOSTO** quanto à necessidade de acatar as orientações da Administração, inclusive quanto ao cumprimento das Normas Internas e de Segurança e Medicina do Trabalho.

5.3. A **CONTRATANTE** poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a **CONTRATADA** designará outro para o exercício da atividade.

6. Fiscalização

6.1 A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos, conforme indicação

em portaria específica publicada no Diario Oficial do MPAM.

6.2 Compete ao **Gestor da Ata/Contrato,** além de outras atribuições, nos termos da lei:

a) Acompanhar os prazos de execução e de vigência do contrato, conforme as rotinas e procedimentos estabelecidos pelo MPAM, e as cláusulas do contrato ou instrumento equivalente, comunicando à **CONTRATADA** e à unidade competente da Administração eventuais atrasos e encaminhando, em tempo hábil, expediente para a prorrogação do contrato;

b) Coordenar e acompanhar a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração;

c) Acompanhar a manutenção das condições de habilitação da **CONTRATADA**, para fins de empenho de despesa e pagamento, e anotar os problemas que obstam o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais;

d) Comunicar à Autoridade Competente as ocorrências relacionadas à execução do contrato que ultrapassarem a sua competência;

e) Emitir TERMO DE RECEBIMENTO DEFINITIVO, juntamente com a **FISCALIZAÇÃO**, comprovando a avaliação do cumprimento das obrigações assumidas pela **CONTRATADA**;

f) Receber e conferir as faturas/notas fiscais emitidas pela **CONTRATADA**, e encaminhar, devidamente certificadas/atestadas ao setor competente, observando, previamente, se a fatura apresentada pela **CONTRATADA** refere-se ao objeto que foi efetivamente pactuado;

g) Encaminhar o processo à unidade competente para proceder à liquidação da despesa, alertando para a data limite para pagamento das notas fiscais/fatura;

h) Requisitar a prorrogação de contrato, se possível, junto à Autoridade Competente, que deve ser providenciada antes de seu término, reunindo as justificativas necessárias;

i) Elaborar a comunicação à área competente para abertura de nova licitação, antes de findo a prestação de serviços e com antecedência razoável;

j) Cuidar das alterações de interesse da **CONTRATADA**, que deverão ser por ela formalizadas e devidamente fundamentadas, principalmente em se tratando de pedido de reequilíbrio econômico-financeiro ou repactuação, sendo que, no caso de pedido de prorrogação de prazo, deverá ser comprovado o fato impeditivo da execução, o qual, por sua vez, deverá corresponder àqueles previstos na Lei n. 14.133/21 e alterações, se possível;

k) Esclarecer dúvidas e transmitir instruções à **CONTRATADA**, comunicando alterações de prazos, cronogramas de execução e especificações do projeto, inclusive solicitando ao setor competente da

Administração, quando necessário a emissão de parecer técnico;

l) Deflagrar e conduzir os procedimentos de fiscalização à **CONTRATADA**, com base nos termos contratuais, sempre que houver descumprimento de suas cláusulas por culpa da **CONTRATADA**, acionando as instâncias superiores e/ou os órgãos públicos competentes quando o fato exigir;

m) Verificar se a entrega de materiais ou a prestação do serviço está sendo executada em conformidade com o pactuado, no tocante a prazo, especificações, preço e quantidade;

n) Rejeitar equipamentos e serviços que estejam em desacordo com as especificações do objeto contratado;

o) Zelar pelo efetivo cumprimento das obrigações contratuais assumidas e pela qualidade dos produtos fornecidos e dos serviços prestados;

p) Notificar a **CONTRATADA** em qualquer ocorrência desconforme com as cláusulas contratuais, sempre por escrito, com prova de recebimento da notificação (procedimento formal, com prazo);

q) Verificar a regularidade fiscal, trabalhista e previdenciária da contratada para fins de pagamento; e

r) Orientar a **CONTRATADA**, por intermédio do preposto, sobre a correta execução do contrato e, pelo mesmo meio, levar ao seu conhecimento as situações temerárias, recomendando medidas e estabelecendo prazo de resolução.

6.3 Compete ao **Fiscal Técnico**, além de outras atribuições, nos termos da lei:

a) Acompanhar e fiscalizar a execução do contrato nos aspectos técnicos da solução, conforme o respectivo regramento técnico aplicável;

b) Zelar pelo efetivo cumprimento das obrigações contratuais assumidas e pela qualidade dos produtos fornecidos e dos serviços prestados, de modo a assegurar os melhores resultados para a Administração;

c) Ler atentamente o Termo de Contrato e anotar em registro próprio todas as ocorrências relacionadas à sua execução, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados;

d) Esclarecer dúvidas do preposto/representante da **CONTRATADA** que estiverem sob a sua alçada, encaminhando às áreas competentes os problemas que surgirem quando lhe faltar competência;

e) Notificar à **CONTRATADA**, para a correção da execução do contrato, de determinando prazo para a correção, qualquer inexatidão ou irregularidade;

f) Informar ao Gestor do Contrato, em tempo hábil, irregularidades que possam demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso;

g) Comunicar ao Gestor do Contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva

ou à prorrogação contratual;

h) Avaliar a qualidade dos serviços realizados ou dos itens entregues e justificativas, de acordo com os critérios de aceitação definidos em contrato; e

i) Orientar a **CONTRATADA**, por intermédio do preposto, sobre a correta execução do contrato e, pelo mesmo meio, levar ao seu conhecimento as situações temerárias, recomendando medidas e estabelecendo prazo de resolução.

CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DA CONTRATANTE:

São obrigações da **CONTRATANTE**:

1. Acompanhar e fiscalizar, como lhe aprouver e no seu exclusivo interesse, na forma prevista na Lei n.º 14.133/21, exigindo o cumprimento de todas as obrigações assumidas, de acordo com o contrato e seus anexos.

2. Nomear **GESTOR** e **FISCALIZAÇÃO** técnica e administrativa, para acompanhar e fiscalizar, a execução dos contratos.

3. As ações de fiscalização não excluem nem reduzem a responsabilidade da **CONTRATADA**, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios ou emprego de material inadequado ou de qualidade inferior.

4. Fornecer à **CONTRATADA** as informações necessárias à fiel execução do objeto deste instrumento.

5. Permitir o acesso, acompanhar e fiscalizar a execução do contrato, verificando a conformidade da prestação dos serviços e regular a entrega dos itens, de forma a assegurar o perfeito cumprimento do contrato.

6. Anotar em registro próprio e notificar a **CONTRATADA**, por escrito, a ocorrência de eventuais imperfeições, defeitos de fabricação, e avarias nos itens, fixando prazo para a sua reposição.

7. Rejeitar, no todo ou em parte, serviço ou fornecimento executado em desacordo com o contrato.

8. Efetuar regularmente o pagamento da **CONTRATADA**, dentro dos critérios estabelecidos neste contrato, quanto aos serviços devidamente realizados, por meio de Ordem Bancária, após o atesto das notas fiscais/faturas pelo comitê responsável.

9. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

9.1 A **CONTRATANTE** terá o prazo de 1 (um) mês, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

10. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pela **CONTRATADA** no prazo máximo de 1 (um) mês.

11. A **CONTRATANTE** não responderá por quaisquer compromissos assumidos pela **CONTRATADA** com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da **CONTRATADA**, de seus empregados, prepostos ou subordinados.

CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES DA CONTRATADA:

A **CONTRATADA** deverá cumprir todas as obrigações constantes neste termo de referência, minuta de contrato e seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando:

1. Apresentar, no prazo de até 10 (dez) dias corridos, contados a partir da assinatura do contrato ou do recebimento da Nota de Empenho e da Autorização de Fornecimento de Materiais/Serviços:

1.1 Indicação formal do preposto da **CONTRATADA** apto a representá-la junto à **CONTRATANTE**, que deverá responder pela fiel execução do contrato, designado para acompanhar sua execução e atuar como interlocutor principal junto à **CONTRATANTE**, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

a) A indicação do preposto deverá ser acompanhada de seus dados pessoais, (no mínimo o nome completo e CPF do funcionário da empresa) e dados de contrato, como e-mail, telefone, whatsapp e outros.

1.2 Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste instrumento.

2. Efetuar a entrega do objeto contratado, dentro do prazo e de acordo com as especificações constantes deste contrato, observando as prescrições e as recomendações do fabricante, a legislação estadual ou municipal, se houver, bem como outras normas correlatas, ainda que não estejam explicitamente citadas neste documento e seus anexos.

3. Apresentar, no prazo de até 10 (dez) dias úteis, contados a partir da entrega do objeto, o correspondente TERMO DE GARANTIA E ASSISTÊNCIA TÉCNICA, para os equipamentos/softwares/licenças fornecidos incluindo seus números de série, com o prazo de garantia solicitado nesta avença.

4. Não transferir a outrem, no todo ou em parte, o objeto deste termo, não sendo aceita a transferência de responsabilidade para outras entidades, sejam fabricantes, técnicos, subempreiteiros ou quaisquer outros.

4.1 É vedada a subcontratação total ou parcial do objeto, bem como a cessão ou transferência deste instrumento contratual, no todo ou em parte, incluindo a transferência da execução a terceiros, a qualquer título, sem prejuízo da possibilidade de a **CONTRATADA** contratar atividades-meio acessórias (ex.: frete, seguro, logística), desde que:

I – tais contratações não caracterizem subcontratação do objeto nem delegação de atividades técnicas essenciais; e

II – permaneça a **CONTRATADA** integralmente responsável pela execução, qualidade, prazos, garantias e assistência técnica previstas no Contrato e no Termo de Referência.

5. Comunicar imediatamente à **CONTRATANTE**, formalmente, toda e qualquer anormalidade que dificulte ou impossibilite a execução do objeto deste contrato e prestar os esclarecimentos julgados necessários.

6. Aceitar todas as decisões, métodos de inspeção, verificação e controle, obrigando-se a fornecer todos os dados, elementos e explicações que a

CONTRATANTE julgar necessário.

6.1 A ação de fiscalização não exonera a **CONTRATADA** de suas responsabilidades contratuais.

7. Manter contato e realizar o planejamento dos serviços com a **CONTRATANTE** de forma a executar quaisquer tarefas ou ajustes inerentes ao objeto contratado.

8. Acatar as observações feitas pela **FISCALIZAÇÃO** da **CONTRATANTE** quanto à execução dos serviços.

9. Atender prontamente quaisquer orientações e exigências da equipe de **FISCALIZAÇÃO** do contrato ou autoridade superior (art. 137, II, da Lei n.º 14.133/21, e prestar todo esclarecimento ou informação por eles solicitados, inerentes à execução do objeto contratual;

9.1 A **CONTRATADA** deverá responder por escrito, no prazo máximo de até 2 (dois) dias consecutivos, a quaisquer comunicações e/ou esclarecimentos requisitados pela **CONTRATANTE**, pertinentes à execução do contrato e que venham a ser solicitados pelo MPAM.

10. A **CONTRATADA** deverá responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com Código de Defesa do Consumidor, Lei nº 8.078/90, e às demais normas pertinentes.

11. Apresentar justificativa por escrito, devidamente comprovada, nos casos de ocorrência de fato superveniente, excepcional ou imprevisível, estranho à vontade das partes, e de impedimento de execução por fato ou ato de terceiro reconhecido pela **CONTRATANTE** em documento contemporâneo a sua ocorrência, quando não puder cumprir os prazos estipulados para a execução, total ou parcial, do objeto deste contrato.

11.1 Nos casos de eventual atraso na entrega do objeto, comunicar à **CONTRATANTE**, antes de expirar tal prazo, quaisquer problemas que impossibilitem o cumprimento do prazo previsto, com a devida comprovação.

12. Substituir, reparar, corrigir, remover, refazer ou reconstituir, às suas expensas, no todo ou em parte, no prazo fixado pela **FISCALIZAÇÃO**, os itens que não atendam às especificações exigidas e foram rejeitados, os que se verifiquem imperfeições, vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.

13. Responsabilizar-se por falhas na execução dos serviços que venham a se tornar aparentes em data posterior à sua entrega, ainda que tenha havido aceitação deles.

14. Responsabilizar-se pela garantia e assistência técnica *on-site* dos itens, caso o fabricante e/ou assistência técnica autorizada por este não puder fazê-lo ou se recusar.

15. Manter, durante toda a execução do contrato, todas as condições de habilitação e qualificação exigidas na respectiva licitação, em compatibilidade com as obrigações assumidas.

16. Responder pela idoneidade moral e técnica dos seus empregados, sendo única, integral e exclusivamente responsável, em qualquer caso, por todos os danos e prejuízos, de qualquer natureza, causados, direta ou indiretamente, à **CONTRATANTE** ou a terceiros, provenientes da execução dos serviços objeto deste contrato, quaisquer que tenham sido as medidas preventivas adotadas, respondendo por si e seus procuradores.

17. Responsabilizar-se por obter todas as franquias, licenças, aprovações e demais exigências de órgãos competentes, inclusive responsabilizando-se por todos os ônus decorrentes.

18. A inobservância das especificações constantes deste instrumento implicará a não aceitação parcial ou total dos serviços, devendo a **CONTRATADA** refazer as partes recusadas sem direito a indenização

19. Cumprir as normas de proteção ao trabalho, inclusive aquelas relativas à segurança e à saúde no trabalho;

20. Não submeter os trabalhadores a condições degradantes de trabalho, jornadas exaustivas, servidão por dívida ou trabalhos forçados;

21. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos de idade, exceto na condição de aprendiz para os maiores de quatorze anos de idade, observada a legislação pertinente;

22. Não submeter o menor de dezoito anos de idade:

22.1 à realização de trabalho noturno;

22.2 à realização de trabalho em condições perigosas e insalubres; nem

22.3 à realização de atividades constantes na Lista de Piores Formas de Trabalho Infantil, aprovada pelo Decreto Federal n.º 6.481, de 12 de junho de 2008;

23. Receber e dar o tratamento adequado a denúncias de discriminação, violência e assédio no ambiente de trabalho;

24. Rubricar o contrato ou seus aditivos no prazo de 5 (cinco) dias úteis, contados a partir da notificação enviada pela DCCON.

CLÁUSULA DÉCIMA SEGUNDA – DA MATRIZ DE ALOCAÇÃO DE RISCOS:

1. Disposições gerais.

1.1. Para os fins desta Cláusula entende-se por risco todo evento futuro, incerto e alheio à vontade das partes, capaz de gerar impacto relevante no prazo, no custo ou na qualidade da execução contratual.

1.2. A alocação de riscos observa o art. 22 da Lei n.º 14.133/2021, de modo a atribuir-lhes, sempre que possível, à parte que detenha melhor capacidade de gerenciá-los ou mitigá-los, assegurando o equilíbrio econômico-financeiro do ajuste.

1.3. Sempre que caracterizado caso fortuito ou força maior, devidamente comprovado, aplicar-se-ão as regras desta Matriz, sem prejuízo das demais disposições legais pertinentes.

2. Riscos atribuídos exclusivamente à CONTRATANTE:

Evento	**Abrangência / Limite**	**Medida de mitigação ou compensação**
2.1 Alterações unilaterais do objeto ou das quantidades (art. 124, inciso I, da Lei n.º 14.133/2021).	Até os limites legais	Reequilíbrio mediante reajuste de preço, de prazo ou ambos, a pedido do CONTRATADO, nos termos da Cláusula Vigésima Primeira.

Evento	Abrangência / Limite	Medida de mitigação ou compensação
2.2 Caso fortuito ou força maior **externo** à cadeia de suprimentos do CONTRATADO (greves gerais, calamidade natural que impeça recebimento / instalação).	—	Suspensão de prazos e, se for o caso, recomposição de custos diretos comprovados.
2.3 Atraso de pagamento por fato imputável à Administração.	> 30 (dias) após vencimento	Incidência de atualização financeira (art. 92, inciso V, da Lei n.º 14.133/2021) e possibilidade de paralisação justificada (art. 137, § 3.º, inciso II, da Lei n.º 14.133/2021).
2.4 Falhas de infraestrutura, logística interna ou compatibilidade de sistemas sob gestão do MPAM.	—	Ajuste de cronograma sem ônus ao CONTRATADO; despesas adicionais cobertas pelo CONTRATANTE.
2.5 Contingenciamento ou indisponibilidade orçamentária superveniente.	—	Aplicação dos arts. 137, § 3.º, inciso II, e 138, § 2.º, da Lei n.º 14.133/2021, com suspensão ou rescisão e pagamento de indenizações cabíveis.

3. Riscos atribuídos exclusivamente à CONTRATADA:

Evento	Abrangência / Limite	Medida de mitigação ou compensação
3.1 Execução inadequada, atraso ou descumprimento de prazos sem causa justificada.	—	Aplicação de penalidades contratuais (arts. 155 e 156 da Lei n.º 14.133/2021) e obrigação de corrigir/repactuar às suas expensas.
3.2 Falha de fornecimento de materiais, insumos ou mão de obra.	—	Substituição ou suplementação imediata, sem ônus à CONTRATANTE.
3.3 Não conformidade dos equipamentos às especificações ou às amostras aprovadas.	—	Rejeição, substituição e aplicação de multas previstas.
3.4 Ausência ou insuficiência da garantia técnica **on-site** prevista.	—	Multa específica e extensão proporcional do período de garantia.

Evento	Abrangência / Limite	Medida de mitigação ou compensação
3.5 Danos causados por transporte ou armazenagem sob responsabilidade do fornecedor.	—	Reparação integral e sem custo para a CONTRATANTE.

4. Riscos COMPARTILHADOS:

4.1 São considerados riscos compartilhados aqueles que, pela própria natureza, escapam do controle exclusivo de uma das partes e cuja ocorrência possa comprometer a equação econômico-financeira do contrato.

Evento	Critério de compartilhamento	Forma de compensação
4.1.1 Alterações legais, normativas ou tributárias não previstas na data da proposta que onerem ou desonerem o objeto.	Cada parte arca com o impacto em até **5%** (cinco por cento) do valor atualizado do contrato; excedente será objeto de reequilíbrio conforme Cláusula Vigésima Primeira.	Ajuste de preços ou de escopo, conforme art. 124 da Lei n.º 14.133/2021.
4.1.2 Oscilação inflacionária ou cambial extraordinária, com variação acumulada superior a **10 %** do IPCA.	Impacto até **10 %** suportado pela parte contratada; excedente sujeito a reequilíbrio.	Reajuste ou repactuação após comprovação documental.
4.1.3 Situações de emergência pública ou calamidade que exijam alteração de cronograma.	Prorrogação automática dos prazos equivalente ao período de paralisação.	Eventuais custos diretos adicionais divididos meio a meio, mediante apresentação de planilha analítica.
4.1.4 Oscilações severas de mercado em componentes de manutenção (variação > 15 % do índice ICEI-TI).	Excedente dividido em partes iguais, mediante laudo de mercado independente.	Repactuação de preços de manutenção.

4.2 A superveniência de novos riscos não contemplados será tratada pelos mesmos critérios de alocação (capacidade de controle e gestão), mediante aditivo específico ou termo de apostilamento, observado o procedimento da Cláusula Vigésima Primeira.

5. Revisões e atualização da Matriz:

5.1 Ocorrendo fatos supervenientes relevantes, a presente Matriz poderá

ser revista por aditivo específico, preservados os princípios da legalidade, da eficiência e do equilíbrio econômico-financeiro.

CLÁUSULA DÉCIMA TERCEIRA – DA GARANTIA TÉCNICA:

Todos os equipamentos e softwares utilizados no fornecimento do objeto deverão estar cobertos por suporte, garantia e assistência técnica do fabricante, durante toda a vigência do contrato.

1. A garantia dos hardwares deverá ser na modalidade on-site no Datacenter da **CONTRATADA**.

2. A **CONTRATADA** é a única responsável pelos equipamentos e softwares disponibilizados na prestação dos serviços fornecidos à **CONTRATANTE**, mesmo que tenham sido adquiridos de terceiros.

3. A **CONTRATADA** responderá pela reparação dos danos causados por defeitos relativos ao serviço prestado, conforme descrição e exigências deste instrumento. Por isso, deve prezar pela qualidade e eficiência, garantindo que o serviço e as soluções definitivas fornecidas não causem problemas adicionais àqueles apresentados pela **CONTRATANTE**, quando do recebimento de alertas ou da abertura dos chamados de suporte técnico.

4. Serviços de Suporte Técnico e Manutenção

4.1 Os equipamentos deverão possuir garantia de 60 (sessenta) meses, com suporte 24x7 e prazo de envio de peças até o próximo dia útil após abertura do chamado.

4.2 A **CONTRATANTE** poderá acionar diretamente o suporte do fabricante, sem necessidade de autorização prévia da **CONTRATADA**. Não haverá limitação quanto à quantidade de chamados, seja para dúvidas, configurações ou problemas relacionados a hardware e software.

4.3 Chamados poderão ser abertos via telefone 0800, portal web ou e-mail.

4.4 O atendimento telefônico inicial deverá ser realizado em português.

4.5 A contratada deverá garantir acesso completo ao portal do fabricante, incluindo base de conhecimento, atualizações de software e documentação.

4.6 Durante a vigência do suporte, todas as atualizações de firmware e software deverão ser fornecidas sem ônus à **CONTRATANTE**.

4.7 A contratada deverá apresentar os códigos de serviço (SKU, part number) referentes à garantia do fabricante, com os equipamentos devidamente registrados em nome da contratante.

4.8 É de responsabilidade da contratada garantir a compatibilidade técnica entre todos os componentes da solução durante toda a vigência contratual.

CLÁUSULA DÉCIMA QUARTA – DA GARANTIA CONTRATUAL:

Nos termos dos arts. 96 a 102 da Lei n.º 14.133/2021, a**CONTRATADA** deverá apresentar garantia contratual, podendo optar pela caução em dinheiro ou em títulos da dívida pública, seguro-garantia, fiança bancária ou título de capitalização, em valor correspondente a **5% (cinco por cento)** do valor integral da contratação, correspondendo à quantia de R$ _____.

1. A partir da data em que for notificada pela **CONTRATANTE**, a **CONTRATADA** deverá encaminhar a garantia contratual no prazo de 10 (dez) dias úteis,

prorrogável por igual período, a critério daquela.

2. A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:

2.1 prejuízos advindos do não cumprimento do objeto do contrato;

2.2 prejuízos diretos causados à **CONTRATANTE** decorrentes de culpa ou dolo da **CONTRATADA**.

2.3 multas moratórias e compensatórias aplicadas pela **CONTRATANTE**; e

2.4 obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela **CONTRATADA**, quando couber.

3. No caso de acréscimo no valor contratual, a **CONTRATADA** obriga-se a depositar junto à **CONTRATANTE**, na mesma modalidade, o valor referente à diferença da garantia. Mesma providência deverá ser tomada no caso de prorrogação do prazo contratual para adequar o vencimento da garantia ao do termo aditivo.

4. As garantias prestadas serão liberadas ou restituídas após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da **CONTRATANTE** e, quando em dinheiro, atualizada monetariamente, segundo dispõe o art. 100 da Lei n.º 14.133/2021.

5. Na hipótese de prestação da garantia na modalidade seguro-garantia, este terá por objetivo garantir o fiel cumprimento das obrigações assumidas pela **CONTRATADA** perante a **CONTRATANTE**, inclusive as multas, os prejuízos e as indenizações decorrentes de inadimplemento, observadas as seguintes regras:

5.1 O seguro-garantia garantia deverá ter validade durante a execução do contrato e estender-se-á por mais **3 (três) meses após o término da vigência contratual,** devendo acompanhar as modificações referentes ao ínterim deste mediante a emissão do respectivo endosso pela seguradora;

5.2 O seguro-garantia continuará em vigor mesmo se o contratado não tiver pago o prêmio nas datas convencionadas.

6. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item 3 desta cláusula.

7. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação da multa moratória prevista neste contrato.

8. Caso o prazo a que se refere o item 8 da tabela da Cláusula Vigésima seja exaurido, tal circunstância autoriza a Administração a promover a retenção dos pagamentos devidos à **CONTRATADA** e/ou a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os arts. 137, I, e 139, IV, ambos da Lei n.º 14.133/2021.

8.1 O bloqueio efetuado com base neste item não gera direito a nenhum tipo de compensação financeira à **CONTRATADA**.

8.2 A **CONTRATADA**, a qualquer tempo, poderá substituir o bloqueio efetuado por quaisquer das modalidades de garantia, caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária.

11. A **CONTRATADA** se compromete a repor ou a completar a garantia na hipótese de utilização parcial ou total, para o pagamento da multa contratual ou encargos trabalhistas e previdenciários, e ainda, na alteração do valor contratado, para manter o percentual inicial, **no prazo de até 10 (dez) dias úteis**, contados da assinatura do termo aditivo ou a partir da data em que for

notificada pela **CONTRATANTE**, a partir do qual se observará o disposto nesta cláusula.

12. A garantia somente será liberada ante a comprovação de que a empresa pagou todos os encargos trabalhistas e previdenciárias decorrentes da contratação, bem como apresentação de toda a documentação solicitada no edital pela **CONTRATANTE**.

13. Será considerada extinta a garantia:

13.1 Com a devolução da apólice, acompanhada de declaração da **CONTRATANTE**, mediante termo circunstanciado, de que a **CONTRATADA** cumpriu todas as cláusulas do contrato;

13.2 No prazo de três meses após o término da vigência, caso a **CONTRATANTE** não comunique a ocorrência de sinistros.

14. A garantia não será extinta em caso de ocorrência de sinistro ou irregularidade, devidamente comunicado à seguradora pela **FISCALIZAÇÃO.**

CLÁUSULA DÉCIMA QUINTA – DO ACORDO DE NÍVEL DE SERVIÇO (SLA):

Os chamados de suporte técnico serão classificados conforme o nível de severidade, com base no impacto causado no ambiente computacional da **CONTRATANTE**, conforme as tabelas a seguir:

1. Impacto:

Nível	**Descrição do Impacto**
1	Serviços totalmente indisponíveis
2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos
3	Acesso aos aplicativos

2. Níveis de Severidade:

Modalidade	**Prazo**	**Níveis de Severidade**		
		1	**2**	**3**
Remoto	Início do Atendimento	1 hora	4 horas	8 horas
	Solução do Contorno	8 horas	12 horas	24 horas

3. Quando for necessário atendimento presencial, a **CONTRATADA** deverá disponibilizar técnicos para resolver os problemas no local. Preferencialmente, essas atividades devem ser previamente acordadas entre as partes, exceto em casos de severidade máxima ou evidente indisponibilidade da infraestrutura da **CONTRATANTE**.

4. O início do atendimento será considerado a partir da abertura do chamado técnico.

5. O atendimento será considerado encerrado quando a solução estiver disponível e funcionando perfeitamente no local de instalação.

6. Durante toda a vigência do contrato, a **CONTRATANTE** poderá abrir chamados ilimitados para suporte técnico.

7. A **CONTRATADA** será integralmente responsável por quaisquer danos ou prejuízos causados ao patrimônio da **CONTRATANTE** ou de terceiros, decorrentes de ações ou omissões de seus colaboradores durante a execução dos serviços solicitados.

8. Qualquer atividade relacionada a configurações, ajustes ou parametrizações após a implantação deverá ser precedida da abertura de um chamado técnico.

9. Caso a atividade seja realizada de forma proativa, a **CONTRATADA** deverá comunicar à **CONTRATANTE**, via e-mail, justificando a execução antecipada.

10. Se alguma atividade exigir a interrupção da solução, a **CONTRATANTE** deverá ser imediatamente notificada para autorizar ou reagendar a execução.

11. Atualizações que impliquem indisponibilidade do ambiente devem ser previamente agendadas com a equipe técnica da **CONTRATANTE**.

12. A **CONTRATADA** deverá manter uma Central de Atendimento em português (Brasil), operando 24 horas por dia, 7 dias por semana, durante todo o ano (24x7x365), para abertura de chamados e demais comunicações.

13. A **CONTRATANTE** poderá solicitar serviços específicos por meio dos seguintes canais de comunicação:

a) E-mail;

b) Telefone 0800;

c) Sistema de Chamados Web.

14. O serviço será considerado concluído somente após a confirmação da área técnica da **CONTRATANTE** quanto à sua execução satisfatória.

15. O encerramento de solicitações técnicas dependerá da anuência de ambas as partes: **CONTRATADA** e **CONTRATANTE**.

16. A **CONTRATADA** manterá um cadastro com os nomes das pessoas indicadas pela **CONTRATANTE** autorizadas a abrir e encerrar chamados.

17. O prazo para encerramento do atendimento não poderá ultrapassar os limites estabelecidos para cada nível de criticidade.

18. Considera-se suporte técnico as atividades que requerem acompanhamento por parte de um técnico da **CONTRATANTE**.

19. Quando for necessário atendimento local, o cronograma de execução deverá ser acordado entre as partes.

20. A **CONTRATADA** deverá iniciar o atendimento conforme os prazos definidos para cada nível de criticidade.

21. A manutenção corretiva inclui os serviços necessários para restaurar o funcionamento adequado dos equipamentos, com fornecimento de peças conforme especificações do fabricante, em caso de falhas ou defeitos de hardware.

22. A **CONTRATADA** deverá realizar os serviços de manutenção com ferramentas próprias e técnicos especializados, devidamente identificados.

23. O suporte técnico compreende ações para restabelecer o funcionamento

correto das soluções contratadas, incluindo configuração, habilitação, implementação, manutenção e colocação em produção de funcionalidades.

24. Caso seja necessária a atualização de firmware, a **CONTRATADA** deverá fornecer o pacote de software e realizar a atualização.

25. Considerando que a resolução de problemas de software pode envolver o desenvolvimento de patches, admite-se a adoção de soluções de contorno (workaround) até a implementação da solução definitiva.

26. O período para solução de ocorrências de software será contado entre a formalização e o encerramento efetivo da ocorrência, seja com solução definitiva ou provisória.

27. Para ocorrências de hardware não resolvidas dentro do prazo, a **CONTRATADA** deverá substituir o equipamento ou módulo defeituoso em até 72 (setenta e duas) horas úteis. Após a substituição, deverá ser entregue um documento com as descrições e números de série dos equipamentos substituídos e novos.

28. A substituição definitiva de hardware deverá ser feita com equipamento novo, original, recomendado pelo fabricante, com configuração igual ou superior à do substituído.

29. Durante a substituição, a **CONTRATADA** deverá entregar documento contendo a descrição e número de série do equipamento defeituoso e do novo equipamento.

30. O prazo para solução de ocorrências de hardware será contado entre a formalização e o encerramento efetivo da ocorrência. Quando houver substituição, o encerramento será considerado apenas após o novo equipamento entrar em operação.

31. Para cálculo do tempo de atendimento, serão desconsiderados os períodos em que a **CONTRATANTE** estiver responsável por ações necessárias à análise e solução da ocorrência.

32. Não haverá limitação quanto ao número de técnicos da **CONTRATANTE** autorizados a abrir chamados, desde que previamente registrados como pontos de contato.

33. Durante o período de garantia, a **CONTRATADA** deverá fornecer todas as atualizações de software (versões, releases, patches), firmware ou microcódigos dos hardwares cobertos pela manutenção, sem custo adicional.

CLÁUSULA DÉCIMA SEXTA – DO RECEBIMENTO E DOS PRAZOS DE ENTREGA:

1. Da Entrega

1.1 Do prazo

1.1.1 A **CONTRATADA** deverá em, **no máximo, 60 (sessenta) dias corridos**, contados a partir da assinatura do contrato, finalizar a entrega de todos os itens do objeto especificado, com funcionamento e funcionalidades da solução de Datacenter completamente operacionais, totalmente ativadas e disponíveis na estrutura da **CONTRATADA**, conforme descritas neste contrato.

1.1.2 O prazo para entrega do objeto especificado poderá ser prorrogado mediante apresentação pela **CONTRATADA**, antes do fim do prazo especificado, de solicitação formal e fundamentada,

condicionado à aceitação pela **CONTRATANTE**, que decidirá pela prorrogação do prazo ou aplicação das penalidades previstas em contrato.

1.2 Das condições de fornecimento

1.2.1 A **CONTRATADA** será responsável pelo transporte dos produtos, desde o local de sua fabricação/embalagem, conforme o caso, até o local de entrega, na sede da PROCURADORIA GERAL DE JUSTIÇA, a qual ocorrerá em dias úteis, no horário das 14h às 17h, no seguinte endereço:

Av. Coronel Teixeira, nº 7.995, Nova Esperança II

CEP. 69037-473, Manaus-AM

1.2.2 A entrega dos produtos deverá ser previamente agendada com o SETOR DE PATRIMÔNIO E MATERIAL – SPAT pelo telefone (92) 3655-0767.

1.2.3 Os produtos deverão ser entregues em perfeitas condições, conforme a quantidade e especificações pactuadas, observando o Edital, a Proposta da **CONTRATADA** e este contrato devendo, também, ser acondicionado adequadamente, em seu invólucro original, que deverão ser entregues devidamente acompanhados da respectiva nota fiscal, na qual constarão os valores discriminados dos itens que integram o conjunto, assim como as indicações referentes a: marca, modelo, procedência e prazo de garantia ou validade.

1.2.4 Os produtos devem estar em plena fabricação, não sendo aceitos aqueles com avisos de end-of-sale, end-of-support ou end-of-life emitidos pelo fabricante.

2. Do recebimento provisório e definitivo

2.1 O recebimento dos produtos será conduzido por uma COMISSÃO especialmente designada para essa finalidade. Essa comissão será composta por, no mínimo, três servidores ou empregados públicos, em conformidade com o disposto no Art. 117, §1º e Art. 140, inciso II da Lei n.º 14.133/21, conforme estabelecido neste subitem.

2.2 O RECEBIMENTO PROVISÓRIO será realizado pelo SETOR DE PATRIMÔNIO E MATERIAL - SPAT no ato da entrega da totalidade dos produtos empenhados, devidamente acompanhados da nota fiscal. Constitui-se de uma inspeção quantitativa, para posterior verificação de sua conformidade com as especificações do Termo de Referência e do Contrato.

a) O RECEBIMENTO PROVISÓRIO não constitui aceitação do objeto.

2.3 O RECEBIMENTO DEFINITIVO será realizado por FISCAL TÉCNICO ou COMISSÃO especialmente designada, no prazo máximo de 30 (trinta) dias, a contar do recebimento provisório, para verificação da conformidade dos equipamentos com as condições, especificações e obrigações contratuais.

a) É condição para RECEBIMENTO DEFINITIVO o fornecimento do TERMO DE GARANTIA E ASSISTÊNCIA TÉCNICA, informando que os referidos produtos estão cobertos por garantia de fábrica, de acordo com as exigências constantes neste instrumento;

b) O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais;

c) Uma vez constatado o cumprimento das obrigações de fornecimento, o TERMO DE RECEBIMENTO DEFINITIVO será emitido, que consistirá na declaração formal de que os itens fornecidos atendem aos requisitos estabelecidos no contrato, comprovando o atendimento das exigências contratuais.

2.4 Para avaliação da adequação às exigências contratuais e qualidade, o FISCAL TÉCNICO ou COMISSÃO submeterá os equipamentos recebidos a testes de aceitação, para aferição da boa execução do objeto contratado, após o qual, emitirá um relatório completo dos testes efetuados, devidamente assinado. Os testes serão constituídos das seguintes fases:

a) Abertura das embalagens;

b) Comprovação de que o equipamento/solução atende às especificações mínimas exigidas ou superiores oferecidas;

c) Testes funcionais de configuração e desempenho dos produtos.

2.5 Os itens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste instrumento, seus Anexos e na proposta, sem prejuízo da aplicação das penalidades, cabendo à **CONTRATADA** o dever de substituir os itens que não estejam de acordo com as especificações, observando-se o disposto no Art. 140, §1º da Lei n.º 14.133/21.

2.6 O RECEBIMENTO PROVISÓRIO ou DEFINITIVO do objeto não exclui a responsabilidade civil a ele relativa, nem a ético-profissional, pela perfeita execução do objeto deste termo.

2.7 As não conformidades e desvios de qualidade observados serão descritos em relatório, e não serão recebidos definitivamente, devendo a pendência ser completamente sanada pela **CONTRATADA**, em no máximo 15 (quinze) dias consecutivos, contados da notificação da **CONTRATANTE**.

2.8 Se, a qualquer tempo, vier a ser constatado que o material fornecido o foi em desacordo com as especificações e, em decorrência desse fato, observar-se qualquer tipo de dano ao equipamento onde está sendo utilizado, o reparo do equipamento ou, se for o caso, a sua substituição, será de inteira responsabilidade da **CONTRATADA**, nos termos da lei pertinente.

CLÁUSULA DÉCIMA SÉTIMA – DAS CONDIÇÕES DE PAGAMENTO:

O pagamento devido à **CONTRATADA** será creditado em conta-corrente, por meio de ordem bancária, efetuado mediante apresentação de nota fiscal/fatura, que será atestada pela **FISCALIZAÇÃO** deste contrato.

1. O pagamento será realizado à **CONTRATADA** de forma integral e condicionado ao marco da emissão do Termo de Recebimento Definitivo do objeto, assinado por ambas as partes.

2. Nos termos do art. 139, caput, e do art. 140, ambos do Ato n.º 008/2024/PGJ, os prazos para a **CONTRATANTE** liquidar e pagar são de:

2.1 até 10 (dez) dias úteis para a liquidação da despesa, a contar do

recebimento da nota fiscal ou do instrumento de cobrança equivalente pela **CONTRATANTE**;

2.2 até 10 (dez) dias úteis para o pagamento, contados da liquidação da desepesa.

3. O requerimento de pagamento deverá ser encaminhado aos endereços eletrônicos protocolo@mpam.mp.br e dtic@mpam.mp.br, acompanhado da respectiva nota fiscal/fatura dos produtos, emitidas em conformidade com o Protocolo ICMS 42/2009 (NF-e), deverá estar devidamente discriminada, em nome da **PROCURADORIA-GERAL DE JUSTIÇA**, CNPJ n.º 04.153.748/0001-85, e acompanhada da seguinte documentação:

3.1 Certidão Negativa de Débitos para com a Fazenda Federal, Estadual e Municipal do domicílio ou sede da empresa, ou outra equivalente, na forma da lei.

3.2 Certidão Negativa de Débitos à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS.

3.3 Certidão Negativa de Débitos trabalhistas.

3.4 Requerimento solicitando o pagamento, em duas vias, constando o número da Nota de Empenho e deste contrato.

3.5 Recibo em duas vias.

4. Nenhum pagamento será efetuado à **CONTRATADA** enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência.

4.1 Na hipótese de a **CONTRATADA** não ter executado completamente o objeto, ou tê-lo realizado de maneira insatisfatória, conforme relatório da **FISCALIZAÇÃO**, o pagamento será feito de maneira proprocional e apenas pelos serviços efetivamente prestados.

4.2 Em qualquer dos casos deste item, a **CONTRATANTE** poderá reter os pagamentos devidos à **CONTRATADA** até que as pendências sejam resolvidas.

5. Se, quando da efetivação do pagamento, os documentos comprobatórios de situação regular, apresentados em atendimento às exigências de habilitação, estiverem com a validade expirada, o pagamento ficará retido até a apresentação de novos documentos dentro do prazo de validade.

6. Qualquer atraso ocorrido na apresentação da nota fiscal/fatura, ou dos documentos exigidos como condição de pagamento por parte da **CONTRATADA**, importará em prorrogação automática do prazo de vencimento da obrigação da **CONTRATANTE,** não sendo devido à **CONTRATADA** o pagamento de multa e juros moratórios.

7. Nenhum pagamento isentará a **CONTRATADA** das responsabilidades atinentes ao produto, tampouco implicará a aprovação definitiva da entrega, total ou parcialmente.

8.Nos casos de eventuais atrasos de pagamento, desde que a **CONTRATADA** não tenha concorrido de alguma forma para tanto, fica convencionado que os encargos moratórios devidos pela **CONTRATANTE**, entre a data de vencimento e a do dia do efetivo pagamento da nota fiscal/fatura, a serem incluídos na fatura do mês seguinte ao da ocorrência, serão calculados por meio da aplicação da seguinte fórmula:

EM = I x N x VP, onde:

EM = encargos moratórios

N = número de dias entre a data prevista para o pagamento e a do efetivo pagamento

VP = valor da parcela em atraso

I = índice de compensação financeira = 0,00016438, assim apurado:

I = i ÷ 365 = (6÷100) ÷ 365 = 0,00016438

Onde i = taxa percentual anual no valor de 6%.

CLÁUSULA DÉCIMA OITAVA – DA DOTAÇÃO ORÇAMENTÁRIA:

As despesas oriundas deste contrato correrão à conta da seguinte dotação orçamentária:

Unidade Gestora: 003101 – Procuradoria Geral de Justiça; **Unidade Orçamentária:** 03101 – Procuradoria Geral de Justiça; **Programa de Trabalho**: 03.122.0001.2001.0001 – Administração da Unidade; **Fonte**: – ; **Natureza da Despesa:** – , tendo sido emitida pela **CONTRATANTE**, em _____, a Nota de Empenho n.º _____, no valor global de **R$ _____**.

CLÁUSULA DÉCIMA NONA – DAS SANÇÕES ADMINISTRATIVAS:

Nos termos dos art. 155 da Lei n.º 14.133/2021, a **CONTRATADA** será responsabilizada administrativamente na forma desta cláusula.

1. São condutas passíveis de sanção administrativa:

1.1 Dar causa à inexecução parcial do contrato;

1.2 Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

1.3 Dar causa à inexecução total do contrato;

1.4 Deixar de entregar a documentação exigida para o certame;

1.5 Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

1.6 Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

1.7 Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

1.8 Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

1.9 Fraudar a licitação ou praticar ato fraudulento na execução do contrato;

1.10 Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

1.11 Praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

1.12 Praticar ato lesivo previsto no art. 5º da Lei n.º 12.846/2013.

2. Pela inexecução total ou parcial do compromisso assumido, a **CONTRATANTE** poderá aplicar à **CONTRATADA** as seguintes sanções:

2.1 Advertência, que será aplicada exclusivamente à conduta descrita no subitem 1.1 desta cláusula, quando não se justificar imposição de penalidade mais grave;

2.2 Multas, que serão aplicadas por qualquer das infrações descritas no item 1 desta cláusula, nos percentuais estabelecidos na Cláusula Vigésima deste contrato;

2.3 Impedimento de licitar e contratar com a Administração Pública Direta e Indireta do **ESTADO DO AMAZONAS**, em decorrência das infrações previstas nos subitens 1.2, 1.3, 1.4, 1.5, 1.6 e 1.7 desta cláusula, pelo prazo máximo de 3 (três) anos, havendo possibilidade de reabilitação da **CONTRATADA** após o decurso de 1 (um) ano;

2.4 Declaração de inidoneidade para licitar ou contratar com toda a Administração Pública brasileira, em virtude das condutas descritas nos subitens 1.8, 1.9, 1.10, 1.11 e 1.12 desta cláusula, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a **CONTRATADA** ressarcir a **CONTRATANTE** pelos prejuízos resultantes e após decorrido o prazo de 3 (três) anos;

3. As sanções serão aplicadas pela **CONTRATANTE** em procedimento apuratório que assegure à **CONTRATADA** as garantias do contraditório e da ampla defesa, com os recursos a eles inerentes.

3.1 Compete à Comissão Permanente de Licitação (CPL) da **CONTRATANTE** instruir os procedimentos apuratórios de que trata este item.

4. Cabe ao (à) **SUBPROCURADOR(A)-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS** a aplicação das sançoes descritas nos subitens 2.1, 2.2 e 2.3 desta cláusula.

4.1 Da decisão do (a) **SUBPROCURADOR(A)-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS** cabe recurso dirigido a este, no prazo de 15 (quinze) dias úteis, contado da data da intimação.

4.2 Se o (a) **SUBPROCURADOR(A)-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS** não reconsiderar a decisão em 5 (cinco) dias úteis, encaminhar-la-á ao (à) **PROCURADOR(A)-GERAL DE JUSTIÇA.**

5. Compete ao (à) **PROCURADOR(A)-GERAL DE JUSTIÇA** a aplicação da sanção disposta no subitem 2.4 desta cláusula.

5.1 Da decisão do (a) **PROCURADOR(A)-GERAL DE JUSTIÇA** caberá apenas pedido de reconsideração, que deverá ser apresentado no prazo de 15 (quinze) dias úteis.

6. As penalidades serão obrigatoriamente registradas no Sistema de Cadastro Único de Fornecedores - SICAF.

7. A sanção do subitem 2.2 desta cláusula pode ser aplicada isolada ou conjuntamente com as dos subitens 2.1, 2.3 e 2.4.

8. A aplicação das penalidades previstas nesta cláusula não exclui nem atenua a obrigação de a **CONTRATADA** reparar integralmente os danos causados à **CONTRATANTE**.

CLÁUSULA VIGÉSIMA – DAS MULTAS:

As multas a que se refere o subitem 2.2 da Cláusula Décima Nona serão impostas nas seguintes hipóteses:

Item	Penalidade	Sanção	Limite
1	Atraso injustificado na entrega do objeto contratado, ou pelo não cumprimento dos prazos estabelecidos no Edital	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor total da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **C O N T R A T A D A** às sanções correlatas.
2	Atraso injustificado na regularização pertinente quando da recusa do objeto fornecido, na fase de **RECEBIMENTO**.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor total da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **C O N T R A T A D A** às sanções correlatas.
3	Recusa em substituir o produto defeituoso, que vier a ser rejeitado, ou que na execução dos serviços de garantia e assistência técnica, apontem a necessidade de troca;	Multa de mora diária de **1% (um por cento)** sobre o valor da Nota de Empenho	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **C O N T R A T A D A** às sanções correlatas.

Item	Penalidade	Sanção	Limite
4	Deixar de utilizar peças, componentes ou insumos originais ou certificados pelo fabricante, novos e de primeiro uso.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho. Por ocorrência	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **C O N T R A T A D A** às sanções correlatas.
5	Atraso injustificado para efetiva recolocação do produto em seu pleno estado de funcionamento, conforme condições de GARANTIA E ASSISTÊNCIA TÉCNICA deste Termo.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **C O N T R A T A D A** às sanções correlatas.
6	Deixar de fornecer equipamento backup nos casos em que não for possível recuperar os produtos dentro dos prazos de atendimento previstos.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **C O N T R A T A D A** às sanções correlatas.

Item	Penalidade	Sanção	Limite
7	Atraso injustificado para a substituição de determinado item (equipamento, serviço, software, licença), no atendimento de chamado de garantia e assistência técnica.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da CONTRATADA às sanções correlatas.
8	Atraso injustificado para a análise e correção dos itens (equipamento, serviço, software, licença), no atendimento de chamado de garantia e assistência técnica.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 10º (décimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 11.º (décimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **C O N T R A T A D A** às sanções correlatas.
9	Atraso injustificado para o fornecimento do TERMO DE GARANTIA E ASSISTÊNCIA TÉCNICA.	Multa de mora diária de **0,3% (três décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 10º (décimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 11.º (décimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **C O N T R A T A D A** às sanções correlatas.
10	Atraso injustificado na resposta aos pedidos de esclarecimentos de ordem técnica.	Multa de mora diária de **0,2% (dois décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 10º (décimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 11.º (décimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **C O N T R A T A D A** às sanções correlatas.

Item	Penalidade	Sanção	Limite
11	Deixar de cumprir qualquer outra obrigação não prevista neste contrato	Multa de mora diária de **1% (um por cento)** sobre o valor da Nota de Empenho	Limitada a sua aplicação até **15% (quinze por cento)**.
12	Quando, sem justificativa aceita pela **CONTRATANTE**, o vencedor não providenciar o devido cadastramento junto ao Sistema de Administração Financeira e Contabilidade – Cadastramento de Credores da SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ-AM, na forma prevista no Edital.	Multa de **2,5% (dois inteiros e cinco décimos por cento)** sobre o valor total da proposta.	Não se aplica.
13	Inexecução parcial do objeto contratado.	Multa de até **0,5% (cinco décimos por cento)** até **30% (trinta por cento)** sobre o valor da Nota de Empenho, sem prejuízo das demais sanções previstas.	Não se aplica.
14	Inexecução total do objeto.	Multa de até **5% (cinco por cento)** até **30% (trinta por cento**) sobre o valor total do contrato, sem prejuízo das demais sanções previstas.	Não se aplica.

1. Serão descontados dos pagamentos porventura devidos à **CONTRATADA** as importâncias alusivas a multas, ou efetuar sua cobrança mediante inscrição na dívida ativa do Estado, ou por qualquer outra forma prevista em lei.

2. Caso a **CONTRATANTE** determine, a multa deverá ser recolhida no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

3. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a **CONTRATANTE** poderá cobrar o valor remanescente judicialmente.

CLÁUSULA VIGÉSIMA PRIMEIRA – DO REAJUSTAMENTO DE PREÇOS:

Nos termos do art. 92, §§ 3º e 4°, I, da Lei n.º 14.133/2021, os preços inicialmente contratados poderão ser reajustados, por requerimento da **CONTRATADA**, desde que observado o interregno mínimo de 12 (doze) meses, de acordo com a variação do Índice de Custo da Tecnologia da Informação (ICTI), computado pelo Instituto de Pesquisa Econômica Aplicada (Ipea), ou outro que venha substituí-lo, na forma e periodicidade regulamentadas.

1. Caberá à **CONTRATADA** efetuar os cálculos relativos ao reajustamento OU repactuação e demais documentos comprobatórios, submetendo-os à apreciação da **FISCALIZAÇÃO**.

2. O interregno mínimo de 12 (doze) meses para o primeiro reajustamento será contado a partir da data do orçamento estimado pela **CONTRATANTE**, que corresponderá à da assinatura do Quadro-Resumo de Compras, ocorrida em _____.

3. Nos reajustes subsequentes ao primeiro, o interregno de 12 (doze) meses será contado a partir da data de início dos efeitos financeiros do último reajustamento ocorrido.

4. O prazo para a **FISCALIZAÇÃO** responder ao pedido de reajustamento será de 1 (um) mês, contado do recebimento do pedido.

5. Conforme o art. 136, I, da Lei n.º 14.133/2021, o reajustamento poderá ser efetuado por simples apostila, salvo se coincidir com a porrogação contratual, hipótese em que deverá ser formalizado por termo aditivo.

6. Caso a **CONTRATADA** não requeira tempestivamente o reajustamento e prorrogue o contrato sem pleiteá-lo, ocorrerá a preclusão do direito.

7. A **CONTRATANTE** poderá restabelecer o equilíbrio econômico-financeiro do ajuste em seu favor, visando à adequação dos preços contratuais, quando se verificar que houve redução dos preços dos serviços no mercado, observando-se o disposto no art. 124 da Lei n.º 14.133/2021.

8. A **FISCALIZAÇÃO** poderá solicitar à **CONTRATADA**, durante a vigência deste contrato, a revisão dos preços e dos percentuais de desconto contratados quando o contrato mostrar-se desvantajoso para a Administração.

9. Nos termos do art. 124, II, "d", da Lei n.º 14.133/2021, ainda que não decorrido o interregno mínimo de 1 (um) ano a que se refere o item 2 desta cláusula, a **CONTRATADA** poderá pleitear à **FISCALIZAÇÃO** o reequilíbrio econômico-financeiro inicial do contrato em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução do contrato tal como pactuado, respeitada, em qualquer caso, a repartição objetiva de risco estabelecida no contrato.

CLÁUSULA VIGÉSIMA SEGUNDA – DA ALTERAÇÃO DO CONTRATO:

Nos termos dos arts. 124 e seguintes da Lei n.º 14.133/2021, o presente contrato pode ser alterado pelas partes, mediante termo aditivo.

1. A **CONTRATADA** é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

2. As supressões e acréscimos resultantes de acordo celebrado entre a **CONTRATADA** e a **CONTRATANTE** poderão exceder os limites estipulados no item anterior.

3. Nos termos do art. 136 da Lei n.º 14.133/2021, registros que não caracterizam alteração do contrato poderão ser formalizados por simples apostila.

CLÁUSULA VIGÉSIMA TERCEIRA – DA EXTINÇÃO DO CONTRATO:

O contrato se extingue quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

1. A extinção do contrato por vencimento do prazo não exonerará a **CONTRATADA** de suas responsabilidades contratuais nem das sanções que porventura lhe forem aplicadas.

1.1 A extinção a que alude este item não prejudicará o andamento de procedimento apuratório em face da **CONTRATADA**.

2. O contrato pode ser extinto antes do prazo nele fixado, sem ônus para a **CONTRATANTE**, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

2.1 A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação do contratado pelo contratante nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia.

2.2 Caso a notificação da não continuidade do contrato de que trata este item ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

3. O contrato pode ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no art. 137 da Lei n.º 14.133/21, bem como consensualmente, assegurados o contraditório e a ampla defesa.

3.1 Nessas hipóteses, aplicam-se os arts. 138 e 139 da mesma Lei.

3.2 A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a rescisão se não restringir sua capacidade de concluir o contrato.

3.3 Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

4. O termo de rescisão, sempre que possível, será precedido de:

4.1 Indenizações e multas.

4.2 Relação dos pagamentos já efetuados e ainda devidos;

4.3 Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos.

5. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório, nos termos do art. 131, caput, da Lei n.º 14.133/2021.

CLÁUSULA VIGÉSIMA QUARTA – DA RESERVA DE CARGOS:

Nos termos do art. 92, XVII, da Lei n.º 14.133/2021, a **CONTRATADA**, durante toda a vigência contratual, cumprirá a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz.

CLÁUSULA VIGÉSIMA QUINTA – DA PUBLICAÇÃO:

O presente contrato será publicado no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei n.º 14.133, de 2021, e sob a forma de extrato, no Diário Oficial Eletrônico do Ministério Público do Estado do Amazonas, após a sua assinatura, correndo as despesas por conta da **CONTRATANTE**, nos termos do art. 88, §2º, XV, do Ato n.º 008/2024/PGJ.

1. O contrato em sua íntegra será publicado no sítio oficial do Ministério Público do Estado do Amazonas, por meio do Portal da Transparência, nos termos do art. 91, caput, da Lei n.º 14.133/2021, e do art. 5º, II, da Resolução n.º 86/2012, do Conselho Nacional do Ministério Público - CNMP.

CLÁUSULA VIGÉSIMA SEXTA – DAS NORMAS APLICÁVEIS:

A **CONTRATADA** declara conhecer todas as normas abaixo e concorda em sujeitar-se às estipulações, sistemas de penalidades e demais regras delas constantes, mesmo que não expressamente transcritas no presente instrumento:

1. Lei n.º 14.133/2021 – Licitações e Contratos;

2. Lei n.º 10.406/2002 – Código Civil Brasileiro;

3. Lei n.º 8.078/1990 – Código de Defesa do Consumidor;

4. Decreto Federal n.º 6.481/2008 – Lista de Piores Formas de Trabalho Infantil;

5. Resolução n.º 37/2009, do Conselho Nacional do Ministério Público – CNMP;

6. Instrução Normativa n.º 5/2017, do Ministério do Planejamento, Desenvolvimento e Gestão, de forma subsidiária;

7. Ato n.º 008/2024/PGJ – Procedimentos Administrativos de Contratação de Bens e Serviços no Âmbito do Ministério Público do Estado do Amazonas; e

8. Demais legislações correlatas, de forma suplementar, à luz das normas específicas vigentes.

CLÁUSULA VIGÉSIMA SÉTIMA – DAS DISPOSIÇÕES FINAIS E DOS CASOS OMISSOS:

A **CONTRATADA**, em cumprimento à Resolução n.º 37/2009 do Conselho Nacional do Ministério Público e ao art. 48, parágrafo único, da Lei n.º 14.133/2021, declara que não possui cônjuge, companheira ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do Ministério Público do Estado do Amazonas.

1. A **CONTRATADA** e seus representantes legais apresentaram neste ato os documentos comprobatórios de suas condições jurídico-pessoais indispensáveis à lavratura do presente, inclusive a Certificação de Regularidade dos órgãos fiscais previdenciários públicos, a que estiver vinculada.

2. Os casos omissos neste contrato serão resolvidos pela Administração Superior da **CONTRATANTE***,* baseados na legislação vigente.

CLÁUSULA VIGÉSIMA OITAVA – DO FORO CONTRATUAL:

As questões decorrentes da execução deste instrumento, que não possam ser dirimidas administrativamente, serão processadas e julgadas na justiça estadual, no foro de Manaus/AM, com expressa renúncia da **CONTRATADA** a qualquer outro que tenha ou venha a ter, por mais privilegiado que seja.

E, por estarem de acordo, foi o presente termo de contrato, depois de lido e anuído, assinado digitalmente pelas partes e por duas testemunhas.

Manaus, data da última assinatura eletrônica das partes.

(assinado eletronicamente)
ANDRÉ VIRGÍLIO BELOTA SEFFAIR
Subprocurador-Geral de Justiça para Assuntos Administrativos
Ministério Público do Estado do Amazonas

(assinado eletronicamente)
_____
Representante Legal da Contratada
Empresa _____

Documento assinado eletronicamente por **Adenilson Roberto de Oliveira Filho**, **Chefe da Divisão de Contratos e Convênios - DCCON**, em 17/12/2025, às 13:46, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2033432** e o código CRC **257337B8**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Av. Coronel Teixeira,nº 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MEMORANDO Nº 461.2025.DCCON - CONTRATOS.2033498.2025.007562

Manaus, [data da assinatura eletrônica].

À Senhora
SARAH MADALENA BARBOSA CORTES DE MELO
Presidente da Comissão Permanente de Licitação - CPL

Assunto: Encaminha a Minuta de Contrato Administrativo n.º 69.2025.DCCON - CONTRATOS.2033432.2025.007562 (2033432).

Senhora Presidente,

Em virtude de uma análise mais detalhada dos presentes autos, esta Divisão de Contratos e Convênios (DCCON) remete o novel esboço em epígrafe, com a inclusão da **Cláusula Décima Quarta - Da Garantia Contratual**.

Informamos que essa retificação ocorreu devido à quantia estimada para a contratação - aproximadamente **R $ 12.000.000,00 (doze milhões de reais)**, demandando maior resguardo dos interesses da Administração.

Atenciosamente,

[*assinado eletronicamente*]
ADENILSON ROBERTO DE OLIVEIRA FILHO
Chefe da Divisão de Contratos e Convênios
Ministério Público do Estado do Amazonas

Documento assinado eletronicamente por **Adenilson Roberto de Oliveira Filho**, **Chefe da Divisão de Contratos e Convênios - DCCON**, em 17/12/2025, às 13:47, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2033498** e o código CRC **A48B18E5**.

MINUTA DE EDITAL Nº 79.2025.CPL.2031551.2025.007562

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
PROCURADORIA GERAL DE JUSTIÇA
UASG 925849

OBJETO

Contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma **solução de datacenter,** contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses.

VALOR TOTAL DA CONTRATAÇÃO

Orçamento sigiloso

DATA DA SESSÃO PÚBLICA

Dia **XX/XX/202X** às **10h (horário de Brasília)**

CRITÉRIO DE JULGAMENTO:

[X] MENOR PREÇO / **[__]** MAIOR DESCONTO por [ ] ITEM / [ ] POR GRUPO / **[X] GLOBAL**

MODO DE DISPUTA:

[X] ABERTO / **[_]** ABERTO E FECHADO / **[_]** FECHADO E ABERTO

PREFERÊNCIA ME/EPP/EQUIPARADAS

[__] SIM / [X] NÃO

SUMÁRIO

1. DAS DISPOSIÇÕES GERAIS
2. DO OBJETO
3. DOS RECURSOS ORÇAMENTÁRIOS
4. DO CREDENCIAMENTO
5. DAS CONDIÇÕES PARA PARTICIPAÇÃO
6. DO ENVIO DAS PROPOSTAS E DOS DOCUMENTOS DE HABILITAÇÃO
7. DO PREENCHIMENTO DA PROPOSTA
8. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES
9. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA
10. DA FASE DE JULGAMENTO
11. DA HABILITAÇÃO
12. DOS RECURSOS ADMINISTRATIVOS
13. DA REABERTURA DA SESSÃO PÚBLICA
14. DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO
15. DOS PRAZOS E CONDIÇÕES DE ENTREGA E RECEBIMENTO
16. O TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE
17. DAS OBRIGAÇÕES DA CONTRATADA
18. DAS OBRIGAÇÕES DA CONTRATANTE
19. DO PAGAMENTO
20. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES
21. DA REPACTUAÇÃO, REAJUSTE E REVISÃO DE PREÇO
22. DOS ESCLARECIMENTOS E DA IMPUGNAÇÃO DO ATO CONVOCATÓRIO
23. DAS DISPOSIÇÕES FINAIS

EDITAL DO PREGÃO ELETRÔNICO 94.0XX/202X/CPL/PGJ

O **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS** pelo presente edital e por intermédio da **PROCURADORIA GERAL DE JUSTIÇA**, cadastrada no CNPJ sob o n.º 04.153.748/0001-85, tendo em vista o que consta do **Processo SEI n.º 2025.007562**, através da **COMISSÃO PERMANENTE DE LICITAÇÃO – CPL**, designada pelo Ato PGJ n.º 165/2025, e alterações, de lavra da Procuradora-Geral de Justiça, torna público que realizará licitação, na modalidade **PREGÃO, na forma ELETRÔNICA, com critério de julgamento MENOR PREÇO GLOBAL**, com modo de disputa "**ABERTO"**, nos termos da Lei nº 14.133, de 2021, do Ato PGJ n.º 008/2024 e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

O contrato correspondente, ou o instrumento que vier a substituí-lo, será regido pela Lei nº 14.133, de 2021 e suas alterações.

PROCESSO SEI	**2025.007562**
Recebimento das propostas	a partir da data de publicação do aviso no PNCP
Abertura das propostas	às 10h do dia **XX/XX/202X** (horário de Brasília)
Licitação exclusiva para ME/EPP	**( ) SIM (*X*) NÃO**
Endereço eletrônico	https://www.gov.br/compras/pt-br
Código UASG	925849

1. DAS DISPOSIÇÕES GERAIS

1.1. O pregão será realizado em sessão pública, por meio da utilização de recursos da tecnologia da informação – *internet*, utilizando-se, para tanto, de métodos de autenticação de acesso e recursos de criptografia, garantindo segurança em todas as fases do certame.

1.2. Os trabalhos serão conduzidos por servidor público integrante da **COMISSÃO PERMANENTE DE LICITAÇÃO** deste Órgão, por ato interno, denominado(a) PREGOEIRO(A), e membros da equipe de apoio, previamente credenciados no aplicativo https://www.gov.br/compras/pt-br.

1.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública, observarão rigorosamente o horário de **Brasília – DF**, e, dessa forma, serão registradas no sistema eletrônico e na documentação relativa ao certame.

2. DO OBJETO

2.1. O objeto da presente licitação é a escolha da proposta mais vantajosa para a **contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses**, de acordo com as condições constantes do Edital e seus anexos.

2.2. Por tratar-se de solução integrada, onde o funcionamento efetivo e satisfatório depende de cada um dos seus itens e serviços em conjunto, como um todo, o objeto da presente licitação será organizado em **LOTE ÚNICO**, de acordo com as especificações constantes do **TERMO DE REFERÊNCIA N.º 28.2025.DTIC.2002143.2025.007562**, conforme tabela abaixo:

ITEM	DESCRIÇÃO	QUANTIDADE
01	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9	4
02	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU	1
03	SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX	5

04	SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU	1
05	LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE	50
06	SOFTWARE DE BACKUP DE DADOS	1
07	EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	1
08	SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	1
09	SWITCH CORE	2

2.3. No presente certame não haverá itens com participação exclusiva à microempresas e empresas de pequeno porte, nos termos do art. 48 da Lei Complementar nº 123, de 14 de dezembro de 2006.

2.4. O critério de julgamento adotado será o **menor preço GLOBAL**, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.

2.4.1. Em observância ao disposto no §1º do art. 82 da Lei Federal nº 14.133/2021, o critério de julgamento de menor preço GLOBAL foi adotado, pois, por se tratar de uma solução integrada, a licitação por itens não se revela vantajosa técnica e economicamente, no presente caso.

2.4.2. Não obstante, na fase de aceitação da proposta, serão observados, como critério de aceitabilidade, os preços unitários máximos estimados para cada item.

2.5. O objeto da futura contratação compreenderá, sobretudo, as especificações constantes do **TERMO DE REFERÊNCIA Nº 28.2025.DTIC.2002143.2025.007562**, Anexo I deste Edital, sem prejuízo das demais prescrições figuradas no mencionado documento, bem assim na Minuta do Contrato Administrativo Nº 68.2025.DCCON - CONTRATOS.2031978.2025.007562, Anexo II do Edital.

2.6. Os valores apresentados nos orçamentos e/ou propostas de preço deverão considerar inclusas todas as despesas relativas a frete, taxas, análises, amostras, impostos, licenças, encargos sociais, ou outras que possam influir direta ou indiretamente nos custos.

2.7. Integra a presente licitação, como parte indissolúvel deste Edital:

a) Anexo I — Terno de Referência nº 28.2025.DTIC.2002143.2025.007562;

b) Anexo II — Minuta de Contrato Administrativo Nº 69.2025.DCCON - CONTRATOS.2033432.2025.007562;

c) Anexo III — Modelo de Declarações Complementares;

d) Anexo IV — Modelo de Proposta de Preços;

e) Anexo V — Modelo de Solicitação de Cadastramento – SEFAZ/AM;

f) Anexo VI — Modelo de Credenciamento para Vistoria Técnica;

g) Anexo VII — Modelo de - Atestado de Vistoria Técnica; e

h) Anexo VIII — Modelo de Dispensa de Vistoria Técnica.

3. DOS RECURSOS ORÇAMENTÁRIOS

3.1. A despesa decorrente da contratação do objeto deste Pregão, quando efetivada, deverá recair por conta dos recursos específicos consignados no orçamento da PROCURADORIA-GERAL DE JUSTIÇA DO ESTADO DO AMAZONAS, nas seguintes classificações orçamentárias:

3.1.1. **Fonte de Recurso:** 1.500.100 - Recursos não Vinculados de Impostos, **Programa de Trabalho:** 03.091.3234.2536.0001 - Aparelhamento de Unidades Administrativas e Operacionais, **Elemento:** 4490.52 - Equipamentos e Material Permanente. **Subelemento:** 4490.52.55 - Tecnologia da Informação**.**

4. DO CREDENCIAMENTO

4.1. As empresas interessadas em participar do certame deverão providenciar, previamente, o credenciamento perante o Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras), por meio de Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil

4.1.1. Para ter acesso ao sistema eletrônico, os interessados em participar deste pregão deverão dispor de chave de identificação e senha pessoal, obtidas junto ao SICAF, onde também deverão informar-se à respeito do seu funcionamento, regulamento e receber instruções detalhadas para sua correta utilização.

4.1.2. O credenciamento da licitante, bem como a sua manutenção, dependerá de registro cadastral atualizado no **SISTEMA DE CADASTRAMENTO UNIFICADO DE FORNECEDORES – SICAF**, em seu nível básico, que também será requisito obrigatório para fins de habilitação.

4.1.3. O credenciamento junto ao provedor do sistema implica a responsabilidade legal da licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes ao pregão eletrônico.

4.2. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou do **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS** (entidade promotora da licitação) por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

4.3. É de responsabilidade do licitante Cadastrado conferir a exatidão dos seus dados cadastrais no SICAF e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

4.3.1. A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação.

5. DAS CONDIÇÕES PARA PARTICIPAÇÃO

5.1. Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação, legalmente constituídos, desde que atendam às condições exigidas deste Edital e seus Anexos, inclusive quanto à documentação exigida, e que estejam com Credenciamento regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF.

5.1.1. **A licitante deverá declarar em campo próprio do sistema eletrônico a condição de microempresa ou empresa de pequeno porte**, para os fins previstos na Lei Complementar nº. 123/06.

5.1.1.1. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 16 da Lei nº 14.133, de 2021, para o agricultor familiar, o produtor rural pessoa física e para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006.

5.1.2. Os interessados deverão atender às condições exigidas no cadastramento no Sicaf até o terceiro dia útil anterior à data prevista para recebimento das propostas.

5.2. O licitante deverá estar devidamente credenciado no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras), por meio de Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil.

5.3. O licitante deverá manifestar, em campo próprio do sistema eletrônico, que cumpre plenamente os requisitos de habilitação, e que sua proposta está em conformidade com as exigências do instrumento convocatório.

5.4. Será exigida do licitante Declaração de Elaboração Independente de Proposta, a qual será feita no campo do sistema *Comprasnet* destinado para tanto e/ou nas Declarações Complementares de Habilitação, conforme Anexo III deste Edital.

5.5. Todos os custos decorrentes da elaboração e apresentação de propostas serão de responsabilidade exclusiva da licitante, não sendo o **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**, em nenhum caso, responsável pelos mesmos, inclusive, pelas transações que forem efetuadas em nome do participante no Sistema Eletrônico ou por eventual desconexão.

5.6. **Não poderá participar, direta ou indiretamente**, desta licitação ou da execução dos serviços e do fornecimento de bens a eles necessários:

5.6.1. Os interessados que não atendam às condições deste Edital e seus anexos;

5.6.2. Autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados;

5.6.3. Empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários;

5.6.4. Pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

5.6.4.1. O impedimento de que trata o item 5.6.4. será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

5.6.4.2. Nos termos do art. 42 do Ato nº 008/2024/PGJ "*É vedado ao Ministério Público contratar com pessoas físicas ou jurídicas que em regular processo administrativo foram declaradas impedidas de licitar e contratar com a administração pública direta ou indireta, nas esferas federal, estadual ou municipal, assim como com pessoas físicas ou jurídicas que estão impedidas de contratar com o Poder Público em decorrência de condenação judicial por atos de improbidade administrativa*."

5.6.5. Aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

5.6.6. Empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

5.6.7. Pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

5.6.8. Agente público do órgão ou entidade licitante;

5.6.8.1. A vedação de que trata o item 5.6.8 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

5.6.8.2. É vedada a contratação, durante a vigência do contrato, da prestação de serviço por empregados de empresas fornecedoras de mão de obra que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de dirigente do órgão ou entidade contratante ou de agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato (art. 48, parágrafo único, da Lei de Licitações n. 14.133/2021), de membro ou de servidor do MPAM, nela compreendido o ajuste mediante o acolhimento recíproco para a prestação de serviço entre os Ministérios Públicos ou entre esses e órgãos da Administração Pública direta e indireta dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios, bem como é vedada a realização, manutenção, aditamento ou prorrogação de contrato de prestação de serviços com empresa que tenha entre seus empregados colocados à disposição do Ministério Público para o exercício de funções de chefia, pessoas que incidam nas vedações constantes na Resolução n. 177, de 5 de julho de 2017, do Conselho Nacional do Ministério Público. (Art. 42, §4º do Ato nº 008/2024/PGJ)

5.6.9. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

5.6.10. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei n.º 14.133, de 2021.

5.6.11. Interessado que se encontre em processo de Falência, Recuperação Judicial e Extrajudicial (conforme Lei nº. 11.101/05), salvo decisão judicial em contrário (conforme Acordão 1201/2020 - TCU - PLENÁRIO), concurso de credores, insolvência, dissolução, liquidação, fusão, cisão, incorporação, salvo devidamente justificado;

5.6.12. Interessado(s) em regime de consórcio, qualquer que seja sua forma de constituição, em razão da baixa complexidade de execução do objeto.

5.6.13. Empresa estrangeira não autorizada a funcionar no País e que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou

judicialmente;

5.7. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 5.6.2 e 5.6.3 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

5.8. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

5.9. O disposto nos itens 5.6.2 e 5.6.3 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

5.10. Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da Lei nº 14.133/2021.

5.11. A **declaração falsa** relativa ao cumprimento dos requisitos de habilitação e proposta **sujeitará o licitante às sanções** previstas neste Edital.

5.12. DA VISTORIA TÉCNICA. Considerando que na presente contratação a avaliação prévia do local de execução é relevante para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, o licitante deve atestar, sob pena de desclassificação, que conhece o local e as condições de realização do serviço, assegurado a ele o direito de realização de vistoria prévia.

5.12.1. As empresas LICITANTES PODERÃO realizar, sob o acompanhamento de servidor especialmente designado, vistoria às unidades da Procuradoria-Geral de Justiça, em data e horário previamente acordados segundo a conveniência deste Órgão, com o objetivo de conhecer as instalações onde serão executados os serviços e sanar as dúvidas porventura existentes, a fim de subsidiar a elaboração das propostas a serem submetidas ao certame.

5.12.2. A vistoria deverá ser realizada por representante devidamente credenciado pela empresa LICITANTE, devidamente municiado de documento próprio de credenciamento, conforme ANEXO VI deste Edital;

5.12.3. A comprovação de realização da vistoria será efetuada por meio de apresentação de Atestado de Vistoria Técnica - conforme modelo constante do ANEXO VII deste Edital, que será emitido pelo interessado, assinado por servidor designado da DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - DTIC desta PGJ/AM;

5.12.4. O Atestado de Vistoria Técnica será assinado por servidor do MPAM que acompanhar a vistoria, e deverá ser encaminhada juntamente com a proposta;

5.12.5 As visitas deverão ser previamente agendadas, com 24 (vinte e quatro) horas de antecedência, pelo telefone (92) 3655-0670/0660 – DTIC, no período das 8h às 14h e poderão ser realizadas em até 2 (dois) dias úteis anteriores à data estipulada para abertura da licitação.

5.13. Caso o licitante opte por não realizar vistoria, poderá substituir a declaração exigida no presente item por uma Declaração de Dispensa de Vistoria Técnica assinada pelo seu responsável técnico acerca do conhecimento pleno das condições e peculiaridades da contratação, nos termos do ANEXO VIII deste Edital, que deverá ser encaminhada juntamente com a proposta;

5.14. Não serão aceitas alegações posteriores advindas de desconhecimento das condições prediais, das características do ambiente de prestação dos serviços ou erro orçamentário por parte da futura contratada, quando da execução dos serviços propostos.

6. DO ENVIO DAS PROPOSTAS E DOS DOCUMENTOS DE HABILITAÇÃO

6.1. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço ou o percentual de desconto, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.

6.1.1. Levando-se em conta as nuances do objeto e da inviabilidade de seu parcelamento, somente serão aceitas propostas para o quantitativo total estimado para cada item.

6.2. Caso a fase de habilitação anteceda as fases de apresentação de propostas e lances, os licitantes encaminharão, na forma e no prazo estabelecidos no item anterior, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto nos itens 7.1.1 e 7.12.1 deste Edital.

6.3. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

6.3.1. está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

6.3.2. não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

6.3.3. não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

6.3.4. cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

6.4. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021.

6.5. O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021.

6.5.1. no item exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item;

6.5.2. nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

6.6. A falsidade da declaração de que trata os itens 6.3. ou 6.5. sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

6.7. O envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.

6.8. Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.

6.9. As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1º da LC nº 123, de 2006.

6.10. Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

6.11. Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema.

6.12. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

6.13. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

6.14. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá às seguintes regras:

6.14.1. a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

6.14.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo estabelecido e o intervalo de que trata o subitem acima.

6.15. O valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

6.15.1. valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço; e

6.15.2. percentual de desconto inferior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por maior desconto.

6.16. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 6.14. possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

6.17. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

7. DO PREENCHIMENTO DA PROPOSTA

7.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos (no que couber):

7.1.1. Valor unitário e total do item;

7.1.2. Marca;

7.1.3. Fabricante;

7.1.4. Descrição detalhada do objeto, contendo as informações similares à especificação do Termo de Referência: indicando, no que for aplicável, o modelo, prazo de validade ou de garantia, número do registro ou inscrição do bem no órgão competente, quando for o caso, **sem identificação da licitante**;

7.1.4.1. Não serão aceitas propostas escritas contendo especificações que não contenham as informações necessárias à perfeita caracterização do objeto e suas especificidades, bem como especificações vagas e incompletas.

7.2. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

7.3. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

7.4. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

7.5. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

7.6. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

7.7. O **prazo de validade da proposta não será inferior a 90 (noventa) dias**, a contar da data de sua apresentação.

7.8. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais/estaduais, quando participarem de licitações públicas.

7.8.1. Caso o critério de julgamento seja o de maior desconto, o preço já decorrente da aplicação do desconto ofertado deverá respeitar os preços máximos previstos no item 7.8.

7.9. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a fiscalização do Tribunal de Contas do Estado do Amazonas e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

7.10. O CNPJ da proponente, empresa cadastrada no SICAF e habilitada na licitação, deverão ser o mesmo para efeito de emissão das notas fiscais e posterior pagamento.

7.11. Serão irrelevantes quaisquer ofertas que não se enquadrem nas especificações exigidas, ou

Anexos não solicitados, considerando-se que pelo preço proposto, a empresa obrigar-se-á a executar os serviços/entregar os produtos descritos neste Edital.

7.12. Para efeito de elaboração das propostas, caso haja divergência entre a especificação contida neste Edital e a no sistema SIASG, prevalecerá a descrita neste Edital.

8. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

8.1. A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

8.2. Um vez aberta a sessão, não será mais possível a substituição da proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema.

8.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

8.4. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

8.5. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

8.6. Os licitantes poderão oferecer lances sucessivos, observando as regras estabelecidas no Edital.

8.6.1. Os lances para grupos serão feitos em telas diferentes da tela principal do envio de lances, para cada item do grupo.

8.6.2. O lance vencedor será o menor lance na soma total dos itens do grupo.

8.6.3. O licitante poderá oferecer lance de **valor inferior ou percentual de desconto superior** ao último por ele ofertado e registrado pelo sistema.

8.6.4. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

8.7. O **critério de julgamento adotado será o menor preço GLOBAL**, conforme definido neste Edital e seus anexos.

8.8. **O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser R$ 10,00 (dez reais)**.

8.9. O intervalo entre os lances enviados pelo mesmo licitante não poderá ser inferior a vinte (20) segundos e o intervalo entre lances não poderá ser inferior a três (3) segundos, sob pena de serem automaticamente descartados pelo sistema os respectivos lances (quando implementado).

8.10. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

8.11. O procedimento seguirá de acordo com o modo de disputa adotado.

8.12. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa "**ABERTO**", os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

8.12.1. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

8.12.2. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

8.12.3. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

8.12.4. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

8.12.5. Após o reinício previsto no item supra, os licitantes serão convocados para apresentar lances intermediários.

8.13. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa "**ABERTO E FECHADO**", os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

8.13.1. A etapa de lances da sessão pública terá duração inicial de quinze minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de tempo de até dez minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

8.13.2. Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

8.13.3. No procedimento de que trata o subitem supra, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

8.13.4. Não havendo pelo menos três ofertas nas condições definidas neste item, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

8.13.5. Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

8.14. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa "**FECHADO E ABERTO**", poderão participar da etapa aberta somente os licitantes que apresentarem a proposta de menor preço/ maior percentual de desconto e os das propostas até 10% (dez por cento) superiores/inferiores àquela, em que os licitantes apresentarão lances públicos e sucessivos, até o encerramento da sessão e eventuais prorrogações.

8.14.1. Não havendo pelo menos 3 (três) propostas nas condições definidas no **item 8.14**, poderão os licitantes que apresentaram as três melhores propostas, consideradas as empatadas, oferecer novos lances sucessivos.

8.14.2. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

8.14.3. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

8.14.4. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

8.14.5. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

8.14.6. Após o reinício previsto no subitem supra, os licitantes serão convocados para apresentar lances intermediários.

8.15. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

8.16. Em caso de falha no sistema, os lances em desacordo com os subitens anteriores deverão ser desconsiderados pelo pregoeiro, devendo a ocorrência ser comunicada imediatamente ao Órgão Gestor do Sistemas de Compras do Governo Federal.

8.16.1. Na hipótese do subitem anterior, a ocorrência será registrada em campo próprio do sistema.

8.17. **Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar**.

8.18. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada à identificação do licitante.

8.19. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

8.20. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a 10 (dez) minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

8.21. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas

e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da LC nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

8.21.1. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

8.21.2. A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

8.21.3. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

8.21.4. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

8.22. **Havendo eventual empate** entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021.

8.22.1. Persistindo o empate após as medidas do item 8.23, o sistema fará um sorteio eletrônico das propostas empatadas, a ser realizado em ato público, para o qual todos os licitantes serão convocados, vedado qualquer outro processo, nos termos da **Instrução Normativa SEGES/ME n.º 73, de 2022.**

8.23. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, o pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

8.23.1. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

8.23.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

8.24. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

9. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

9.1. O pregoeiro solicitará ao licitante melhor classificado que, **no prazo máximo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada**, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

9.1.1. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo

9.2. Na proposta vencedora a ser enviada posteriormente deverá constar, conforme modelo do **Anexo IV**:

a) Os valores, os preços e os custos utilizados terão como expressão monetária a moeda corrente nacional (art. 13º, I, da Lei nº 14.133/2021). Ocorrendo divergência entre os preços unitários e o preço total, prevalecerão os primeiros; no caso de divergência entre os valores numéricos e os valores expressos por extenso, prevalecerão estes últimos.

a.1.) Não será admitido nos preços o fracionamento de centavo que ultrapassar duas casas decimais, desprezando-se sumariamente a fração remanescente;

a.2.) No preço deverão estar incluídas todas as despesas que influam no custo, tais como: impostos, transportes, seguros, taxas e outras despesas necessárias ao fornecimento dos materiais e à execução dos serviços correspondentes;

a.3.) Ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo licitante ou seu representante legal;

a.4.) Não se admitirá, na proposta de preços, custos identificados mediante o uso da expressão "verba" ou de unidades genéricas.

b) **Prazo de validade da proposta de, no mínimo, 90 (noventa) dias corridos**, a contar da data;

c) Especificações claras, completas e minuciosas, com detalhes do objeto ofertado, inclusive marca, modelo, tipo e referência, no que couber, observadas as especificações mínimas e quantitativos contidos neste Edital e anexos;

d) A oferta deverá ser firme e precisa, limitada, rigorosamente, ao objeto deste Edital, sem conter alternativas de preço ou de qualquer outra condição que induza o julgamento a mais de um resultado, sob pena de desclassificação;

e) Prazo de entrega da solução: **Até 60 (sessenta) dias corridos**, contados da assinatura do Contrato, consoante **Item 4.1 do Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562**, *Anexo I* e parte integrando deste Edital;

f) **Prazo de garantia/assistência técnica: pelo período de 60 (sessenta) meses, conforme dispõe o Item 1.1 do Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562**, *Anexo I* e parte integrando deste Edital; **.**

g) Os seguintes dados da licitante: Razão Social, endereço, telefone/fax, número do CNPJ/MF, *e-mail*, se houver, Banco, agência, número da conta-corrente e praça de pagamento;

h) Nome, CNPJ ou CPF dos **3 (três) principais integrantes do quadro societário da licitante,** assim compreendidos aqueles que detenham maior parcela das cotas societárias ou o poder de gestão da sociedade;

i) Contato para fins de faturamento: (indicar o nome, cargo, endereço, telefone, fax, *e-mail* de contato do responsável pelo recebimento das futuras notas de empenho)**.**

j) Quando solicitada pelo Pregoeiro, **documentação técnica (manuais, catálogos, prospectos, links da fabricante)**, com as características detalhadas (marca, modelo, cor, tipo de material e medidas - no que couber) e imagens ilustrativas dos produtos propostos, que possibilitem a completa averiguação de conformidade com as especificações, visando facilitar a avaliação a ser realizada por técnicos deste Órgão.

9.3. As **Declarações Complementares, referentes ao Anexo III do Edital**, observado as exigências mínimas do Termo de Referência, deverão ser efetuadas no momento da elaboração e envio da proposta pelos fornecedores, em seu próprio conteúdo ou documento apartado, sendo elas que:

a) Cumpre plenamente os requisitos de habilitação, ciente de que responde pela veracidade das informações prestadas, na forma da lei;

b) Em atenção **item 5.6.** e **art. 14.º e seus incisos da Lei n.º 14.133/2021**, não está impedida de participar direta ou indiretamente desta licitação, e ainda, que não possue sócios, diretores ou gerentes, que sejam cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do Ministério Público do Estado do Amazonas e de sua CPL;

c) Recebeu o edital e todos os documentos que o integram, dispondo de todos os elementos e informações necessários à elaboração da proposta de preços com total e completo conhecimento do objeto da licitação;

d) Os documentos e declarações apresentados são fiéis e verdadeiros;

e) Caso seja vencedor do certame e não cadastrado no SISTEMA DE ADMINISTRAÇÃO FINANCEIRA E CONTABILIDADE da SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ-AM, encaminhará a CONTRATANTE os documentos necessários para efetuar o referido cadastramento no prazo de 05 (cinco) dias úteis, a contar da adjudicação, sob pena de perder o direito de preferência à contratação em favor dos demais licitantes subsequentes, sem prejuízo da possibilidade de responder a procedimento administrativo de responsabilização (PAR) por eventual retardamento da licitação;

f) O preço inclui além do lucro, todos os custos e despesas, com tributos incidentes e encargos devidos, materiais, serviços, transporte, a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas, bem como quaisquer outras despesas diretas e indiretas incidentes na prestação de serviços;

g) Que apresentará, quando da contratação, documento que indique o pessoal técnico operacional, das instalações e do aparelhamento adequado e disponíveis para a realização do objeto da licitação, bem como a qualificação de cada membro da equipe técnica que se

responsabilizará pelos trabalhos.

h) Que a licitante se submete e concorda com todos os termos do presente Edital, elementos e especificações nele contidos e que os cumprirá fielmente, inclusive, que se submete à fiscalização e ao controle técnico a ser efetuado por profissional técnico expressamente designado para tal.

i) A proposta apresentada para participar do presente Pregão foi elaborada de maneira independente por esta licitante e o seu conteúdo não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer outro participante potencial ou de fato, por qualquer meio ou por qualquer pessoa.

9.4. A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do contrato e aplicação de eventual sanção à Contratada, se for o caso.

9.4.1. Todas as especificações do objeto contidas na proposta, tais como marca, modelo, tipo, fabricante e procedência, vinculam a Contratada.

9.5. A proposta deverá obedecer aos termos deste Edital e seus Anexos, não sendo considerada aquela que não corresponda às especificações ali contidas ou que estabeleça vínculo à proposta de outro licitante.

9.6. As propostas que contenham a descrição do objeto, o valor e os documentos complementares estarão disponíveis na *internet*, após a homologação.

10. DA FASE DE JULGAMENTO

10.1. Encerrada a etapa de negociação, o pregoeiro verificará se a licitante provisoriamente classificada em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no **item 5.6.** do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

a) SICAF;

b) Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/ceis); e

c) Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep).

10.1.1. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei n° 8.429, de 1992.

10.1.2. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas. (IN nº 3/2018, art. 29, *caput*)

10.1.3.1.A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros. (IN nº 3/2018, art. 29, §1º).

10.1.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação. (IN nº 3/2018, art. 29, §2º).

10.1.3.3. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

10.1.3. Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

10.1.4. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com os **itens 2.3 e 6.5.** deste edital.

10.1.5. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto nos **itens 10.4 e 10.5** deste Edital.

10.2. A proposta e documentação, se necessário, **será analisada pela equipe da DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - DTIC**, para fins de verificação do atendimento às características e exigências reclamadas no edital e anexos.

10.3. **Será desclassificada a proposta ou lance vencedor que, ressalvado o disposto no subitem 10.7. deste Edital**:

10.3.1. contiver vícios insanáveis;

10.3.2. não obedecer às especificações técnicas contidas no Edital e seus anexos;

10.3.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

10.3.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

10.3.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável;

10.3.6. Também será DESCLASSIFICADA a licitante que no momento do preenchimento do campo de ***"Descrição detalhada do objeto ofertado"*** no Sistema Comprasnet identifique sua empresa, o que não se confunde com a proposta inicial juntada ao Sistema e a proposta final e reajustada após convocação pelo Pregoeiro.

10.4. No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

10.4.1. A inexequibilidade, na hipótese de que trata o ***caput***, só será considerada após diligência do pregoeiro, que comprove:

10.4.1 1. que o custo do licitante ultrapassa o valor da proposta; e

10.4.1.2. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

10.5. Em contratação de serviços de engenharia, além das disposições acima, a análise de exequibilidade e sobrepreço considerará o seguinte:

10.5.1. Nos regimes de execução por tarefa, empreitada por preço global ou empreitada integral, semi-integrada ou integrada, a caracterização do sobrepreço se dará pela superação do valor global estimado;

10.5.2. No regime de empreitada por preço unitário, a caracterização do sobrepreço se dará pela superação do valor global estimado e pela superação de custo unitário tido como relevante, conforme planilha anexa ao edital;

10.5.3. No caso de serviços de engenharia, serão consideradas inexequíveis as propostas cujos valores forem inferiores a 75% (setenta e cinco por cento) do valor orçado pela Administração, independentemente do regime de execução.

10.5.4. Será exigida garantia adicional do licitante vencedor cuja proposta for inferior a 85% (oitenta e cinco por cento) do valor orçado pela Administração, equivalente à diferença entre este último e o valor da proposta, sem prejuízo das demais garantias exigíveis de acordo com a Lei.

10.6. Caso o custo global estimado do objeto licitado tenha sido decomposto em seus respectivos custos unitários por meio de Planilha de Custos e Formação de Preços elaborada pela Administração, o licitante classificado em primeiro lugar será convocado para apresentar Planilha por ele elaborada, com os respectivos valores adequados ao valor final da sua proposta, sob pena de não aceitação da proposta.

10.6.1. Em se tratando de serviços de engenharia, o licitante vencedor será convocado a apresentar à Administração, por meio eletrônico, as planilhas com indicação dos quantitativos e dos custos unitários, seguindo o modelo elaborado pela Administração, bem como com detalhamento das Bonificações e Despesas Indiretas (BDI) e dos Encargos Sociais (ES), com os respectivos valores adequados ao valor final da proposta vencedora, admitida a utilização dos preços unitários, no caso de empreitada por preço global, empreitada integral, contratação semi-integrada e contratação integrada, exclusivamente para eventuais adequações indispensáveis no cronograma físico-financeiro e para balizar excepcional aditamento posterior do contrato.

10.7. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço.

10.7.1. Verificada a presença de erros sanáveis na proposta de preços, o Pregoeiro ou Administração poderá realizar diligência junto à Licitante para a devida correção apenas das falhas apontadas, **limitado a 3 (três) oportunidades**, vedada a juntada de documento novo.

10.7.2. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas.

10.8. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, **24 (vinte e quatro)** horas de antecedência, e a ocorrência será registrada em ata, caso não seja informada na sessão a nova data de reabertura.

10.9. O Pregoeiro poderá convocar o licitante para enviar documento complementar, por meio de funcionalidade disponível no sistema, **no prazo máximo de 02 (duas) horas, sob pena de não**

aceitação da proposta.

10.9.1. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no "chat" pelo licitante, antes de findo o prazo.

10.9.2. Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se os que contenham as características do material ofertado, tais como marca, modelo, tipo, fabricante e procedência, além de outras informações pertinentes, a exemplo de catálogos, folhetos ou propostas, encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pelo Pregoeiro, sem prejuízo do seu ulterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta.

10.10. **DA APRESENTAÇÃO DE AMOSTRAS.** Caso o Termo de Referência exija a apresentação de amostra, ou quando solicitado pelo Pregoeiro, o licitante classificado em primeiro lugar deverá apresentá-la, conforme disciplinado no Termo de Referência e Edital, sob pena de não aceitação da proposta.

10.10.1. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a avaliação das amostras, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

10.10.2. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

10.10.3 No caso de não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita pelo Pregoeiro, ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

10.10.4. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), o Pregoeiro analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da(s) amostra(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência.

10.10.5. Se o Termo de Referência não dispor sobre o trâmite da apresentação da amostra, caso seja solicitada a apresentação pelo Pregoeiro, o licitante classificado em primeiro lugar deve apresentá-la, sob pena de não aceitação da proposta, no local a ser indicado e dentro de **05 (cinco) dias úteis** contados da solicitação, observando-se:

10.10.5.1. Para avaliação da qualidade, os bens recebidos serão sujeitos à testes de aceitação. Após o qual, emitirá um relatório completo dos testes efetuados, devidamente assinado. Quando não estabelecido o procedimento no Termo de Referência, os testes serão constituídos das seguintes fases:

a) Abertura das embalagens;

b) Comprovação de que os materiais atendem às especificações mínimas exigidas ou superiores oferecidas;

c) Colocação de amostra dos bens em funcionamento; e

d) Testes funcionais de configuração e desempenho deles.

10.10.5.2. Por meio de mensagem no sistema, será divulgado o local e horário da realização do procedimento para a avaliação das amostras, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

10.10.5.3. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

10.10.5.4. No caso de não haver entrega da amostra ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

10.10.5.5. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), o Pregoeiro analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da(s) amostra(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência.

10.10.5.6. Os exemplares colocados à disposição da Administração serão tratados como protótipos, podendo ser manuseados e desmontados pela equipe técnica responsável pela análise, não gerando direito a ressarcimento.

10.10.5.7. Após a divulgação do resultado final da licitação, as amostras entregues deverão ser **recolhidas pelos licitantes no prazo de 10 (dez) dias corridos,** após o qual poderão ser descartadas ou incorporadas pela Administração, sem direito a ressarcimento.

10.10.5.8. Os licitantes deverão colocar à disposição da Administração todas as condições indispensáveis à realização de testes e fornecer, sem ônus, os manuais impressos em língua portuguesa, necessários ao seu perfeito manuseio, quando for o caso.

10.11. Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance

subsequente, e, assim sucessivamente, na ordem de classificação.

10.12. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a sua continuidade.

10.13. Nos itens não exclusivos para a participação de microempresas e empresas de pequeno porte, sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso.

10.14. A apresentação da proposta implicará a plena aceitação, por parte do licitante, de todas as condições estabelecidas neste Edital e seus anexos, bem como, todas as especificações do objeto contidas na proposta vinculam a Contratada.

10.15. Quando da proposta de preços não constar quaisquer das declarações complementares, os prazos previstos, quer sejam os de garantia, validade dos produtos, validade da proposta ou de entrega, entender-se-á que estão aceitos os constantes do Edital.

10.16. Encerrada a análise quanto à aceitação da proposta, o pregoeiro verificará a habilitação do licitante, observado o disposto neste Edital.

10.17. Decorrido o prazo de validade das propostas, sem convocação para contratação, ficam as licitantes liberadas dos compromissos assumidos, podendo ser consultado acerca da manutenção dos preços ofertados.

11. DA HABILITAÇÃO

11.1. Os documentos previstos no Termo de Referência e neste Edital, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.

11.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira poderá ser substituída pelo registro cadastral no Sicaf.

11.2. Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

11.2.1. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato ou da ata de registro de preços, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto n o Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

11.3. Quando permitida a participação de consórcio de empresas, a habilitação técnica, quando exigida, será feita por meio do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, quando exigida, será observado o somatório dos valores de cada consorciado.

11.3.1. Se o consórcio não for formado integralmente por microempresas ou empresas de pequeno porte e o termo de referência exigir requisitos de habilitação econômico-financeira, haverá um acréscimo de 10% para o consórcio em relação ao valor exigido para os licitantes individuais.

11.4. **Todos os documentos enviados eletronicamente deverão ser enviados em original, ou por cópia autenticada, devidamente assinado(s) pelo(s) representante(s) legal(is) no dia subsequente ao do resultado da habilitação, impreterivelmente, sob pena de desclassificação**, observado o disposto no **item 23.8.** e seguintes, à Comissão Permanente de Licitação da Procuradoria-Geral de Justiça do Estado do Amazonas, Av. Coronel Teixeira, 7.995, Nova Esperança II, CEP: 69037-473.

11.4.1. Caso a autenticação do documento ou o próprio documento esteja em formato digital, com assinatura por certificado digital, padrão ICP-Brasil, ou ainda torne possível sua convalidação em sítio eletrônico de autoridade certificadora oficial e/ou cartório digital respectivo, a licitante está dispensada da obrigação do item anterior.

11.5. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei nº 14.133/2021.

11.6. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133/2021).

11.7. Será verificado se o licitante apresentou no sistema, sob pena de inabilitação, a declaração de que

cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

11.8. O licitante deverá apresentar, sob pena de desclassificação, declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

11.9. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

11.9.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir.

11.10. É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

11.10.1. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

11.11. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

11.11.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de **02 (duas) horas**, prorrogável por igual período, contado da solicitação do pregoeiro.

11.11.2. Na hipótese de a fase de habilitação anteceder a fase de apresentação de propostas e lances, os licitantes encaminharão, por meio do sistema, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto.

11.12. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

11.12.1. Os documentos relativos à regularidade fiscal que constem do Termo de Referência somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

11.12.2. Respeitada a exceção do subitem anterior, relativa à regularidade fiscal, quando a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, a verificação ou exigência do presente subitem ocorrerá em relação a todos os licitantes.

11.13. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (Lei 14.133/21, art. 64):

11.13.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

11.13.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

11.14. Na análise dos documentos de habilitação, o Pregoeiro ou a comissão de contratação poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

11.15. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital.

11.16. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

11.17. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, e não como condição para participação na licitação (art. 4º do Decreto nº 8.538/2015).

11.18. Quando a fase de habilitação anteceder a de julgamento e já tiver sido encerrada, não caberá exclusão de licitante por motivo relacionado à habilitação, salvo em razão de fatos supervenientes ou só conhecidos após o julgamento.

11.19. Os documentos necessários à habilitação deverão estar com prazo vigente, à exceção daqueles que por sua natureza, não contenham validade, e poderão ser apresentados em original, por qualquer processo de cópia autenticada por tabelião de notas ou por servidor da CPL, ou por publicação em

órgãos da imprensa oficial, **não sendo aceitos "protocolos" ou solicitação de documento em substituição aos documentos requeridos neste Edital**.

11.20. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

11.20.1. Serão aceitos registros de CNPJ de licitante matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

11.21. Ressalvado o disposto no subitem **6.3.**, os licitantes deverão encaminhar, nos termos deste Edital, a documentação relacionada nos itens a seguir, para fins de habilitação.

11.22. Relativos à Habilitação Jurídica:

11.22.1. No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

11.22.2. Em se tratando de microempreendedor individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio http://www.portaldoempreendedor.gov.br;

11.22.3. No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

11.22.4. Inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência;

11.22.5. No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

11.22.6. No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização;

11.22.7. Os documentos relativos à Habilitação Jurídica indicados, deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

11.23. Relativo à Regularidade Fiscal e Trabalhista:

11.23.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso.

11.23.2. Prova de regularidade perante a Fazenda federal, estadual e/ou municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei.

11.23.3. Prova de regularidade relativa à Seguridade Social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei;

11.23.4. Prova de regularidade perante a Justiça do Trabalho;

11.23.5. Declaração de cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal, conforme declaração do sistema;

11.23.6. Caso o licitante detentor do menor preço seja qualificado como microempresa ou empresa de pequeno porte deverá apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição, sob pena de inabilitação.

11.23.7. A aceitação de certidões emitidas via *internet* ficará sujeita à confirmação de sua validade mediante consulta *on line* ao cadastro emissor respectivo.

11.23.8. Caso o licitante seja considerado isento dos tributos estaduais/municipais relacionados ao objeto licitatório, deverá comprovar tal condição mediante declaração da Fazenda Estadual do seu domicílio ou sede, ou outra equivalente, na forma da lei;

11.23.9. Os documentos referidos nos subitens acima poderão ser substituídos ou supridos, no todo ou em parte, por outros meios hábeis a comprovar a regularidade do licitante, inclusive por meio eletrônico (§1.º, art. 68, da Lei 14.133/21);

11.23.10. A comprovação de atendimento do disposto nos subitens 11.23.2, 11.23.3 e 11.23.11. deverá ser feita na forma da legislação específica (§2.º, art. 68, da Lei 14.133/21);

11.24. Relativos à Qualificação Econômico-Financeira:

11.24.1. Balanço patrimonial e demonstrações contábeis dos 2 (dois) últimos exercícios sociais, já exigíveis e apresentados na forma da lei, podendo ser apresentado de acordo com o Sistema Público de Escrituração Digital (SPED – Decreto Federal n.º 6.022/2007), que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios,

podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta;

11.24.1.1. O Balanço apresentado deverá cumprir as seguintes formalidades:

a) Assinatura do contador e do titular ou representante legal da empresa no balanço patrimonial e DRE (pode ser feita digitalmente);

b) Prova de registro na Junta Comercial ou Cartório (devidamente carimbado, com etiqueta, chancela da Junta Comercial ou código de registro).

11.24.1.2. No caso de fornecimento de bens para pronta entrega, não será exigido da licitante qualificada como microempresa ou empresa de pequeno porte, a apresentação de balanço patrimonial do último exercício financeiro. (Art. 3º do Decreto nº 8.538, de 2015);

11.24.1.3. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e ficarão autorizadas a substituir os demonstrativos contábeis pelo balanço de abertura;

11.24.1.4. Quando solicitado ou autorizado pelo Pregoeiro, será permitido apresentação de balanço intermediário, desde que se decorra de lei ou contrato social/estatuto social da Licitante.

11.24.1.5. A comprovação da situação financeira da empresa será constatada mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um) resultantes da aplicação das fórmulas e Patrimônio Líquido mínimo de 10% do valor estimado da proposta de preços ou do item pertinente.

11.24.3. Certidões Negativas de Falência e Recuperação Judicial (conforme Lei nº 11.101/05), expedida pela Central de Certidões do Tribunal de Justiça ou órgão equivalente do domicílio ou da sede do licitante, **expedida até 90 (noventa) dias antes da abertura desta licitação**, quando do documento não constar data expressa de validade;

11.24.3.1 Onde não houver **CENTRAL DE CERTIDÕES DO TRIBUNAL DE JUSTIÇA**, deverá ser apresentada Certidão emitida pela **SECRETARIA DO TRIBUNAL DE JUSTIÇA** ou órgão equivalente do domicílio ou da sede do licitante constando a quantidade de Cartórios Oficiais de Distribuição de Pedidos de Falência e Recuperação Judicial (conforme Lei nº 11.101/05), devendo ser apresentadas Certidões expedidas na quantidade de cartórios indicadas no respectivo documento, no prazo referido no item **11.24.3.**;

11.24.3.2. Caso os prazos de validade não constem expressamente das certidões, serão considerados para esse fim, o prazo descrito no subitem **11.24.3**. deste instrumento convocatório.

11.24.4. Os documentos referidos no item **11.24. e subitens** limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos

11.25. Relativos à Qualificação Técnica

11.25.2. **Apresentação de Atestado de Capacidade Técnica** (Art. 67, II, da Lei 14.133/21) fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado, que comprove(m) que a empresa licitante tenha executado/entregue, a contento, serviços/materiais de natureza e vulto compatíveis com o presente objeto, que permitam estabelecer, por comparação, proximidade de características funcionais técnicas, dimensionais, quantitativas e qualitativas com o objeto do presente Edital, sendo aceitável a soma de atestados para a comprovação desse quantitativo, conforme Termo de Referência**.**

11.25.1.1. Para fins de comprovação de aptidão, serão considerados compatíveis com objeto, os atestados de capacidade técnica que comprovem o fornecimento concomitante do objeto licitado ou do item vencido.

11.25.1.2. No caso de pessoa jurídica de direito público, o(s) atestado(s) ou certidão (ões) deverá (ão) ser assinado(s) pelo responsável do setor competente do órgão;

11.25.1.3. No caso de pessoa jurídica de direito privado, o(s) atestado(s) deverá(ão) conter dados suficientes para identificação civil do declarante, com referência ao cargo/função que ocupa na empresa.

11.25.1.4. A ausência de apresentação de atestado claro, legível e idôneo, em não conformidade com este Edital, será motivo de inabilitação, a critério do Pregoeiro.

11.26. Disposições Gerais da Habilitação:

11.26.1. O licitante enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado: (a) da prova de inscrição nos cadastros de contribuintes estadual e municipal.

11.26.2. Se a documentação de habilitação não estiver completa e correta ou contrariar qualquer dispositivo deste Edital e seus Anexos, **o pregoeiro considerará o proponente inabilitado**, sendo convocado outro licitante, observada a ordem de classificação, e assim **sucessivamente**, sem prejuízo das sanções legais cabíveis.

11.26.3. Sob pena de inabilitação os documentos apresentados deverão estar em nome da licitante, com o nº do CNPJ e o endereço respectivo, conforme segue:

11.26.3.1. se a licitante for a matriz, todos os documentos deverão estar em nome da matriz, e

11.26.3.2. se a licitante for a filial, todos os documentos deverão estar em nome da filial.

11.11.3.3. no caso dos subitens anteriores, serão dispensados da filial aqueles documentos que COMPROVADAMENTE, forem emitidos SOMENTE em nome da matriz, e vice-versa.

11.26.4. Caso os prazos de validade não constem expressamente das certidões apresentadas, será considerado para esse fim, o prazo descrito no subitem **11.24.3**. deste instrumento convocatório.

11.27. Havendo alguma restrição na comprovação da regularidade fiscal para microempresas e empresas de pequeno porte, lhes será assegurado o prazo de 05 (cinco) dias úteis, a contar do momento em que o licitante for declarado vencedor, prorrogáveis por igual período, a requerimento da interessada e a critério da Administração Pública, para a regularização da documentação, pagamento ou parcelamento do débito e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.

11.27.1. A não-regularização fiscal e trabalhista no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação. Se, na ordem de classificação, seguir-se outra microempresa, empresa de pequeno porte ou sociedade cooperativa com alguma restrição na documentação fiscal e trabalhista, será concedido o mesmo prazo para regularização.

11.28. Para fins de julgamento da habilitação no certame, considerar-se-á vigente o documento com prazo de validade, pelo menos, até a data de abertura da licitação.

11.29. Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a continuidade da mesma.

11.30. Nos itens não exclusivos a microempresas e empresas de pequeno porte, em havendo inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45, da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

11.31. O licitante provisoriamente vencedor em um item, que estiver concorrendo em outro item, ficará obrigado a comprovar os requisitos de habilitação cumulativamente, isto é, somando as exigências do item em que venceu às do item em que estiver concorrendo, e assim sucessivamente, sob pena de inabilitação, além da aplicação das sanções cabíveis.

11.31.1. Não havendo a comprovação cumulativa dos requisitos de habilitação, a inabilitação recairá sobre o(s) item(ns) de menor(es) valor(es) cuja retirada(s) seja(m) suficiente(s) para a habilitação do licitante nos remanescentes.

11.32. Atendidas as exigências habilitatórias fixadas neste Edital, o licitante será declarado **vencedor**, sendo-lhe adjudicado o objeto do certame, caso não haja interposição de recursos, encaminhando-se, em seguida os autos à autoridade competente para homologação.

11.33. Da sessão pública será lavrada ata circunstanciada, que mencionará todos os licitantes, a classificação dos lances, bem como as ocorrências que interessarem ao julgamento desta licitação.

12. DOS RECURSOS ADMINISTRATIVOS

12.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

12.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.

12.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

12.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

12.3.2. o prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos.

12.3.2. o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

12.3.3. na hipótese de adoção da inversão de fases prevista no§ 1º do art. 17 da Lei nº 14.133, de 2021, o prazo para apresentação das razões recursais será iniciado na data de intimação da ata de julgamento.

12.3.4. Os recursos deverão ser encaminhados em campo próprio do sistema.

12.3.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de **3 (três) dias úteis**, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

12.4. Os recursos interpostos fora do prazo não serão conhecidos.

12.5. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de**3 (três) dias úteis**, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

12.6. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

12.7. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

12.8. Os autos do processo permanecerão com vista franqueada aos interessados na**COMISSÃO PERMANENTE DE LICITAÇÃO**, localizada na Av. Coronel Teixeira, n.º 7.995, Nova Esperança, CEP.: 69037-473, nos dias úteis, no horário das 8h às 14h (horário local).

12.8.1. Os interessados poderão solicitar cópia dos autos por meio do e-mail licitacao@mpam.mp.br

12.9. Não serão providos recursos de caráter protelatório, fundada em mera insatisfação da licitante, podendo ainda ser aplicado, supletiva e subsidiariamente, no que couberem, as regras previstas na Lei n.º 13.105/2015 (Código de Processo Civil).

12.10. A alegação de preço inexequível por parte de uma das licitantes com relação à proposta de preços de outra licitante deverá ser devidamente comprovada.

12.11. A sessão pública do pregão somente será concluída após declarado o vencedor do certame e encerrado o prazo para manifestação de intenção de interposição de recurso, cabendo aos licitantes permanecerem conectados ao sistema até o final desta etapa.

12.12. Decididos os recursos, a autoridade competente fará a adjudicação do objeto da licitação ao licitante vencedor.

13. DA REABERTURA DA SESSÃO PÚBLICA

13.1. A sessão pública poderá ser reaberta:

13.1.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

13.1.2. Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal e trabalhista, nos termos do art. 43, §1º da LC nº 123/2006. Nessas hipóteses, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

13.2. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

13.2.1. A convocação se dará por meio do sistema eletrônico (“chat”) ou ainda, *e-mail*, de acordo com a fase do procedimento licitatório.

13.2.2. A convocação feita por *e-mail* dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

14. DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

14.1. O objeto da licitação será adjudicado e homologado ao licitante declarado vencedor pela autoridade competente.

14.2. Homologado o resultado, o adjudicatário, quando convocado a comparecer, terá o**prazo máximo de 5 (cinco) dias úteis**, para celebrar o contrato ou retirar o instrumento equivalente, devendo manter as condições de habilitação exibidas na licitação.

14.2.1. Se o vencedor do certame não apresentar situação regular no ato da assinatura do contrato (ou retirada do instrumento equivalente), ou recusar-se a assiná-lo, ou sobrevier fato impeditivo de sua celebração, a sessão será retomada e os demais licitantes chamados, procedendo-se na forma do item **10.11**., sem prejuízo das sanções cabíveis.

14.2.2. O vencedor do certame deverá apresentar ao órgão interessado, antes da assinatura do contrato (ou retirada do instrumento equivalente), nova proposta de preços escrita, com a devida recomposição dos custos unitários decorrentes da diminuição dos valores na fase de lances.

14.3. A homologação do resultado desta licitação não implicará direito à contratação.

15. DOS PRAZOS E CONDIÇÕES DE ENTREGA E RECEBIMENTO

15.1. As informações suficientes à execução do objeto constituem os **ITENS 4 e 6** do **TERMO DE REFERÊNCIA Nº 28.2025.DTIC.2002143.2025.007562**, Anexo I deste Edital.

15.2. O recebimento dos materiais/serviços será realizado pela fiscalização da CONTRATANTE.

16. O TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

16.1. Após a homologação da licitação, em sendo realizada a contratação, será firmado Termo de Contrato ou emitido instrumento equivalente.

16.1.1. O adjudicatário **terá o prazo de 5 (cinco) dias úteis**, contados a partir da data de sua convocação, para assinar o Termo de Contrato ou aceitar o instrumento equivalente, conforme o caso (Nota de Empenho/Carta Contrato/Autorização), sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

16.1.1.1. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato ou aceite do instrumento equivalente, a Administração poderá encaminhá-lo para assinatura ou aceite da adjudicatária, mediante correspondência eletrônica no *e-mail* constante da proposta, para que seja assinado eletronicamente pelo Sistema SEI ou aceito no prazo de 5 (cinco) dias, a contar da data de seu recebimento.

16.1.1.2. O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração;

16.1.1.3. Nos termos do art. 6º, do Decreto n º 40.674/2019, o termo contratual ou instrumento equivalente poderá ser assinado por certificação digital ou mediante assinatura eletrônica via Sistema Eletrônico de Informação - SEI, conforme disposição do ATO Nº 141/2017/PGJ;

16.1.1.3.1. O uso da senha de acesso ao Sistema Eletrônico de Informação - SEI é de **inteira e exclusiva responsabilidade da licitante**, incluindo qualquer acesso efetuado diretamente ou por seu representante, não cabendo ao MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS, promotora da licitação, **qualquer responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.**

16.1.1.4. Para fins do atendimento do disposto no item anterior, antes da assinatura da Ata de Registro de Preços – ARP, será solicitado do representante da fornecedora o preenchimento de cadastro disponível no endereço eletrônico: https://sei.mpam.mp.br/sei/controlador_externo.php?acao=usuario_externo_logar&id_orgao_acesso_externo=0 e envio dos seguintes documentos:

I – Documento de identidade;

II – Cadastro de Pessoa Física – CPF;

III – Comprovante de residência atualizado;

IV – Ato constitutivo e suas alterações, devidamente registrados; e

V – Ato de nomeação ou eleição de dirigentes ou procuração, quando for o caso, devidamente registrados.

16.1.1.5. Será dispensado da apresentação dos documentos referidos o representante que já os tiver enviado durante a sessão pública do pregão.

16.1.1.6. Ao assinar o termo contratual ou instrumento equivalente, a empresa adjudicatária obriga-se a fornecer/executar os bens/serviços a ela adjudicados, conforme especificações e condições contidas neste Edital, em seus Anexos e também na proposta apresentada, prevalecendo, no caso de divergência, as especificações e condições do Edital;

16.2. O aceite da Nota de Empenho ou do instrumento equivalente, emitida à empresa adjudicada, implica no reconhecimento de que:

16.2.1 referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 14.133, de 2021;

16.2.2. a CONTRATADA se vincula à sua proposta e às previsões contidas no Edital e seus Anexos;

16.2.3. a CONTRATADA reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 137 e 138 da Lei nº 14.133, de 2021, e reconhece os direitos da Administração previsto no artigo 139 da mesma Lei.

16.3. Previamente à contratação, a Administração realizará consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018, e nos termos do art. 6º, III, da Lei nº 10.522, de 19 de julho de 2002, consulta prévia ao CADIN.

16.4. Na assinatura do contrato ou da Ata de Registro de Preços, será exigida a comprovação das condições de habilitação consignadas no Edital, que deverão ser mantidas pelo licitante durante a vigência do contrato ou da Ata de Registro de Preços.

16.5. Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no Edital ou se recusar a assinar o contrato ou a Ata de Registro de Preços, a Administração, sem prejuízo da aplicação das sanções das demais cominações legais cabíveis a esse licitante, poderá convocar outro licitante, respeitada a ordem de classificação, para, após a comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o Contrato ou a Ata de Registro de Preços.

16.6. **DA GARANTIA CONTRATUAL**. Nos termos do art. 96 da Lei n.º 14.133/2021, para segurança do integral cumprimento do contrato, a **CONTRATADA** apresentará garantia de **5% (cinco por cento)** do valor total do contrato, observadas as disposições da Cláusula Décima Quarta da Minuta de Contrato Administrativo Nº 69.2025.DCCON - CONTRATOS.2033432.2025.007562, Anexo II deste Edital.

17. DAS OBRIGAÇÕES DA CONTRATADA

17.1. As obrigações da CONTRATADA constituem o **Item 7.1 do Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562**, bem como a **Cláusula Décima Primeira da Minuta de Contrato Administrativo Nº 69.2025.DCCON - CONTRATOS.2033432.2025.007562,** *Anexos I e II* deste Edital, respectivamente.

17.2. Se a licitante vencedora não apresentar situação de regularidade documental, no ato da emissão da nota de empenho, ou recusar-se injustificadamente a receber a nota de empenho no prazo estabelecido, os demais licitantes serão convocados observada a ordem de classificação, e assim sucessivamente, sem prejuízo da aplicação das sanções cabíveis.

17.2.1. O prazo de convocação poderá ser prorrogado uma vez, por igual período, quando solicitado pela vencedora durante o seu transcurso, desde que ocorra motivo justificado e aceito pela Administração.

17.3. A empresa deverá encaminhar, quando solicitado, via *e-mail*, os seguintes dados: Banco, agência e número da conta corrente, endereço, telefone e representante legal da empresa, com o número do CNPJ e Inscrição Estadual ou Inscrição Municipal.

18. DAS OBRIGAÇÕES DA CONTRATANTE

18.1. As obrigações da CONTRATANTE constituem o **Item 7.2 do Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562**, bem como a **Cláusula Décima da Minuta de Contrato Administrativo Nº 69.2025.DCCON - CONTRATOS.2033432.2025.007562**, *Anexos I e II* deste Edital, respectivamente.

19. DO PAGAMENTO

19.1 O pagamento resultante da contratação do objeto será efetuado de acordo com o **Item 10** do **Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562**, bem como a Cláusula Décima Sétima da **Minuta de Contrato Administrativo Nº 69.2025.DCCON - CONTRATOS.2033432.2025.007562**, *Anexos I e II* deste Edital, respectivamente, em consonância, também, com a proposta de preços aceita pela Administração.

19.2. O pagamento devido à CONTRATADA será creditado em conta corrente por meio de ordem bancária, efetuado mediante apresentação de nota fiscal/fatura atestada e visada pelos órgãos de fiscalização e acompanhamento do fornecimento do material.

19.2.1. Os prazos e condições de pagamento são as estabelecidos no Art. 140 do Ato nº 008/2024/PGJ:

I - 10 (dez dias) úteis para a liquidação da despesa, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração;

II - 10 (dez dias) úteis para pagamento, a contar da liquidação da despesa.

19.2.1.1. Para os fins de liquidação, deverá ser observado o disposto no art. 63 da Lei nº 4.320, de 17 de março de 1964, certificando-se do adimplemento da obrigação do contratado nos prazos e forma previstos no contrato.

19.2.1.2. O prazo de que trata o inciso I do caput do Art. 140 do Ato nº 008/2024/PGJ poderá ser excepcionalmente prorrogado, justificadamente, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

19.2.1.3. O prazo para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins de que trata o inciso I do caput e o § 2º do Art. 140 do Ato nº 008/2024/PGJ.

19.2.1.4. Na hipótese de caso fortuito ou força maior que impeça a liquidação ou o pagamento da despesa, o prazo para o pagamento será suspenso até a sua regularização, devendo ser mantida a posição da ordem cronológica que a despesa originalmente estava inscrita.

19.2.1.5. No caso de insuficiência de recursos financeiros disponíveis para quitação integral da obrigação, poderá haver pagamento parcial do crédito, permanecendo o saldo remanescente na mesma posição da ordem cronológica.

19.2.2. As respectivas notas fiscais/faturas, emitidas em conformidade com o Protocolo ICMS 42/2009 (NF-e), deverão estar devidamente discriminadas, em nome da **PROCURADORIA-GERAL DE JUSTIÇA, CNPJ nº 04.153.748/0001-85**, e acompanhada das respectivas Certidões Negativas de Débito para com a Seguridade Social, para com o Fundo de Garantia por Tempo de Serviço, junto à Justiça Trabalhista e, ainda, das certidões de regularidade junto à Fazenda Federal, Estadual e Municipal, conforme descrito no link: https://www.mpam.mp.br/servicos-sp261893274/licitacoes/34-licitacoes/paginas-internas-licitacoes/2148-orientacaopagamentofornecedor;

19.2.3. Deverão constar das Notas Fiscais as especificações dos serviços, o número da Nota de Empenho e do instrumento contratual correspondente, conforme o caso;

19.2.4. Enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência contratual, nenhum pagamento será efetuado à Contratada, sem que isso gere direito a acréscimos de qualquer natureza.

19.3. Qualquer atraso ocorrido na apresentação da nota fiscal/fatura, ou dos documentos exigidos como condição de pagamento por parte da CONTRATADA, importará prorrogação automática do prazo de vencimento da obrigação do Contratante.

19.4. Nenhum pagamento isentará o fornecedor das responsabilidades atinentes ao objeto contratual, nem tampouco implicará a aprovação definitiva da entrega, total ou parcialmente.

19.5. A nota fiscal (atestada) e os documentos exigidos no Edital e no contrato, para fins de liquidação e pagamento das despesas, deverão ser entregues, exclusivamente, no Setor de Protocolo da CONTRATANTE.

19.6. Como condição para emissão da nota de empenho, a licitante vencedora deverá manter as condições de habilitação, cuja confirmação será feita através de consulta ao SICAF ou através da internet nos respectivos sites dos órgãos emissores das certidões de regularidade fiscal.

19.7. Se a licitante vencedora não apresentar situação de regularidade documental, no ato da emissão da nota de empenho, ou se recusar injustificadamente a recebê-la no prazo estabelecido, os demais licitantes serão convocados, observada a ordem de classificação, e assim sucessivamente, sem prejuízo da aplicação das sanções cabíveis.

19.7.1. Como condição inafastável a que seja emitida Nota de Empenho à Fornecedora, esta deverá, também, estar cadastrada junto ao Sistema de Administração Financeira e Contabilidade – Cadastramento de Credores – da Secretaria da Fazendo do Estado do Amazonas – SEFAZ.

19.7.1.1. Com relação ao Cadastramento de Credores, a empresa deverá providenciar o envio dos documentos abaixo elencados ao órgão promotor da licitação (MPAM), durante o certame no próprio Sistema *Comprasnet* na fase de envio da proposta, quando convocado pelo

Pregoeiro ou posteriormente após a adjudicação para o endereço eletrônico licitacao@mpam.mp.br, sendo que naquele primeiro momento não será motivo para sua desclassificação:

a) Carta solicitando o cadastramento (conforme **Anexo V)**;

b) Comprovante de inscrição e de situação cadastral emitido pela Receita Federal do Brasil;

c) Cópia legível dos dados bancários (por ex: extrato, cópia reprográfica de cartão bancário etc.);

d) Comprovante de endereço, tais como: conta de água, energia, gás, serviços de internet ou contrato de aluguel.

19.7.1.2. Caso a vencedora não realize o **cadastro em até 5 (cinco) dias úteis** após a homologação do certame, poderá responder a procedimento de apuração de responsabilidade por eventual retardamento da execução do ajuste, com possível aplicação das sanções previstas neste Edital, bem como perda do direito de preferência à contratação em favor dos demais licitantes subsequentes:

20. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

20.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

20.1.1. deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a pregoeiro/a durante o certame;

20.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

20.1.2.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

20.1.2.2. recusar-se a enviar o detalhamento da proposta quando exigível;

20.1.2.3. pedir para ser desclassificado quando encerrada a etapa competitiva; ou

20.1.2.4. deixar de apresentar amostra;

20.1.2.5. apresentar proposta ou amostra em desacordo com as especificações do edital;

20.1.3. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

20.1.3.1. recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

20.1.4. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;

20.1.5. fraudar a licitação;

20.1.6. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

20.1.6.1. agir em conluio ou em desconformidade com a lei;

20.1.6.2. induzir deliberadamente a erro no julgamento;

20.1.6.3. apresentar amostra falsificada ou deteriorada;

20.1.7. praticar atos ilícitos com vistas a frustrar os objetivos da licitação

20.1.8. praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

20.2. Com fulcro na Lei nº 14.133, de 2021, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

20.2.1. advertência;

20.2.2. multa;

20.2.3. impedimento de licitar e contratar e

20.2.4. declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

20.3. Na aplicação das sanções serão considerados:

20.3.1. a natureza e a gravidade da infração cometida.

20.3.2. as peculiaridades do caso concreto

20.3.3. as circunstâncias agravantes ou atenuantes

20.3.4. os danos que dela provierem para a Administração Pública

20.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

20.4. A multa será recolhida em percentual de 0,5% (cinco décimos por cento) a 30% (trinta por cento) incidente sobre o valor do contrato licitado, recolhida no prazo máximo de 5 (cinco) dias úteis, a contar da comunicação oficial.

20.4.1. Para as infrações previstas nos itens 20.1.1., 20.1.2. e 20.1.3., a multa será de 0,5% (cinco décimos por cento) a 15% (quinze por cento) do valor do contrato licitado.

20.4.2. Para as infrações previstas nos itens 20.1.4., 20.1.5., 20.1.6., 20.1.7. e 20.1.8., a multa será de 15% (quinze por cento) a 30% (trinta por cento) do valor do contrato licitado.

20.5. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

20.6. Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

20.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 22.1.1., 22.1.2. e 22.1.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito do **ESTADO DO AMAZONAS**, pelo prazo máximo de 3 (três) anos.

20.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 20.1.4, 20.1.5, 20.1.6, 20.1.7 e 20.1.8, bem como pelas infrações administrativas previstas nos itens 20.1.1, 20.1.2 e 20.1.3 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.

20.9. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 20.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor da Procuradoria-Geral de Justiça.

20.10. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

20.11. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

20.12. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

20.13. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

20.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

20.15. O disposto nos itens acima também se aplica aos integrantes do cadastro de reserva, em pregão para registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente ou com justificativa recusada pela Administração Pública.

20.16. As sanções serão aplicadas pela **AUTORIDADE COMPETENTE**, em processo regular que assegure ao acusado o direito prévio da citação, do contraditório e da ampla defesa, com os recursos a ela inerentes.

20.17. As penalidades serão obrigatoriamente publicadas no Diário Eletrônico do Ministério Público do Estado do Amazonas e registradas no Sistema de Cadastramento Unificado de Fornecedores – SICAF.

20.18. Se a CONTRATADA, sem justa causa, não cumprir as obrigações assumidas ou infringir preceitos legais, serão aplicadas as sanções previstas no **Item 8 do Termo de Referência n.º 28.2025.DTIC.2002143.2025.007562**, bem como nas **Cláusulas Décima Nona e Vigésima**

da Minuta de Contrato Administrativo Nº 69.2025.DCCON - CONTRATOS.2033432.2025.007562, Anexos I e II, respectivamente, deste instrumento convocatório, segundo a gravidade da falta, observando-se os limites estabelecidos no **subitem 20.4.**

20.19. A inexecução total ou parcial do contrato enseja a sua rescisão pelos motivos legais.

20.20. Se a multa for de valor superior ao valor da garantia prestada, além da perda desta, responderá a CONTRATADA pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela CONTRATANTE ou ainda, quando for o caso, cobrada judicialmente.

20.20.1. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, o Estado ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

20.21. Se, durante o processo de aplicação de penalidade, houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à Administração Pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização – PAR.

20.22. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

20.23. O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Estadual resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

22.24. O fluxo procedimental quanto ao procedimento preliminar e o processo de apuração de responsabilidade visando a aplicação das sanções administrativas no âmbito do Ministério Público do Estado do Amazonas está disciplinado no Ato PGJ n.º 217/2024 (publicado no DOMPE, Ed. 2874, de 02.07.2024).

21. DA REPACTUAÇÃO, REAJUSTE E REVISÃO DE PREÇO

21.1. A interessada deverá protocolar o seu pedido de repactuação, reajuste e revisão de preços antes da assinatura do contrato ou, nos casos em que este vier a ser substituído por instrumento equivalente, **em até 5 (cinco) dias do recebimento da Nota de Empenho**, sob pena de não apreciação do pedido por intempestividade.

21.1.1. Deverá constar do pedido a planilha de custos e documentos comprovantes da situação superveniente, decorrente de caso fortuito ou de força maior.

21.1.2. A CONTRATADA deverá demonstrar de maneira clara a composição do preço de cada item constante de sua proposta, através de Planilha de Custos contendo, por exemplo: as parcelas relativas à mão de obra direta, demais insumos, encargos em geral, lucro e participação percentual em relação ao preço final.

21.1.3. O pedido deverá vir instruído com os seguintes documentos/informações:

a) Planilha ou equivalente, contendo o custo (preço de custo, impostos, frete, lucro) de cada item constante da proposta inicial em confronto com a nova planilha atualizada, a fim de comprovar a elevação dos encargos do particular;

b) Demonstração de forma cabal que o desequilíbrio decorre de fato superveniente, isto é, ocorrência de evento posterior à apresentação da proposta;

c) Vínculo de causalidade entre o evento ocorrido e a majoração dos encargos da empresa;

d) Comprovação de que o desequilíbrio decorre de fato, imprevisível ou previsível, porém de consequências incalculáveis, apresentado, para tanto TODOS os documentos que comprovem a imprevisibilidade da ocorrência do evento (notas fiscais, cotações e etc.);

e) Memória de cálculo em conformidade com a variação pleiteada, por item;

f) Demonstração de que o desequilíbrio de fato alheio à vontade das partes.

21.2. A não-apresentação da planilha de custos impossibilitará o **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS** de proceder o reequilíbrio, reajuste ou revisão de preços, caso venha a empresa contratada solicitar qualquer uma dessas alterações no contrato.

21.3. A cada pedido de reequilíbrio, reajuste ou revisão de preço, deverá a contratada comprovar e justificar as alterações havidas na planilha apresentada à época da elaboração da proposta, demonstrando a nova composição do preço.

21.4. No caso de o detentor do registro de preços/contratado ser revendedor ou representante comercial deverá demonstrar de maneira clara a composição do preço constante de sua proposta, com descrição das parcelas relativas ao valor de aquisição do produto com notas fiscais de fábrica/indústria, encargos em geral, lucro e participação percentual de cada item em relação ao preço final *(planilha de custos)*.

21.5. **A critério do MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS, poderá ser exigido da contratada, listas de preços expedidas pelos fabricantes**, que conterão, obrigatoriamente, a data de início de sua vigência e numeração sequencial, para instrução de pedidos de revisão de preços.

21.6. Na análise do pedido de reequilíbrio, reajuste ou revisão, dentre outros critérios, o **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS** adotará, para verificação dos preços constantes dos demonstrativos que acompanhem o pedido, pesquisa de mercado dentre empresas de reconhecido porte mercantil, produtoras e /ou comercializadoras, a ser realizada pela própria unidade ou por instituto de pesquisa, utilizando-se, também, de índices setoriais ou outros adotados pelo Governo Estadual, devendo a deliberação de deferimento ou indeferimento da alteração solicitada ser instruída com justificativa da escolha do critério e memória dos respectivos cálculos, para decisão da Administração.

21.7. O percentual de diferença entre os preços de mercado vigentes à época do julgamento da licitação, devidamente apurado, e os propostos pela CONTRATADA/Detentora do registro de preços será mantido durante toda a vigência do registro. **O percentual não poderá ser alterado de forma a configurar reajuste econômico durante a vigência deste registro**.

21.8. A repactuação, reajuste ou revisão do preço, caso deferido, somente terá validade a partir da data da publicação da deliberação na Imprensa Oficial.

21.9. É vedado à contratada interromper o fornecimento ou a prestação do serviço enquanto aguarda o trâmite do processo de reequilíbrio, reajuste ou revisão de preços, estando, neste caso, sujeita às sanções previstas neste Edital.

21.10. A repactuação, reajuste ou revisão levará em consideração preponderantemente as normas legais federais e estaduais, que são soberanas à previsão do conteúdo exposto neste item.

22. DOS ESCLARECIMENTOS E DA IMPUGNAÇÃO DO ATO CONVOCATÓRIO

22.1. **Até o dia XX/XX/202X, 03 (três) dias úteis antes da data designada para a abertura da sessão pública, qualquer pessoa poderá IMPUGNAR** este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, mediante **petição**, que deverá obrigatoriamente (art. 10, caput, da Lei nº 12.527/2011) conter a identificação do Impugnante (CPF/CNPJ).

22.2. Os pedidos de **ESCLARECIMENTOS** referentes a este processo licitatório deverão ser enviados ao Pregoeiro, **até o dia XX/XX/202X, 3 (três) dias úteis anteriores à data designada para abertura da sessão pública**, até às 15h (horário de Brasília), exclusivamente por meio eletrônico via internet, no endereço indicado no Edital, mediante **petição**, que deverá obrigatoriamente (art. 10, caput, da Lei nº 12.527/2011) conter a identificação do Impugnante (CPF/CNPJ).

22.3. Os pedidos de impugnações e esclarecimentos, bem como as respectivas respostas, serão divulgados no site https://www.gov.br/compras/pt-br, na área Gestor Público/consultas/pregões/agendados (http://comprasnet.gov.br/acesso.asp?url=/livre/Pregao/lista_pregao_filtro.asp?Opc=0) e no **site oficial do MPAM**. O fornecedor, além do acesso livre, poderá visualizar também no menu principal, no link: "visualizar impugnações /esclarecimentos/avisos".

22.4. A impugnação ou pedido de esclarecimento poderá ser realizada por forma eletrônica, pelo e-mail licitacao@mpam.mp.br, no horário local de expediente da Instituição, até às 15 horas (horário de Brasília) da data limite fixada ou por petição dirigida/protocolada no Prédio-Sede desta PGJ, localizado na Av. Coronel Teixeira, nº 7995 - Nova Esperança, CEP: 69037-473, endereçado à Comissão Permanente de Licitação.

22.5. Acolhida a impugnação ou determinadas as providências requeridas, será designada nova data para realização da sessão pública, salvo quando estas não afetarem a formulação das propostas.

22.6. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

22.6.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos autos do processo de licitação.

22.7. As respostas aos pedidos de esclarecimentos divulgadas pelo sistema vincularão os participantes e a Administração.

23. DAS DISPOSIÇÕES FINAIS

23.1. A **COMISSÃO PERMANENTE DE LICITAÇÃO** prestará todos os esclarecimentos solicitados pelos interessados nesta licitação, estando disponível para atendimento de segunda a sexta-feira, das 9h às 15 horas (horário de Brasília), na Avenida Coronel Teixeira, n.º 7.995, Nova Esperança, Manaus – AM, pelo telefone (92) 3655-0743 ou, ainda, pelo e-mail: licitacao@mpam.mp.br.

23.2. A **Autoridade Competente** designará o pregoeiro que conduzirá esta licitação, necessariamente escolhido dentre os Pregoeiros Oficiais do **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**.

23.3. É facultada ao pregoeiro ou autoridade superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou complementar a instrução do processo.

23.3.1. O pregoeiro, durante as fases de julgamento das propostas e/ou habilitação, deve sanear eventuais erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível aos licitantes, sendo que a vedação à inclusão de novo documento, prevista no art. 64 da Nova Lei de Licitações (Lei 14.133/2021), não alcança documento ausente, comprobatório de condição atendida pelo licitante quando apresentou sua proposta, que não foi juntado com os demais comprovantes de habilitação e/ou da proposta, por equívoco ou falha, o qual deverá ser solicitado e avaliado pelo pregoeiro. (Acórdão TCU 1211/2021 - Plenário, relator Ministro Walton Alencar Rodrigues).

23.3.2. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento de que trata o subitem anterior, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, 24 (vinte e quatro) horas de antecedência, e a ocorrência será registrada em ata.

23.4. A **Autoridade Competente** para determinar a contratação poderá revogar a licitação por razões de interesse público derivado de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo anulá-la por ilegalidade, de ofício ou por provocação de qualquer pessoa, mediante ato escrito e fundamentado.

23.4.1. No caso de revogação ou anulação do procedimento licitatório, ficará assegurada oportunidade de ampla e prévia manifestação dos interessados, na forma da Lei.

23.4.2. A anulação pode ser declarada a qualquer tempo.

23.4.3. As licitantes não terão direito a indenização em decorrência de anulação do procedimento licitatório, ressalvado o direito do FORNECEDOR de boa-fé de ser ressarcida pelos encargos que tiver suportado em eventual cumprimento da obrigação decorrente da execução do objeto deste certame.

23.5. Os proponentes assumem todos os custos de preparação e apresentação de sua proposta e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

23.6. **Após apresentação da proposta, não caberá desistência, salvo por motivo justo decorrente de fato superveniente e aceito pelo pregoeiro, sob pena de abertura de procedimento apuratório em face da conduta do licitante**.

23.7. Quando todos os licitantes forem inabilitados ou todas as propostas forem desclassificadas, o Pregoeiro poderá fixar aos licitantes o prazo de 3 (três) dias úteis para apresentar nova documentação ou nova proposta escoimada das causas que ensejaram a inabilitação ou desclassificação das empresas.

23.8. Em caso de licitante vencedor sediado fora da cidade de Manaus, cujo envio de documentos e demais solicitações ensejem utilização de serviços postais, será obrigatória a apresentação de cópia do comprovante de envio dos itens solicitados, como forma de confirmação do atendimento aos prazos previstos em cada subitem.

23.8.1. O comprovante poderá ser digitalizado e enviado para o e-mail: licitacao@mpam.mp.br.

23.8.2. O descumprimento dos prazos para envio dos documentos ou demais solicitações, sem apresentação de justificativa, ensejará a desclassificação da empresa licitante, sem prejuízo das sanções cabíveis.

23.8.3. Caso a autenticação do documento ou o próprio documento esteja em formato digital, com assinatura por certificado digital, padrão ICP-Brasil, ou ainda torne possível sua convalidação em sítio eletrônico de autoridade certificadora oficial e/ou cartório digital respectivo, a licitante está dispensada da obrigação do item anterior.

23.8.3.1. Os documentos eletrônicos produzidos com a utilização de processo de certificação disponibilizada pela ICP-Brasil, nos termos da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, serão recebidos e presumidos verdadeiros em

relação aos signatários, dispensando-se o envio de documentos originais e cópias autenticadas em papel.

23.9. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no horário e local aqui estabelecidos, desde que não haja comunicação do Pregoeiro em contrário.

23.10. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente normal no **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**.

23.11. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível a verificação de suas condições de habilitação e a exata compreensão da sua proposta, durante a realização da sessão pública de pregão.

23.12. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

23.13. Será divulgada ata da sessão pública no sistema eletrônico.

23.14. Nenhuma pessoa física ou jurídica ainda que credenciada poderá representar mais de uma empresa concorrente, sob pena de não participação das empresas representadas.

23.15. A homologação do resultado desta licitação não implicará direito à contratação.

23.16. Em substituição aos respectivos originais todos os documentos poderão ser apresentados em cópia autenticada por Cartório competente ou conferida com o original por servidor da CPL. **Neste último caso, a autenticação administrativa poderá ser feita, preferencialmente, até o dia anterior à data prevista para o recebimento dos envelopes da Proposta e da Documentação**;

23.17. Somente serão aceitos propostas e lances encaminhados pelo sistema eletrônico.

23.18. É de inteira responsabilidade do licitante o acompanhamento do processo referente a este pregão eletrônico, no endereço eletrônico https://www.gov.br/compras/pt-br.

23.19. Para as demais condições de contratação, observar-se-ão as disposições constantes dos Anexos deste Edital.

23.20. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

23.21. Este Edital e seus Anexos poderão ser examinados sem ônus para o interessado, antes da realização da licitação, no formato eletrônico, através de consulta aos sítios https://www.gov.br/compras/pt-br e www.mpam.mp.br, ou através do correio eletrônico da CPL, licitacao@mpam.mp.br.

23.20.1. O Edital e seus anexos também estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico https://www.gov.br/pncp/pt-br.

23.20.1. Poderão ser, também, adquiridos impressos mediante depósito da quantia referente ao custo reprográfico, calculado no produto de R$ 0,50 (cinquenta centavos) por página, depositado na Conta-Corrente n.º 13200-4, Agência 6019-4, do Banco Bradesco S/A (237), em nome do **FUNDO DE APOIO DO MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**.

23.22. Os casos omissos serão resolvidos pelo Pregoeiro, com base no Ato PGJ n.º 008/2024 e na Lei n.º 14.133/21 e alterações.

23.23. As questões decorrentes da execução deste Instrumento, que não possam ser dirimidas administrativamente, serão processadas e julgadas no foro da cidade de Manaus, com exclusão expressa de qualquer outro.

Manaus, XX de XXXXXXXXXX de 202X.

Sarah Madalena B. Côrtes de Melo

Presidente da Comissão Permanente de Licitação
Ato PGJ n.º 165/2025 - DOMPE, Ed. 3121, de 15.07.2025

ANEXO I - DO EDITAL

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

TERMO DE REFERÊNCIA Nº 28.2025.DTIC.2002143.2025.007562

ANEXO II - DO EDITAL

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MINUTA DE CONTRATO ADMINISTRATIVO Nº 69.2025.DCCON - CONTRATOS.2033432.2025.007562

ANEXO III - DO EDITAL

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS

Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MODELO DE DECLARAÇÕES COMPLEMENTARES

Declaro, sob as penas da Lei, para os devidos fins junto à Comissão Permanente deLicitação que:

a) Cumpro plenamente os requisitos de habilitação, ciente de que responde pela veracidade das informações prestadas, na forma da lei;

b) Em atenção item 5.6. e art. 14.º e seus incisos da Lei n.º 14.133/2021, não estou impedido de participar direta ou indiretamente desta licitação, e ainda, não possuo sócios, diretores ou gerentes, que sejam cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do Ministério Público do Estado do Amazonas e de sua CPL;

c) Recebeu o edital e todos os documentos que o integram, dispondo de todos os elementos e informações necessários à elaboração da proposta de preços com total e completo conhecimento do objeto da licitação;

d) Os documentos e declarações apresentados são fiéis e verdadeiros;

e) Caso seja vencedor do certame e não cadastrado no SISTEMA DE ADMINISTRAÇÃO FINANCEIRA E CONTABILIDADE da SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ-AM, encaminhará a CONTRATANTE os documentos necessários para efetuar o referido cadastramento no prazo de 05 (cinco) dias úteis, a contar da adjudicação, sob pena de perder o direito de preferência à contratação em favor dos demais licitantes subsequentes, sem prejuízo da possibilidade de responder a procedimento administrativo de responsabilização (PAR) por eventual retardamento da licitação;

f) O preço inclui além do lucro, todos os custos e despesas, com tributos incidentes e encargos devidos, materiais, serviços, transporte, a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas, bem como quaisquer outras despesas diretas e indiretas incidentes na prestação de serviços;

g) Que apresentará, quando da contratação, documento que indique o pessoal técnico operacional, das instalações e do aparelhamento adequado e disponíveis para a realização do objeto da licitação, bem como a qualificação de cada membro da equipe técnica que se responsabilizará pelos trabalhos.

h) Que a licitante se submete e concorda com todos os termos do presente Edital, elementos e especificações nele contidos e que os cumprirá fielmente, inclusive, que se submete à fiscalização e ao controle técnico a ser efetuado por profissional técnico expressamente designado para tal.

i) A proposta apresentada para participar do presente Pregão foi elaborada de maneira independente por esta licitante e o seu conteúdo não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer outro participante potencial ou de fato, por qualquer meio ou por qualquer pessoa.

Local e data:

(assinatura)
(nome do representante legal pela empresa)

(CPF do representante legal)

ANEXO IV - DO EDITAL

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS

Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MODELO DE PROPOSTA DE PREÇOS

Proposta que faz a empresa _____, inscrita no CNPJ (MF) n.º _____, localizada _____, na cidade de _____, CEP _____, fone _____, e-mail _____, para o fornecimento dos bens abaixo relacionados, de acordo com todas as especificações e condições estabelecidas no **Pregão Eletrônico n.º 94.0XX/202X-CPL/MP/PGJ-SRP**, promovido pelo **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS / PROCURADORIA-GERAL DE JUSTIÇA**:

Item	Descrição	Marca / Modelo / Tipo / Referência	Qtd. (A)	Valor Unitário R$ (B)	Valor Total R$ (C=A*B)
01	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9	NUTANIX	4		
02	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU	NUTANIX	1		
03	SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX	NUTANIX	5		
04	SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU	NUTANIX	1		
05	LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE	NUTANIX	50		
...	...	...			
VALOR TOTAL DA PROPOSTA					**R$**

A _____(*nome da empresa)*_____ declara que concorda com todas as especificações do Edital.

a. **Prazo de validade da proposta: _____** (não será inferior a 90 (noventa) dias, a contar da data de sua apresentação).

b. **Prazo de entrega da solução: _____** (até 60 (sesenta) dias corridos, conforme dipõe o Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562;

c. **Modo de Transporte dos Produtos:**

( ) rodoviário/terrestre

( ) aéreo: ( ) normal ( ) expresso

( ) outros. Especificar:_____

d. **Prazo de garantia e assistência técnica**: _____ (mínimo 60 (sessenta) meses, conforme dipõe o Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562;

e. ***Site* e/ou e-mail do fabricante, se houver**: _____

f. **Dados Bancários**: (*indicar o nome e número do banco, nome e número completo da agência e número da conta corrente*);

g. **Contato para fins de faturamento:** *(indicar o nome, cargo, endereço, telefone, e-mail de contato do responsável pelo recebimento das futuras notas de empenho);*

h. **Contato para fins de faturamento:** *(indicar o nome, cargo, endereço, telefone, e-mail de contato do responsável pelo recebimento das futuras notas de empenho)*

Nome: _____

CNPJ ou CPF: _____

DECLARAÇÕES:

Declaro, sob as penas da Lei, para os devidos fins junto à Comissão Permanente de Licitação que:

a) Cumpre plenamente os requisitos de habilitação, ciente de que responde pela veracidade das informações prestadas, na forma da lei;

b) Em atenção item 5.6. e art. 14.º e seus incisos da Lei n.º 14.133/2021, não está impedida de participar direta ou indiretamente desta licitação, e ainda, que não possue sócios, diretores ou gerentes, que sejam cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do Ministério Público do Estado do Amazonas e de sua CPL;

c) Recebeu o edital e todos os documentos que o integram, dispondo de todos os elementos e informações necessários à elaboração da proposta de preços com total e completo conhecimento do objeto da licitação;

d) Os documentos e declarações apresentados são fiéis e verdadeiros;

e) Caso seja vencedor do certame e não cadastrado no SISTEMA DE ADMINISTRAÇÃO FINANCEIRA E CONTABILIDADE da SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ-AM, encaminhará a CONTRATANTE os documentos necessários para efetuar o referido cadastramento no prazo de 05 (cinco) dias úteis, a contar da adjudicação, sob pena de perder o direito de preferência à contratação em favor dos demais licitantes subsequentes, sem prejuízo da possibilidade de responder a procedimento administrativo de responsabilização (PAR) por eventual retardamento da licitação;

f) O preço inclui além do lucro, todos os custos e despesas, com tributos incidentes e encargos devidos, materiais, serviços, transporte, a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas, bem como quaisquer outras despesas diretas e indiretas incidentes na prestação de serviços;

g) Que apresentará, quando da contratação, documento que indique o pessoal técnico operacional, das instalações e do aparelhamento adequado e disponíveis para a realização do objeto da licitação, bem como a qualificação de cada membro da equipe técnica que se responsabilizará pelos trabalhos.

h) Que a licitante se submete e concorda com todos os termos do presente Edital, elementos e especificações nele contidos e que os cumprirá fielmente, inclusive, que se submete à fiscalização e ao controle técnico a ser efetuado por profissional técnico expressamente designado para tal.

i) A proposta apresentada para participar do presente Pregão foi elaborada de maneira independente por esta licitante e o seu conteúdo não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer outro participante potencial ou de fato, por qualquer meio ou por qualquer pessoa.

Local e data:

(assinatura)
(nome do representante legal pela empresa)
(CPF do representante legal)

Observação: A apresentação da proposta implicará a plena aceitação, por parte do licitante, das condições estabelecidas neste edital e seus anexos, bem como, todas as especificações do objeto contidas na proposta vinculam a Contratada.

ANEXO V - DO EDITAL

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS

Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MODELO DE SOLICITAÇÃO DE CADASTRAMENTO – SEFAZ/AM

À DIRETORIA DE ORÇAMENTO E FINANÇAS

Procuradoria-Geral de Justiça do Estado do Amazonas
Avenida Coronel Teixeira, 7995, Nova Esperança
CEP: 69037-473 – Manaus / AM

A empresa (informar a razão social, CNPJ e endereço) solicita a esse Setor o seu cadastro no SISTEMA DE ADMINISTRAÇÃO FINANCEIRA E CONTABILIDADE, dessa S ECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ.

Assim sendo, acompanha esta carta de solicitação de cadastramento a documentação abaixo listada, exigida para a efetivação do registro:

a) Comprovante de inscrição e de situação cadastral emitido pela Receita Federal do Brasil;

b) Cópia legível do comprovante (por ex: extrato, cópia reprográfica de cartão bancário, etc.) dos seguintes dados bancários:

Banco: _____

Agência: _____

Conta: _____

Local e data:

(assinatura)
(nome do representante legal pela empresa)
(CPF do representante legal)

ANEXO VI - DO EDITAL

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS

Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MODELO - CREDENCIAMENTO PARA VISTORIA TÉCNICA

Pelo presente instrumento credenciamos o(a) Sr.(a) ...., portador do documento de Identidade n.º ....., o(a) qual está habilitado a proceder à vistoria técnica e assinar o Atestado de Vistoria em nome da empresa ..... CNPJ ..... prevista no ITEM 3.1 do Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562, referente ao procedimento licitatório PE 94.0XX/2026.

Local e data:

(assinatura)
(nome do representante legal pela empresa)
(CPF do representante legal)

ANEXO VII - DO EDITAL

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS

Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MODELO - ATESTADO DE VISTORIA TÉCNICA

Atestamos, para cumprimento do item 5.12 do Edital referente ao procedimento licitatório PE 94.0XX/2026, que a empresa ....., inscrita no CNPJ ....., representada neste ato por seu representante credenciado, o(a) Sr.(a) ....., portador(a) do documento de identidade profissional nº ....., compareceu ao local onde será executado o serviço/solução, conforme previsto no Item 3.1. do Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562 e, acompanhado por representante deste Ministério Público do Estado do Amazonas / Procuradoria-Geral de Justiça, tomou conhecimento *in loco* dos locais e instalações, tendo pleno conhecimento das especificações e condições locais para cumprimento das obrigações decorrentes do objeto da licitação em questão.

Manaus, AM, de de 202X.

Representante(a) designado(a) pela empresa licitante

De acordo

Representante da PGJ-AM

ANEXO VIII - DO EDITAL

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS

Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MODELO DE DE DISPENSA DE VISTORIA TÉCNICA

Declaro(amos), para cumprimento do Item 5.12 do Edital referente ao procedimento licitatório ....., que a empresa ....., representada pelo, o(a) Sr.(a) ....., portador(a) do documento de identidade nº ....., optou por não vistoriar o local dos serviços conforme previsto no Subitem 3.1. do Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562.

Declaro, ainda, que quaisquer alegações de desconhecimento ou erro orçamentário por parte da futura contratada, para a execução dos serviços propostos não serão considerados nem usados como possível juízo de valor afim de compensações futuras.

Local e data:

(assinatura)
(nome do representante legal pela empresa)
(CPF do representante legal)

Documento assinado eletronicamente por **Sarah Madalena Barbosa Santos Cortes**, **Presidente da Comissão Permanente de Licitação - CPL**, em 23/12/2025, às 16:26, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2031551** e o código CRC **7A952FEC**.

DESPACHO Nº 89.2025.CPL.2037097.2025.007562

Processo SEI N.º 2025.007562

Objeto: Contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma **solução de datacenter,** contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses.

Trata-se dos autos do procedimento interno em epígrafe, versando sobre o objeto de referência, instruído por solicitação formalizada pelo senhor **EUDO DE LIMA ASSIS JUNIOR, Diretor de Tecnologia da Informação e Comunicação – DTIC,** que apresentou o detalhamento do objeto, inicialmente, por intermédio do ESTUDO TÉCNICO PRELIMINAR - ETP Nº 7.2025.DTIC.1591885.2025.007562 e Termo de Referência Nº 9.2025.DTIC.1605182.2025.007562.

Os artefatos da contratação foram devidamente analisados pela Assessoria Jurídica, oportunidade na qual foram determinadas algumas adequações nos documentos, nos termos do Despacho Nº 605.2025.01AJ-SUBADM.1673215.2025.007562, lavrado pelo Exmo. Sr. Dr. ANDRÉ VIRGÍLIO BELOTA SEFFAIR, *Subprocurador-Geral de Justiça para Assuntos Administrativo*, em 15/07/2025.

Dando prosseguimento ao feito, a **DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – DTIC** encaminhou novo **Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562**, datado de 14/11/2025, sendo aprovado pelo Exmo. Sr. Dr. ANDRÉ VIRGÍLIO BELOTA SEFFAIR, *Subprocurador-Geral de Justiça para Assuntos Administrativo*, nos termos do Despacho Nº 1123.2025.01AJ-SUBADM.2013504.2025.007562, datado de 24/11/2025.

Por sua vez, o **SETOR DE COMPRAS E SERVIÇOS – SCOMS,** em 05/12/2025, emitiu o **Quadro-Resumo do Processo de Compra N.º 547.2025.SCOMS.2023741.2025.007562**.

Na sequência, a **DIRETORIA DE ORÇAMENTOS E FINANÇAS - DOF** carreou aos autos, em 11/12/2025, a correspondente **NOTA DE AUTORIZAÇÃO DE DESPESAS / ADJUDICAÇÃO -NAD Nº 512.2025.DOF - ORÇAMENTO.2028015.2025.007562.**

Vindo os autos a esta Comissão, em 16/12/2025, procedeu-se, de pronto, diligência junto à **Divisão de Contratos e Convênios - DCCON**, através do Ofício Nº 479.2025.CPL.2031552.2025.007562, "para análise quanto à necessidade de elaboração de minuta de termo contratual ou instrumento equivalente, especialmente em face do teor do Termo de Referência nº 28.2025.DTIC.2002143.2025.007562**."**

Por seu turno, a **DIVISÃO DE CONTRATOS E CONVÊNIOS - D C C O N** emitiu, em 17/12/2025, elaborou a **MINUTA DE CONTRATO ADMINISTRATIVO Nº 68.2025.DCCON. No entanto,** após uma análise mais detalhada dos autos, a Divisão de Contratos e Convênios (DCCON) remete uma nova minuta a **MINUTA DE CONTRATO ADMINISTRATIVO Nº 69.2025.DCCON - CONTRATOS.2033432.2025.007562,** visando à inclusão da **Cláusula Décima Quarta - Da Garantia Contratual**.

Logo, esta CPL, considerando as nuances do caso, bem como a necessidade de assegurar a boa contratação e prover-se dos instrumentos necessários para seleção da melhor proposta à Administração, confeccionou a **MINUTA DE EDITAL DE PREGÃO ELETRÔNICO Nº 79.2025.CPL.2031551.2025.007562,** em conformidade com o Ato PGJ n.º 8/2024 e com a Lei n.º 14.133/2021.

Pelo exposto, encaminhem-se os autos do Processo SEI em epígrafe à **SUBPROCURADORIA GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS** do **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**, a fim de cumprir o disposto no art. 53 da Lei n.º 14.133/2021 e art. 37, *caput,* da Constituição Federal, quanto à emissão do parecer jurídico e posterior aprovação pelo Ordenador de Despesas dos seguintes documentos/minutas:

a) Minuta de Edital de Pregão Eletrônico Nº 79.2025.CPL.2031551.2025.007562; es

b) Minuta de Contrato Administrativo Nº 69.2025.DCCON - CONTRATOS.2033432.2025.007562.

Manaus, *na data da assinatura eletrônica.s*

Sarah Madalena B. Côrtes de Melo

Presidente da Comissão Permanente de Licitação
Ato PGJ n.º 165/2025 - DOMPE, Ed. 3121, de 15.07.2025

Documento assinado eletronicamente por **Sarah Madalena Barbosa Santos Cortes**, **Presidente da Comissão Permanente de Licitação - CPL**, em 23/12/2025, às 16:25, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2037097** e o código CRC **CBA9B6EA**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

PARECER Nº 201.2025.01AJ-SUBADM.2037607.2025.007562

PROCESSO N.º: 2025.007562

ASSUNTO: *Contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses.*

EMENTA: ADMINISTRATIVO - PARECER OBRIGATÓRIO - ARTIGO 53 DA LEI N° 14.133/2021 E ARTIGO 37, *CAPUT* , DA CRFB/88 - **ANÁLISE JURÍDICA DE TERMO DE REFERÊNCIA; MINUTA DE EDITAL DE PREGÃO ELETRÔNICO; E MINUTA DE CONTRATO** - REQUISITOS LEGAIS OBSERVADOS - ELEMENTOS FORMAIS E MATERIAIS OBRIGATÓRIOS PRESENTES - **PARECER PELA APROVAÇÃO.**

I. RELATÓRIO

Trata-se dos autos do procedimento interno em epígrafe, versando sobre o objeto de referência, instruído por solicitação formalizada pelo senhor **EUDO DE LIMA ASSIS JUNIOR, Diretor de Tecnologia da Informação e Comunicação – DTIC,** que apresentou o detalhamento do objeto, inicialmente, por intermédio do ESTUDO TÉCNICO PRELIMINAR - ETP Nº 7.2025.DTIC.1591885.2025.007562 e Termo de Referência Nº 9.2025.DTIC.1605182.2025.007562.

Os artefatos da contratação foram devidamente analisados pela Assessoria Jurídica, oportunidade na qual foram determinadas algumas adequações nos documentos, nos termos do Despacho Nº 605.2025.01AJ-SUBADM.1673215.2025.007562, lavrado pelo Exmo. Sr. Dr. ANDRÉ VIRGÍLIO BELOTA SEFFAIR, *Subprocurador-Geral de Justiça para Assuntos Administrativo*.

Dando prosseguimento ao feito, a **DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – DTIC** encaminhou novo **Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562**, sendo aprovado pelo Exmo. Sr. Dr. ANDRÉ VIRGÍLIO BELOTA SEFFAIR, *Subprocurador-Geral de Justiça para Assuntos Administrativo*, nos termos do Despacho Nº 1123.2025.01AJ-SUBADM.2013504.2025.007562.

Por sua vez, o **SETOR DE COMPRAS E SERVIÇOS – SCOMS** emitiu o **Quadro-Resumo do Processo de Compra N.º 547.2025.SCOMS.2023741.2025.007562**.

Na sequência, a **DIRETORIA DE ORÇAMENTOS E FINANÇAS - DOF** carreou aos autos a correspondente **NOTA DE AUTORIZAÇÃO DE DESPESAS / ADJUDICAÇÃO -NAD Nº 512.2025.DOF - ORÇAMENTO.2028015.2025.007562.**

Encaminhados os autos à Comissão Permanente de Licitação (CPL) diligência junto à **Divisão de Contratos e Convênios - DCCON**, através do Ofício Nº 479.2025.CPL.2031552.2025.007562, "para análise quanto à necessidade de elaboração de minuta de termo contratual ou instrumento equivalente, especialmente em face do teor do Termo de Referência nº 28.2025.DTIC.2002143.2025.007562**."**

Por seu turno, a **DIVISÃO DE CONTRATOS E CONVÊNIOS - DCCON** elaborou a **MINUTA DE CONTRATO ADMINISTRATIVO Nº 68.2025.DCCON. No entanto,** após uma análise mais detalhada dos autos, a Divisão de Contratos e Convênios (DCCON) remete uma nova minuta a **MINUTA DE CONTRATO ADMINISTRATIVO Nº 69.2025.DCCON - CONTRATOS.2033432.2025.007562,** visando à inclusão da **Cláusula Décima Quarta - Da Garantia Contratual**.

Assim, a Comissão Permanente de Licitação, através do **Despacho Nº 89.2025.CPL (2037097)**, realizou a juntada da **Minuta de Edital 79 (2031551)**, cujo objeto é a *contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses.*

Dessa forma vieram os autos para manifestação desta Assessoria Jurídica.

II. DA FUNDAMENTAÇÃO

Da Licitação como Mandamento Constitucional

Inicialmente, é essencial destacar que, como regra geral, a aquisição de bens e serviços pela Administração Pública exige a realização de um prévio procedimento licitatório. Essa obrigatoriedade decorre expressamente do artigo 37, inciso XXI, da Constituição Federal e implicitamente dos princípios da isonomia, impessoalidade e moralidade administrativa. Vejamos:

> **Art. 37. A administração pública direta e indireta** de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios **obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte**:
>
> **XXI - ressalvados os casos especificados na legislação**, as obras, serviços, **c o m p r a s** e alienações **serão contratados mediante processo de licitação pública que assegure igualdade de condições a todos os concorrentes**, com cláusulas que estabeleçam obrigações de pagamento, mantidas as condições efetivas da proposta, nos termos da lei, o qual somente permitirá as exigências de qualificação técnica e econômica indispensáveis à garantia do cumprimento das obrigações. (*grifo*)

Sobre o tema, Marçal Justen Filho[1] traz uma interpretação relevante ao analisar a obrigatoriedade da licitação e a possibilidade de contratação direta:

> A Constituição acolheu a presunção de que **prévia licitação produz a melhor contratação – entendida como aquela que assegura a maior vantagem possível à Administração Pública, com observância do princípio da isonomia**. Mas a própria Constituição se encarregou de limitar tal presunção, facultando contratação direta (sem licitação) nos casos previstos por lei. (*grifo*)

Complementando essa análise, Celso Antônio Bandeira de Mello[2] define licitação como:

> um certame que as entidades governamentais devem promover e no qual abrem disputa entre os interessados em com elas travar determinadas relações de conteúdo patrimonial, para escolher a proposta mais vantajosa às conveniências públicas. Estriba-se na ideia de competição, a ser travada isonomicamente entre os que preencham os atributos e aptidões necessários ao bom cumprimento das obrigações que se propõem assumir. (MELLO, Celso Antônio Bandeira de. Curso de Direito Administrativo. São Paulo: Malheiros, 2009)

Princípios Norteadores da Licitação e da Administração Pública

O procedimento licitatório não apenas assegura igualdade de condições entre os concorrentes, mas também busca selecionar a proposta mais vantajosa para a Administração e promover o desenvolvimento nacional sustentável, conforme o artigo 5º da **Lei nº 14.133/2021**:

> **Art. 5º** Na aplicação desta Lei, **serão observados os princípios da legalidade, da impessoalidade, da moralidade, da publicidade, da eficiência, do interesse público, da probidade administrativa, da**

> **igualdade, do planejamento, da transparência, da eficácia, da segregação de funções, da motivação, da vinculação ao edital, do julgamento objetivo, da segurança jurídica, da razoabilidade, da competitividade, da proporcionalidade, da celeridade, da economicidade e do desenvolvimento nacional sustentável**, assim como as disposições do Decreto-Lei nº 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro). (*grifo*)

Dentre esses princípios, destaca-se o princípio da **legalidade**, amplamente abordado por Hely Lopes Meirelles[3] :

> a legalidade, como princípio de administração, significa que o administrador público está, em toda sua atividade funcional, sujeito aos mandamentos da lei, e às exigências do bem comum, e deles não se pode afastar ou desviar, sob pena de praticar ato inválido e expor-se à responsabilidade disciplinar, civil e criminal, conforme o caso.

Além disso, o princípio da **impessoalidade** impõe ao administrador o dever de agir com finalidade pública, sem promover favorecimentos indevidos. Segundo Meirelles[4] :

> O princípio da impessoalidade referido na Constituição Federal nada mais é que o clássico princípio da finalidade, o qual impõe ao administrador que só pratique o ato para seu fim legal. E o fim legal é unicamente aquele que a norma de direito indica expressa ou virtualmente com objetivo do ato de forma impessoal.

Já o princípio da **moralidade administrativa** exige que tanto a Administração quanto os particulares que com ela interagem observem padrões éticos e de boa-fé. Como ensina Maria Sylvia Zanella Di Pietro (2015)[5]: “o princípio deve ser observado não apenas pelo administrador, mais também pelo particular que se relaciona com administração pública”.

Justificativa do Procedimento Licitatório

A realização da presente licitação, na modalidade de **registro de preços**, justifica-se pela necessidade de garantir isonomia, transparência e obtenção da proposta mais vantajosa para a Administração Pública, em conformidade com os princípios regentes da Lei nº 14.133/2021. Do contexto dos artefatos de planejamento, a unidade de planejamento, indentificou a necessidade de aquisição de móveis, com garantia mínima de 60 (sessenta) meses, a serem disponibilizados pelo Setor de Patrimônio e Material-SPAT, objetivando atender às demandas dos órgãos integrantes do Ministério Público do Estado do Amazonas.

Do Planejamento da Contratação

A **Lei nº 14.133/2021** estabelece que a **fase preparatória do processo licitatório** deve ser caracterizada pelo planejamento, garantindo sua compatibilidade com o **Plano de Contratações Anual**, conforme disposto no **inciso VII do caput do art. 12**, e com as **leis orçamentárias**. Além disso, essa fase deve abranger todas as **considerações técnicas, mercadológicas e de gestão** que possam impactar a contratação, conforme prevê o **caput do art. 18**.

O **art. 18 da Lei nº 14.133/2021** detalha as providências e os documentos que devem compor a fase de planejamento, conforme transcrito a seguir:

> Art. 18. A fase preparatória do processo licitatório é caracterizada pelo planejamento e deve compatibilizar-se com o **plano de contratações anual d**e que trata o inciso VII do **caput** do art. 12 desta Lei, sempre que elaborado, e com as **leis orçamentárias**, bem como abordar todas as **considerações técnicas, mercadológicas e de gestão** que podem interferir na contratação, compreendidos:
>
> I - a descrição da necessidade da contratação fundamentada em **estudo técnico preliminar** que caracterize o interesse público envolvido;
>
> II - a definição do objeto para o atendimento da necessidade, por meio de **termo de referência**, anteprojeto, projeto básico ou projeto executivo, conforme o caso;
>
> III - a definição das **condições de execução e pagamento, das garantias exigidas e ofertadas e das condições de recebimento**;
>
> IV - o **orçamento estimado**, com as composições dos preços utilizados para sua formação;
>
> V - a elaboração do **edital** de licitação;
>
> VI - a elaboração de **minuta de contrato**, quando necessária, que constará obrigatoriamente como anexo do edital de licitação;
>
> VII - o **regime de fornecimento de bens**, de prestação de serviços ou de execução de obras e serviços de engenharia, observados os potenciais de economia de escala;
>
> VIII - a **modalidade** de licitação, o **critério de julgamento**, o **modo de disputa** e a adequação e eficiência da forma de combinação desses parâmetros, para os fins de seleção da proposta apta a gerar o resultado de contratação mais vantajoso para a Administração Pública, considerado todo o **ciclo de vida do objeto**;
>
> IX - a **motivação circunstanciada das condições do edital, tais como justificativa de exigências de qualificação técnica, mediante indicação das parcelas de maior relevância técnica ou valor significativo do objeto, e de qualificação econômico-financeira, justificativa dos critérios de pontuação e julgamento das propostas técnicas, nas licitações com julgamento por melhor técnica**

> **ou técnica e preço, e justificativa das regras pertinentes à participação de empresas em consórcio**;
>
> X - a **análise dos riscos** que possam comprometer o sucesso da licitação e a boa execução contratual;
>
> XI - a motivação sobre o **momento da divulgação do orçamento da licitação**, observado o art. 24 desta Lei. (*grifo*)

Nos termos do **§1º do Art. 18**, que dispõe sobre os **elementos do Estudo Técnico Preliminar (ETP),** o planejamento da contratação exige uma análise detalhada da **necessidade administrativa**, permitindo compreender os fundamentos que justificam a requisição.

Com o advento da Lei nº 14.133/2021, o planejamento foi alçado à condição de um dos princípios fundamentais das contratações públicas. Nas palavras de Felipe Dalenogare Alves e Marilene Carneiro Matos (2025)[6]

> A Lei n. 14.133/2021 preocupou-se com o princípio do planejamento aplicado às contratações públicas. Para tanto, instituiu inúmeras ferramentas que devem ser elaboradas na fase preparatória da licitação, inerentes não só ao procedimento de licitação, mas à fase contratual.
>
> Dentre eles, merecem destaque o Plano de Contratações Anual – PCA, que deve consolidar as demandas ordinárias da Administração, a fim de que possa realizar as contratações de modo planejado, atendendo-se as suas necessidades sem sustos e improvisos, o Estudo Técnico Preliminar, que deve verificar a melhor alternativa a atender o interesse público à futura contratação, e o mapa de riscos, o qual deve evidenciar os riscos relacionados à licitação e à gestão contratual.

De igual modo, Matheus Carvalho, João Paulo Oliveira e Paulo Germano Rocha (2024)[7], ao abordarem o instituto, firmaram o seguinte entendimento:

> O estudo técnico preliminar - ETP, regulamentado minuciosamente no parágrafo primeiro, representa verdadeira concretização do princípio do planejamento nas licitações. Nesse sentido, o princípio do planejamento **não é meramente uma norma de conteúdo aberto,** tendo sido dotado de um asernal de normas-regra que o tornam efetivo na seara das contratações públicas, e não uma norma de finalidade hermenêutica.

Uma vez identificada a necessidade subjacente ao pedido inicial, deve-se buscar no mercado **as soluções disponíveis**, as quais podem diferir do que foi inicialmente demandado. Após a identificação da melhor alternativa — caso haja mais de uma viável —, inicia-se a etapa de **análise e detalhamento técnico**, com o objetivo de definir o **objeto licitatório e suas especificações**.

De modo geral, a **instrução do processo licitatório** deve refletir esse **encadeamento lógico**, garantindo que cada etapa seja devidamente fundamentada e estruturada para assegurar eficiência, economicidade e alinhamento aos princípios da administração pública.

Da Análise da Assessoria Jurídica

No que se refere ao **papel da Assessoria Jurídica** na **Lei nº 14.133/2021**, o referido diploma legal apresenta **novos contornos** quanto às **competências do órgão consultivo jurídico**, conforme se observa a seguir:

> **Art. 53. Ao final da fase preparatória, o processo licitatório seguirá para o órgão de assessoramento jurídico da Administração, que realizará controle prévio de legalidade mediante análise jurídica da contratação**.
>
> **§ 1º Na elaboração do parecer jurídico, o órgão de assessoramento jurídico da Administração deverá:**
>
> **I - apreciar o processo licitatório conforme critérios objetivos prévios de atribuição de prioridade;**
>
> **II - redigir sua manifestação em linguagem simples e compreensível e de forma clara e objetiva, com apreciação de todos os elementos indispensáveis à contratação e com exposição dos pressupostos de fato e de direito levados em consideração na análise jurídica;**
>
> III - (VETADO).
>
> § 2º (VETADO).
>
> § 3º Encerrada a instrução do processo sob os aspectos técnico e jurídico, a autoridade determinará a divulgação do edital de licitação conforme disposto no art. 54.
>
> § 4º Na forma deste artigo, o órgão de assessoramento jurídico da Administração também realizará controle prévio de legalidade de contratações diretas, acordos, termos de cooperação, convênios, ajustes, adesões a atas de registro de preços, outros instrumentos congêneres e de seus termos aditivos.
>
> § 5º É dispensável a análise jurídica nas hipóteses previamente definidas em ato da autoridade jurídica máxima competente, que deverá considerar o baixo valor, a baixa complexidade da contratação, a entrega imediata do bem ou a utilização de minutas de editais e instrumentos de contrato, convênio ou outros ajustes previamente padronizados pelo órgão de assessoramento jurídico.
>
> § 6º (VETADO). (*grifo*)

Assim, conforme previsto na **Lei nº 14.133/2021**, ao término da **fase preparatória**, o processo deve ser encaminhado à **Assessoria Jurídica**, que realizará o **controle prévio de legalidade da contratação**. Essa análise envolve a verificação dos aspectos jurídicos de todos os artefatos, com base em **critérios objetivos**, utilizando **linguagem clara e acessível**, e fundamentando sua

manifestação nos **pressupostos fáticos e de direito**.

Somente após a conclusão das análises **técnica e jurídica**, a autoridade competente poderá determinar a **divulgação do edital**, conforme estabelece o **§ 3º do artigo 18 da Lei nº 14.133/2021**.

Do Estudo Técnico Preliminar

O **Estudo Técnico Preliminar (ETP)** deve conter, de forma fundamentada, a **descrição da necessidade da contratação**, com especial atenção à **demonstração do interesse público envolvido**. Além disso, é essencial que sejam abordadas as **considerações técnicas, mercadológicas e de gestão**, as quais podem impactar a contratação e influenciar a tomada de decisão.

O **art. 18, § 1º, da Lei nº 14.133/2021** estabelece os **elementos essenciais** que devem ser considerados na elaboração do **ETP**, conforme apresentado a seguir:

> § 1º O estudo técnico preliminar a que se refere o inciso I do **caput** deste artigo deverá evidenciar o problema a ser resolvido e a sua melhor solução, de modo a permitir a avaliação da viabilidade técnica e econômica da contratação, e conterá os seguintes elementos:
>
> I - **descrição da necessidade da contratação**, considerado o problema a ser resolvido sob a perspectiva do interesse público;
>
> II - demonstração da previsão da contratação no plano de contratações anual, sempre que elaborado, de modo a indicar o seu alinhamento com o planejamento da Administração;
>
> III - requisitos da contratação;
>
> IV - **estimativas das quantidades para a contratação**, acompanhadas das memórias de cálculo e dos documentos que lhes dão suporte, que considerem interdependências com outras contratações, de modo a possibilitar economia de escala;
>
> V - levantamento de mercado, que consiste na análise das alternativas possíveis, e justificativa técnica e econômica da escolha do tipo de solução a contratar;
>
> VI - **estimativa do valor da contratação**, acompanhada dos preços unitários referenciais, das memórias de cálculo e dos documentos que lhe dão suporte, que poderão constar de anexo classificado, se a Administração optar por preservar o seu sigilo até a conclusão da licitação;
>
> VII - descrição da solução como um todo, inclusive das exigências relacionadas à manutenção e à assistência técnica, quando for o caso;
>
> VIII - **justificativas para o parcelamento ou não da contratação**;
>
> IX - demonstrativo dos resultados pretendidos em termos

> de economicidade e de melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis;
>
> X - providências a serem adotadas pela Administração previamente à celebração do contrato, inclusive quanto à capacitação de servidores ou de empregados para fiscalização e gestão contratual;
>
> XI - contratações correlatas e/ou interdependentes;
>
> XII - descrição de possíveis impactos ambientais e respectivas medidas mitigadoras, incluídos requisitos de baixo consumo de energia e de outros recursos, bem como logística reversa para desfazimento e reciclagem de bens e refugos, quando aplicável;
>
> XIII - **posicionamento conclusivo** sobre a adequação da contratação para o atendimento da necessidade a que se destina. (*grifo*)

Diante da análise do **Estudo Técnico Preliminar - ETP n.º 7.2025 (1591885)**, verifica-se que o documento contempla os elementos essenciais exigidos pelo **art. 18, § 1º, da Lei nº 14.133/2021**, especialmente aqueles de observância obrigatória, conforme dispõe o § 2º do mesmo artigo.

Dessa forma, conclui-se que o documento analisado está em conformidade com os requisitos mínimos previstos na legislação.

Do Termo de Referência

O artigo 6º da Lei nº 14.133/2021 trata do **Termo de Referência**, que é um dos documentos essenciais no processo licitatório para a contratação de bens e serviços. Assim, com base na análise do **Termo de Referência n.º 28.2025.DTIC (2002143)**, verifica-se se o documento atende aos **parâmetros e elementos descritivos exigidos pelo art. 6º, XXIII, da Lei nº 14.133/2021**.

Da Natureza do Objeto Licitado e da Modalidade de Licitação Escolhida

A Lei Federal nº 14.133/2021, instituiu o Pregão como modalidade de licitação obrigatória para aquisição de bens e serviços comuns, cujo critério de julgamento poderá ser o de **menor preço** ou o de **maior desconto**, conforme se verifica no art. 6°, inciso XLI, do referido diploma legal:

> Art. 6º Para os fins desta Lei, consideram-se:
>
> (...)
>
> XLI - pregão: modalidade de licitação obrigatória para aquisição de bens e serviços comuns, cujo critério de julgamento poderá ser o de menor preço ou o de maior desconto;

Assim, a partir da Nova Lei de Licitações, o Pregão passa a ser obrigatório para a contratação de todo e qualquer bem ou serviço comum, a partir de dois critérios de julgamento: (i) menor preço; ou (ii) maior desconto.

A definição de **bens e serviços comuns** está prevista no iniciso XIII do artigo 6º da Lei nº 14.133/2021: "*aqueles cujos padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado*", repetindo a definição dada pela Lei nº 10.520/2002, extinta Lei do Pregão.

Na realidade, a norma, ao restringir o âmbito de aplicação do Pregão, objetiva viabilizar a realização de um procedimento mais simples para aquisição de bens e serviços razoavelmente padronizados, possibilitando à Administração negociar o melhor preço, sem comprometer a viabilidade da proposta.

No caso em questão, o objeto do certame refere-se ao *Registro de preços para eventual aquisição de móveis, com garantia mínima de 60 (sessenta) meses, a serem disponibilizados pelo Setor de Patrimônio e Material-SPAT, a fim de garantir a manutenção da qualidade no atendimento às demandas do Ministério Público do Estado do Amazonas, por um período de 12 meses.*

Dessa forma, verifica-se que a solução em análise, **em regra, configura-se como bens comuns para fins de licitação**, uma vez que possui **natureza simples**, com **condições de execução claras e padronizáveis**. Assim, é permitida a **utilização do pregão como modalidade de licitação**, conforme disposto na **Lei nº 14.133/2021.**

Pelo exposto, em observância aos preceitos legais acima mencionados, caracteriza-se como adequada a modalidade selecionada para a realização de licitação, na modalidade **PREGÃO, na forma ELETRÔNICA, para REGISTRO DE PREÇOS, com critério de julgamento MENOR PREÇO GLOBAL**, com modo de disputa "**ABERTO"**, nos termos da Lei nº 14.133, de 2021, do Ato nº 008/2024/PGJ e demais legislações aplicáveis e, ainda, de acordo com as condições estabelecidas neste Edital.

Dos Atos Essenciais ao Pregão

O art. 29 da Lei n° 14.133/2021 dispõe que o pregão segue o rito procedimental comum previsto no art. 17 do referido diploma legal, *in verbis*:

> Art. 17. O processo de licitação observará as seguintes fases, em sequência:
>
> I - preparatória;
>
> II - de divulgação do edital de licitação;
>
> III - de apresentação de propostas e lances, quando for o caso;
>
> IV - de julgamento;
>
> V - de habilitação;
>
> VI - recursal;
>
> VII - de homologação.

Em especial, no que se refere à **fase preparatória**, que é o objeto de análise neste momento processual, o **art. 18 da Lei nº 14.133/2021** estabelece um conjunto de providências e documentos que devem necessariamente instruir o planejamento da contratação, conforme se demonstrará a seguir.

Da Minuta de Edital

Consoante se disse alhures, na lição de Ronny Charles Lopes de Torres (2018)[8], o certame licitatório é um procedimento prévio de seleção por meio do qual a Administração, mediante critérios previamente estabelecidos, isonômicos, abertos ao público e fomentadores da competitividade, busca escolher a melhor alternativa para a celebração de um contrato.

Desta feita, conforme leciona Di Pietro[9], o edital é "*ato pelo qual a Administração divulga a abertura da concorrência, fixa os requisitos para participação, define o objeto e as condições básicas do contrato e convida a todos os interessados para que apresentem suas propostas*".

Portanto, conclui-se que o Edital é o instrumento adequado para que a Administração Pública tenha êxito em atingir os objetivos impostos pelo Regime Jurídico Administrativo, bem como trazer segurança jurídica a avença.

Esse entendimento está consolidado no âmbito do Superior Tribunal de Justiça, como se pode aferir, *in verbis*: "*(...) o Poder Discricionário da Administração esgota-se com a elaboração do Edital de Licitação. A partir daí, nos termos do vocábulo constante da própria Lei, a Administração Pública vincula-se 'estritamente' a ele.*" (REsp. nº 421.946/DF, 1ª T., rel. Min, Francisco Falcão, j. em 7.02.2006, DJ em 6.3.2006, p. 163).

Ademais, o Edital é o instrumento convocatório do cotejo, cabendo a ele dispor acerca das condições e regras de habilitação, critérios de julgamento, bem como definir as penalidades a serem cominadas, a forma de pagamento, dentre outros aspectos. Assim, cumpre-lhe atribuir mecanismos que assegurem e promovam a máxima competitividade e a igualdade entre os licitantes, de maneira que o resultado do certame seja o mais efetivo e legítimo aos interesses da Administração Pública.

A Lei nº 14.133/2021 estabelece diretrizes para a elaboração do edital de licitação, determinando, em seu **art. 25**, que o instrumento convocatório deve conter regras claras sobre **o objeto da licitação, a convocação dos interessados, os critérios de julgamento e habilitação, as sanções, as condições contratuais e os critérios de fiscalização e pagamento**.

Especificamente sobre **licitações para registro de preços**, o edital deverá observar o disposto no **Art. 82**. Assim, a **Minuta de Edital n.º 79.2025.CPL (2031551)** foi analisada à luz dos requisitos legais mencionados, contemplando os requisitos legais exigidos pela Lei nº 14.133/2021,

observando, de forma adequada, os princípios da legalidade, isonomia e transparência que regem a contratação pública.

Da Análise da Minuta de Contrato

Inicialmente, cumpre esclarecer que, ressalvadas as hipóteses legais de contratação verbal, todos os ajustes celebrados pela Administração Pública devem ser formalizados mediante instrumento contratual, o que pode ocorrer por meio de termo de contrato, nota de empenho, ordem de serviço ou outro instrumento equivalente, conforme previsto no art. 95 da Lei nº 14.133/2021. Vejamos:

> Art. 95. O instrumento de contrato é obrigatório, salvo nas seguintes hipóteses, em que a Administração poderá substituí-lo por outro instrumento hábil, como carta-contrato, nota de empenho de despesa, autorização de compra ou ordem de execução de serviço:
>
> I - dispensa de licitação em razão de valor;
>
> II - compras com entrega imediata e integral dos bens adquiridos e dos quais não resultem obrigações futuras, inclusive quanto a assistência técnica, independentemente de seu valor.

Assim, o fato de a Administração optar pela formalização do ajuste por meio de termo de contrato ou outro instrumento hábil não descaracteriza a natureza jurídica contratual da relação estabelecida, a qual permanece submetida ao regime jurídico das contratações públicas. Sobre esse aspecto, são pertinentes as observações de Renato Geraldo Mendes[10] :

> **O contrato – como negócio jurídico que é – deve ser instrumentalizado ou formalizado por escrito**, pois o contrato verbal só é admitido nas pequenas compras de pronto pagamento, consoante parágrafo único do art. 60. A formalização do contrato, na visão tradicional, ocorre mediante as seguintes formas: a) instrumento de contrato; b) carta-contrato; c) nota de empenho; d) autorização de compra; e) ordem de execução de serviços; f) outros. **Todas essas formas são espécies ou modos distintos de instrumentalização do negócio, que é o contrato.** Entretanto, o chamado 'instrumento ou termo de contrato' é obrigatório sempre que do ajuste resultar obrigação futura a ser assegurada ou cumprida pelo contratado. (...). (Destacamos.)

Como se observa, o termo de contrato constitui apenas um dos instrumentos hábeis à formalização do vínculo contratual, entendido este como a relação jurídica de natureza obrigacional, na qual a contratada se compromete a executar a prestação nos moldes previamente pactuados, enquanto à contratante incumbe a obrigação de promover o pagamento correspondente, condicionado ao recebimento regular do objeto contratado.

Diante disso, é relevante compreender as diretrizes que orientam a escolha do instrumento a ser adotado na formalização dos contratos administrativos, decisão esta que deve observar o disposto na legislação vigente e nas normas internas aplicáveis.

De acordo com o entendimento majoritário do TCU, a exigência de formalização por termo de contrato subsiste sempre que a avença implicar obrigações futuras, ainda que nas hipóteses de contratação por dispensa em razão de valor. Em outras palavras, mesmo diante de contratações de pequeno vulto, a substituição do termo de contrato não será admitida quando não houver entrega imediata e integral do objeto, ou quando houver obrigações posteriores, como assistência técnica, garantias ou prestações contínuas.

Esse entendimento restou evidenciado, por exemplo, no seguinte Acórdão, que inclusive reconhece a existência de divergência interpretativa sobre o tema:

Acórdão nº 3352/2015 - Plenário

[Relatório]

6.1.1. O caput do art. 62 da Lei de Licitações estabelece que o instrumento de contrato é obrigatório nos casos de concorrência e de tomada de preços, bem como, nas dispensas e inexigibilidades cujos preços estejam compreendidos nos limites destas duas modalidades de licitação, podendo, nos demais casos, ocorrer a substituição daquele documento por instrumentos equivalentes, tais como a carta-contrato, a nota de empenho de despesa, a autorização de compra ou a ordem de execução de serviço. O §4º do art. 62, por sua vez, prevê que o termo de contrato poderá ainda ser substituído nos casos de compra com entrega imediata e integral dos bens adquiridos, dos quais não resultem obrigações futuras, inclusive assistência técnica, independentemente do valor da contratação;

6.1.2. **Na jurisprudência desta Casa, conforme podemos denotar do Acórdão 2147/2015-P, com posicionamento acolhido pelo Exmo. Sr. Ministro José Múcio Monteiro, existem divergências de entendimento (como no Acórdão 3528/2015-P) quanto à interpretação do dispositivo**:

‘7.9. Dessa norma, extraem-se duas interpretações relevantes. Primeiramente, mesmo no caso de contratações com valores inseridos nos limites da concorrência e tomada de preços, quando a entrega dos bens adquiridos for imediata e integral, o termo de contrato é dispensável. De outro lado, caso das contratações resultem em obrigações futuras, o instrumento formalizado é obrigatório.

7.10. Muitos analistas entendem o dispositivo como exceção dupla ao art. 62 do Estatuto, pois prevê a possibilidade de aquisições sem termo de contrato em qualquer hipótese e obrigatoriedade do instrumento contratual, mesmo em

valores abaixo dos limites da concorrência e da tomada de preços. Para o último caso, bastaria a existência de obrigações futuras.

7.11. **O Tribunal tem manifestações nos dois sentidos, mas mantém jurisprudência sistematizada com entendimento de que a contratação deve ser formalizada obrigatoriamente por meio de termo de contrato sempre que houver obrigações futuras decorrentes do fornecimento de bens e serviços, independentemente da modalidade de licitação, sua dispensa ou inexigibilidade, conforme preconizado no art. 62, § 4º, da Lei 8.666/1993**;'

[Voto]

5. Quanto à ausência de instrumento de contrato, com esteio no art. 62, § 4º, da Lei de Licitações, restou evidenciado que a Sesau/TO, nesse ponto específico, incorreu apenas em falha de menor gravidade, já que, apesar de o valor do contrato ter ultrapassado o valor permitido para o uso da modalidade convite, **os medicamentos adquiridos tiveram a sua entrega em curto espaço de tempo, destacando que 80% dos insumos adquiridos foram entregues em um intervalo inferior a 30 dias, com os 20% restantes sendo entregues dentro de mais 40 dias, sem envolver obrigações futuras de parte a parte**.

6. Sendo assim, e considerando que essa falha não se consumou em prejuízo efetivo, entendo assistir razão à unidade técnica no sentido de que a conduta dos gestores da Sesau/TO, nesse ponto específico, não justifica a apenação. (Destacamos.)

Especificamente em relação ao disposto no art. 95 da Lei nº 14.133/2021, observa-se que o legislador adotou dois critérios objetivos para excepcionar a regra da obrigatoriedade do instrumento de contrato, permitindo, nesses casos, a utilização de instrumento hábil mais simples para a formalização da avença:

- no inciso I, o **caráter econômico da contratação**, ou seja, contratos com valores inferiores aos limites admitidos para a contratação direta por dispensa de licitação em razão do valor (art. 75, incisos I e II da Lei nº 14.133/2021); e

- no inciso II, independentemente do valor da contratação, **a simplicidade das obrigações contratadas e a ausência de risco,** o que ocorre nas compras com entrega imediata e integral dos bens adquiridos e dos quais não resultem obrigações futuras, inclusive quanto à assistência técnica.

Com base em uma interpretação estritamente literal do art. 95 da Lei nº 14.133/2021, seria possível concluir que o instrumento de contrato é obrigatório, exceto nas hipóteses de contratação por dispensa de licitação fundadas no critério do valor, previstas nos incisos I e II do art. 75 da referida norma.

Essa leitura conduziria à conclusão de que, mesmo quando a

contratação se der por meio de licitação ou por outras hipóteses legais de contratação direta, **não seria admissível substituir o termo de contrato por outro instrumento hábil**, ainda que os valores envolvidos estejam abaixo dos limites estabelecidos nos incisos I e II do art. 75 da Lei.

Contudo, essa conclusão **não se revela adequada**, pois desconsidera a aplicação dos demais métodos de interpretação jurídica, especialmente o **sistemático e o teleológico**, os quais se impõem na análise de normas voltadas à racionalização e à eficiência administrativa.

Nesse sentido, é pertinente a advertência de **Marçal Justen Filho**[11], ao destacar que:

> No entanto, deve-se reputar que as palavras da lei (até mesmo da Lei Constitucional) configuram uma espécie de 'indício', em termos hermenêuticos. Significa que o hermeneuta não pode restringir sua atividade à simples constatação da existência de um texto legal. Não pode isolar uma vontade normativa restrita e autônoma, de existência circunscrita a um dispositivo. Deve considerar o conjunto normativo: a compreensão de cada regra depende da compreensão do conjunto de todas elas.
>
> (...). A atividade hermenêutica pressupõe o método gramatical. Sem compreender o sentido das palavras, é impossível compreender a norma jurídica. Mas o Direito é um conjunto de normas, que se orienta à produção de determinados resultados. Portanto, a interpretação inicia-se com a gramática, mas não se encerra com ela. **Interpretar significa avaliar o conjunto de normas jurídicas e apreender os fins a que se norteia a norma**. É tarefa complexa, que pressupõe um postulado fundamental: a letra da lei não se apresenta como um fim em si mesma mas não se encerra em si própria. (...).
>
> Vale dizer, as normas jurídicas não se confundem com a letra da lei. (...).
>
> (...). A lei não é elaborada para bastar-se em si mesma, tal como se os fins do Direito fossem menos relevantes do que as palavras do legislador. Como ensinou Engish, 'não só a lei pode ser mais inteligente do que o seu autor, como também o intérprete pode ser mais inteligente do que a lei'.
>
> Nesse passo, a atividade administrativa exige prestígio aos princípios da razoabilidade e proporcionalidade. (...). O princípio da regra da razão expressa-se em '**procurar a solução que está mais em harmonia com as regras de direito existentes e que, por isso, parece a mais satisfatória, em atenção à preocupação primária de segurança, temperada pela justiça, que é a base do direito**'. (Destacamos)

Em oposição ao método literal de interpretação, forma-se a **interpretação sistemática,** a qual, como leciona Maria Helena Diniz[12], "considera o sistema em que se insere a norma, relacionando-a com outras concernentes ao mesmo objeto. Isto é assim porque o sistema jurídico não se

compõe de um só sistema de normas, mas de vários, que constituem um conjunto harmônico e interdependente, embora cada qual esteja fixado em seu lugar próprio”

A partir de uma interpretação sistemática do art. 95, inciso I, da Lei nº 14.133/2021, infere-se que, tratando-se de contratação cujo valor seja inferior ao limite estabelecido para a contratação direta por dispensa de licitação em razão do valor (art. 75, incisos I e II), será admissível a substituição do termo de contrato por outro instrumento hábil, **independentemente do procedimento utilizado para a escolha do contratado**, seja por meio de licitação ou por contratação direta, por dispensa ou inexigibilidade de licitação.

No mesmo sentido, destaca-se o entendimento adotado pela Advocacia-Geral da União, conforme disposto na **Orientação Normativa AGU nº 21/2022**, a qual estabelece que:

> I - Nas contratações decorrentes da Lei nº 14.133/2021, **independentemente do objeto, do prazo de vigência, do parcelamento do fornecimento, da existência ou não de obrigações futuras e da forma empregada para selecionar o contratado (processo licitatório, contratação direta por dispensa ou inexigibilidade de licitação),** será possível substituir o instrumento de contrato por instrumentos mais simples **sempre que o contrato possuir valor inferior aos limites para a dispensa de licitação em razão do valor (art. 75, incisos I e II);**
>
> II - Nas contratações decorrentes da Lei nº 14.133/2021, **independentemente do valor, será possível substituir o instrumento de contrato por instrumentos mais simples sempre que o contrato consistir na compra de bens com entrega imediata e integral e dos quais não resultem obrigações futuras,** inclusive quanto a assistência técnica”. (Destacamos.)

Acerca de obrigações futuras, a Consultoria Zênite[13], externou o seguinte posicionamento:

> obrigações futuras são aquelas que vinculam a Administração **ao contratado** durante determinado período, para além da entrega do objeto, podendo dizer respeito tanto ao objeto principal do contrato (como na hipótese de execução fracionada no tempo), como a outras obrigações decorrentes da execução desse objeto principal (tal como garantia prestada pelo próprio contratado).
>
> É importante observar que a Administração fica vinculada ao contratado na aquisição dos bens. No entanto, quando a garantia é oferecida diretamente pelo fabricante do produto adquirido, essa vinculação não se aplica.
>
> Nesse caso, o fabricante do produto, diferentemente do vendedor, caracteriza-se como terceiro diante da relação jurídica formada entre a Administração e

> o contratado que vendeu o produto, sendo a garantia por ele prestada de caráter extracontratual. E, além disso, essa garantia oferecida pelo fabricante refere-se ao produto e não à pessoa que o está adquirindo, ou seja, toda e qualquer pessoa que comprar aquele produto terá a mesma garantia.
>
> Situação diversa é aquela que deriva da garantia oferecida pela própria contratada, esta sim, caracterizando obrigação futura, pois se refere à relação jurídica estabelecida entre ela e a Administração.
>
> Nesse sentido, esta Consultoria entende que a garantia do fabricante do bem adquirido, a rigor, não deve ser considerada como obrigação futura imposta ao contratado, para fins de determinar a obrigatoriedade de formalização do instrumento de contrato. Nesse caso, desde que não exista garantia oferecida pelo próprio contratado (vendedor), será possível a substituição do termo de contrato por outros instrumentos hábeis.

No caso em exame, verifica-se que a Divisão de Contratos e Convênios elaborou a **Minuta de Contrato Administrativo n.º 69.2025.DCCON - CONTRATOS (2033432)**, na forma **art. 92 da Lei nº 14.133/2021.**

Destaca-se que o **Contrato Administrativo**, a ser firmado com a futura contratada, deve estar em consonância com o art. 89 c/c art. 92 da Lei n° 14.133/21, vejamos:

> Art. 89. Os contratos de que trata esta Lei regular-se-ão pelas suas cláusulas e pelos preceitos de direito público, e a eles serão aplicados, supletivamente, os princípios da teoria geral dos contratos e as disposições de direito privado.
>
> § 1º Todo contrato deverá mencionar os nomes das partes e os de seus representantes, a finalidade, o ato que autorizou sua lavratura, o número do processo da licitação ou da contratação direta e a sujeição dos contratantes às normas desta Lei e às cláusulas contratuais.
>
> § 2º Os contratos deverão estabelecer com clareza e precisão as condições para sua execução, expressas em cláusulas que definam os direitos, as obrigações e as responsabilidades das partes, em conformidade com os termos do edital de licitação e os da proposta vencedora ou com os termos do ato que autorizou a contratação direta e os da respectiva proposta.
>
> Art. 92. São necessárias em todo contrato cláusulas que estabeleçam:
>
> I - o objeto e seus elementos característicos;
>
> II - a vinculação ao edital de licitação e à proposta do licitante vencedor ou ao ato que tiver autorizado a contratação direta e à respectiva proposta;
>
> III - a legislação aplicável à execução do contrato,

inclusive quanto aos casos omissos;

IV - o regime de execução ou a forma de fornecimento;

V - o preço e as condições de pagamento, os critérios, a data-base e a periodicidade do reajustamento de preços e os critérios de atualização monetária entre a data do adimplemento das obrigações e a do efetivo pagamento;

VI - os critérios e a periodicidade da medição, quando for o caso, e o prazo para liquidação e para pagamento;

VII - os prazos de início das etapas de execução, conclusão, entrega, observação e recebimento definitivo, quando for o caso;

VIII - o crédito pelo qual correrá a despesa, com a indicação da classificação funcional programática e da categoria econômica;

IX - a matriz de risco, quando for o caso;

X - o prazo para resposta ao pedido de repactuação de preços, quando for o caso;

XI - o prazo para resposta ao pedido de restabelecimento do equilíbrio econômico-financeiro, quando for o caso;

XII - as garantias oferecidas para assegurar sua plena execução, quando exigidas, inclusive as que forem oferecidas pelo contratado no caso de antecipação de valores a título de pagamento;

XIII - o prazo de garantia mínima do objeto, observados os prazos mínimos estabelecidos nesta Lei e nas normas técnicas aplicáveis, e as condições de manutenção e assistência técnica, quando for o caso;

XIV - os direitos e as responsabilidades das partes, as penalidades cabíveis e os valores das multas e suas bases de cálculo;

XV - as condições de importação e a data e a taxa de câmbio para conversão, quando for o caso;

XVI - a obrigação do contratado de manter, durante toda a execução do contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições exigidas para a habilitação na licitação, ou para a qualificação, na contratação direta;

XVII - a obrigação de o contratado cumprir as exigências de reserva de cargos prevista em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social e para aprendiz;

XVIII - o modelo de gestão do contrato, observados os requisitos definidos em regulamento;

XIX - os casos de extinção.

§ 1º Os contratos celebrados pela Administração Pública com pessoas físicas ou jurídicas, inclusive as domiciliadas no exterior, deverão conter cláusula que declare competente o foro da sede da Administração para dirimir qualquer questão contratual, ressalvadas as seguintes hipóteses:

I - licitação internacional para a aquisição de bens e serviços cujo pagamento seja feito com o produto de financiamento concedido por organismo financeiro internacional de que o Brasil faça parte ou por agência estrangeira de cooperação;

II - contratação com empresa estrangeira para a compra

de equipamentos fabricados e entregues no exterior precedida de autorização do Chefe do Poder Executivo;

III - aquisição de bens e serviços realizada por unidades administrativas com sede no exterior.

§ 2º De acordo com as peculiaridades de seu objeto e de seu regime de execução, o contrato conterá cláusula que preveja período antecedente à expedição da ordem de serviço para verificação de pendências, liberação de áreas ou adoção de outras providências cabíveis para a regularidade do início de sua execução.

§ 3º Independentemente do prazo de duração, o contrato deverá conter cláusula que estabeleça o índice de reajustamento de preço, com data-base vinculada à data do orçamento estimado, e poderá ser estabelecido mais de um índice específico ou setorial, em conformidade com a realidade de mercado dos respectivos insumos.

§ 4º Nos contratos de serviços contínuos, observado o interregno mínimo de 1 (um) ano, o critério de reajustamento de preços será por:

I - reajustamento em sentido estrito, quando não houver regime de dedicação exclusiva de mão de obra ou predominância de mão de obra, mediante previsão de índices específicos ou setoriais;

II - repactuação, quando houver regime de dedicação exclusiva de mão de obra ou predominância de mão de obra, mediante demonstração analítica da variação dos custos.

§ 5º Nos contratos de obras e serviços de engenharia, sempre que compatível com o regime de execução, a medição será mensal.

§ 6º Nos contratos para serviços contínuos com regime de dedicação exclusiva de mão de obra ou com predominância de mão de obra, o prazo para resposta ao pedido de repactuação de preços será preferencialmente de 1 (um) mês, contado da data do fornecimento da documentação prevista no § 6º do art. 135 desta Lei.

§ 7º Para efeito do disposto nesta Lei, consideram-se como adimplemento da obrigação contratual a prestação do serviço, a realização da obra ou a entrega do bem, ou parcela destes, bem como qualquer outro evento contratual a cuja ocorrência esteja vinculada a emissão de documento de cobrança. (Incluído pela Lei nº 14.770, de 2023).

Dessa forma, a análise da **Minuta de Contrato Administrativo** evidencia que o documento **está em conformidade com a Lei nº 14.133/2021**, atendendo aos **princípios da transparência, segurança jurídica e eficiência administrativa**.

III) CONCLUSÃO

Assim, esta Assessoria Jurídica manifesta-se pela **REGULARIDADE JURÍDICA** do procedimento submetido ao exame. Ressalta-se, ainda, que esta manifestação não abrange o juízo de mérito da Administração, tampouco os aspectos técnicos, econômicos e financeiros, os quais não são objeto de análise

desta assessoria.

Deste modo, caso a autoridade competente assim decida, conforme disposto no **§ 3° do art. 53 da Lei nº 14.133/2021,** estão presentes os requisitos para a tornar pública a licitação, na modalidade **PREGÃO, na forma ELETRÔNICA, para REGISTRO DE PREÇOS, com critério de julgamento MENOR PREÇO GLOBAL**, com modo de disputa "**ABERTO"**, nos termos da Lei nº 14.133, de 2021, do Ato nº 008/2024/PGJ, para *contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses*.

É o parecer que submento à apreciação de Vossa Excelência.

ASSESSORIA DA SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, Manaus (AM), *na data de assinatura*.

GUILHERME HENRICH BENEK VIEIRA

Assessor Jurídico de Subprocurador-Geral de Justiça

Ato n.º 082/2025/PGJ - DOMPE, ed. 3.058, de 3.04.2025

Matrícula nº 000.819-2A

---

[1] FILHO, Marçal Justen. Comentários à Lei de Licitações e Contratos Administrativos. 12ª ed. São Paulo: Dialética, 2008a.
[2] DE MELLO, Celso Antonio Bandeira, em Curso de Direito Administrativo. São Paulo: Malheiros, 2009.
[3] MEIRELES, Hely Lopes, Direito Administrativo Brasileiro. 44ª ed., Salvador: JusPODIVM, 2020.
[4] MEIRELLES, Hely Lopes. Direito administrativo brasileiro. 43 ed., São Paulo: Malheiros, 2018.
[5] DI PIETRO, Maria Silvia, Direito Administrativo, 28ª ed., São Paulo; Atlas, 2015a.
[6] ALVES, Felipe Dalenogare. Manual de Licitações e Contratos Administrativos / Felipe Dalenogare Alves, Marilene Carneiro Matos, São Paulo: Saraiva-jur, 2025.
[7] CARVALHO, Matheus. Nova Lei de Licitações Comentada e Comparada / Matheus Carvalho, João Paulo Oliveira e Paulo Germano Rocha, São Paulo: Editora Juspodivm, 2024. p.165.
[8] TORRES, Ronny Charles Lopes de. Lei de Licitações Públicas Comentadas, Salvador: Juspodivm, 2018. p.44.
[9] DI PIETRO, Maria Sylvia Zanela, Direito Administrativo, 23ª Ed., Editora Atlas, 2010. p. 388
[10] Zênite Fácil. Lei nº 8.666/93, nota ao art. 62, categoria Doutrina. Disponível em: http://www.zenitefacil.com.br
[11] JUSTEN FILHO, Marçal. Comentários à lei de licitações e contratos administrativos. 7. ed. São Paulo: Dialética, p. 77
[12] DINIZ, Maria Helena. Curso de direito civil brasileiro. São Paulo: Saraiva, 2003. p. 49.
[13] A Nova Lei de Licitações e as hipóteses de substituição contratual previstas no art. 95. Zênite Fácil, categoria Orientação Prática, 16 set. 2024. Disponível em: http://www.zenitefacil.com.br. Acesso em: 14 abr. 2025.

Documento assinado eletronicamente por **Guilherme Henrich Benek Vieira**, **Assessor(a) Jurídico(a) de Subprocurador-Geral de Justiça**, em 29/12/2025, às 14:39, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2037607** e o código CRC **A0C22838**.

DESPACHO Nº 1245.2025.01AJ-SUBADM.2037699.2025.007562

PROCESSO N.º: 2025.007562

ASSUNTO: Contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses.

INTERESSADO: Diretoria de Tecnologia da Informação e Comunicação (DTIC)

Trata-se dos autos do procedimento interno em epígrafe, versando sobre o objeto de referência, instruído por solicitação formalizada pelo senhor **EUDO DE LIMA ASSIS JUNIOR, Diretor de Tecnologia da Informação e Comunicação – DTIC,** que apresentou o detalhamento do objeto, inicialmente, por intermédio do ESTUDO TÉCNICO PRELIMINAR - ETP Nº 7.2025.DTIC.1591885.2025.007562 e Termo de Referência Nº 9.2025.DTIC.1605182.2025.007562.

Os artefatos da contratação foram devidamente analisados pela Assessoria Jurídica, oportunidade na qual foram determinadas algumas adequações nos documentos, nos termos do Despacho Nº 605.2025.01AJ-SUBADM.1673215.2025.007562, lavrado pelo Exmo. Sr. Dr. ANDRÉ VIRGÍLIO BELOTA SEFFAIR, *Subprocurador-Geral de Justiça para Assuntos Administrativo*.

Dando prosseguimento ao feito, a **DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – DTIC** encaminhou novo **Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562**, sendo aprovado pelo Exmo. Sr. Dr. ANDRÉ VIRGÍLIO BELOTA SEFFAIR, *Subprocurador-Geral de Justiça para Assuntos Administrativo*, nos termos do Despacho Nº 1123.2025.01AJ-SUBADM.2013504.2025.007562.

Por sua vez, o **SETOR DE COMPRAS E SERVIÇOS – SCOMS** emitiu o **Quadro-Resumo do Processo de Compra N.º 547.2025.SCOMS.2023741.2025.007562**.

Na sequência, a **DIRETORIA DE ORÇAMENTOS E FINANÇAS - DOF** carreou aos autos a correspondente **NOTA DE AUTORIZAÇÃO DE DESPESAS / ADJUDICAÇÃO -NAD Nº 512.2025.DOF - ORÇAMENTO.2028015.2025.007562.**

Encaminhados os autos à Comissão Permanente de Licitação (CPL) diligência junto à **Divisão de Contratos e Convênios - DCCON**, através do Ofício Nº 479.2025.CPL.2031552.2025.007562, "para análise quanto à necessidade de elaboração de minuta de termo contratual ou instrumento equivalente, especialmente em face do teor do Termo de Referência nº 28.2025.DTIC.2002143.2025.007562**."**

Por seu turno, a **DIVISÃO DE CONTRATOS E CONVÊNIOS - DCCON** elaborou a **MINUTA DE CONTRATO ADMINISTRATIVO Nº 68.2025.DCCON. No entanto,** após uma análise mais detalhada dos autos, a Divisão de Contratos e Convênios (DCCON) remete uma nova minuta a **MINUTA DE CONTRATO ADMINISTRATIVO Nº 69.2025.DCCON - CONTRATOS.2033432.2025.007562,** visando à inclusão da **Cláusula Décima Quarta - Da Garantia Contratual**.

Assim, a Comissão Permanente de Licitação, através do **Despacho Nº 89.2025.CPL (2037097)**, realizou a juntada da **Minuta de Edital 79 (2031551)**, cujo objeto é a *contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses.*

Dando seguimento à analise da minuta de edital apresentada, a Assessoria Jurídica, por meio do **Parecer n.º 201.2025.01AJ-SUBADM (2037607)**, opinou da seguinte maneira:

> **III) CONCLUSÃO**
>
> Assim, esta Assessoria Jurídica manifesta-se pela **REGULARIDADE JURÍDICA** do procedimento submetido ao exame. Ressalta-se, ainda, que esta manifestação não abrange o juízo de mérito da Administração, tampouco os aspectos técnicos, econômicos e financeiros, os quais não são objeto de análise desta assessoria.
>
> Deste modo, caso a autoridade competente assim decida, conforme disposto no **§ 3° do art. 53 da Lei nº 14.133/2021,** estão presentes os requisitos para a tornar pública a licitação, na modalidade **PREGÃO, na forma ELETRÔNICA, para REGISTRO DE PREÇOS, com critério de julgamento MENOR PREÇO GLOBAL**, com modo de disputa "**ABERTO"**, nos termos da Lei nº 14.133, de 2021, do Ato nº 008/2024/PGJ, para *contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses*.
>
> .

Assim sendo, com fulcro no no § 3.º do art. 53 da Lei nº 14.133/2021, pelos fatos e fundamentos apresentados nos autos, **ACOLHO** na íntegra a citada peça opinativa e **APROVO** a **Minuta de Edital 79 (2031551)** e a **Minuta de Contrato Administrativo 69 (2033432)**, para realização de **PREGÃO, na forma ELETRÔNICA, com critério de julgamento MENOR PREÇO GLOBAL**, com modo de disputa "**ABERTO"**, que tem como objeto a *contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses,* nos termos da Lei nº 14.133, de 2021, do Ato PGJ 008/2024 e demais legislação aplicável.

Dessa forma, **ENCAMINHE-SE** à **Comissão Permanente de Licitação** para as demais providências cabíveis.

CUMPRA-SE.

GABINETE DA SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, Manaus (AM), *data da assinatura eletrônica.*

ANDRÉ VIRGÍLIO BELOTA SEFFAIR

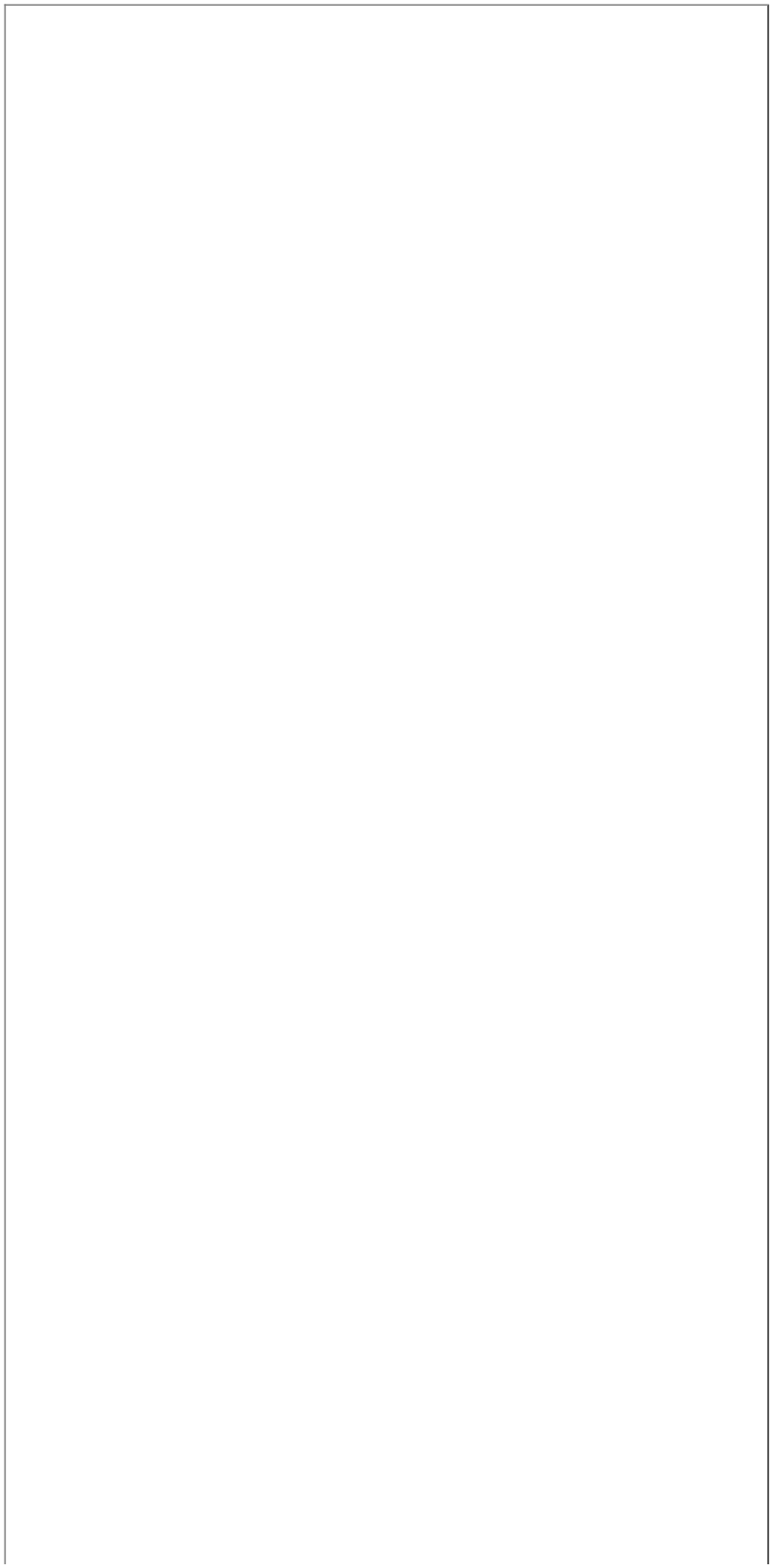
Subprocurador-Geral de Justiça para Assuntos Administrativos

Documento assinado eletronicamente por **André Virgílio Belota Seffair**, **Subprocurador(a)-Geral de Justiça para Assuntos Administrativos**, em 29/12/2025, às 15:22, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2037699** e o código CRC **04BCB19B**.

AVISO Nº 2037915 - CPL

Área de publicação:



Ministério Público do Estado do Amazonas
Procuradoria-Geral de Justiça

AVISO DE LICITAÇÃO

PREGÃO ELETRÔNICO N.º 94.001/2026-CPL/MP/PGJ

PROCESSO SEI N.º 2025.007562

O B J E T O : Contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma **solução de datacenter**, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, **com garantia de 60 (sessenta) meses.**

REGIME JURÍDICO: Lei Federal n.º 14.133 de 2021.

ABERTURA: 19/01/2026 às 10h. (horário de Brasília)

ENTREGA DAS PROPOSTAS: a partir de **05/01/2026**

LOCAL: no site **https://www.gov.br/compras/pt-br**

UASG: 925849 – PROCURADORIA GERAL DE JUSTIÇA AM.

Informações adicionais, dúvidas e pedidos de esclarecimentos deverão ser dirigidos à COMISSÃO PERMANENTE DE LICITAÇÃO pelo telefone **(92) 3655-0743 ou pelo e-mail licitacao@mpam.mp.br.**

Manaus, 30 de dezembro de 2025.

Sarah Madalena Barbosa Côrtes de Melo
Presidente da Comissão Permanente de Licitação
Ato PGJ n.º 165/2025 - DOMPE, Ed. 3121, de 15.07.2025

Fim da área de publicação.

Em 30 de dezembro de 2025.

Documento assinado eletronicamente por **Sarah Madalena Barbosa Santos Cortes**, **Presidente da Comissão Permanente de Licitação - CPL**, em 30/12/2025, às 12:19, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2037915** e o código CRC **1586396D**.

EDITAL PREGÃO ELETRÔNICO N.º 94.001/2026-CPL/MP/PGJ

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS

PROCURADORIA GERAL DE JUSTIÇA

UASG 925849

OBJETO

Contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma **solução de datacenter,** contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com **garantia de 60 (sessenta) meses**.

VALOR TOTAL DA CONTRATAÇÃO

Orçamento sigiloso

DATA DA SESSÃO PÚBLICA

Dia **19/01/2026** às **10h (horário de Brasília)**

CRITÉRIO DE JULGAMENTO:

[X] MENOR PREÇO / **[__]** MAIOR DESCONTO por [ ] ITEM / [ ] POR GRUPO / **[X] GLOBAL**

MODO DE DISPUTA:

[X] ABERTO / **[_]** ABERTO E FECHADO / **[_]** FECHADO E ABERTO

PREFERÊNCIA ME/EPP/EQUIPARADAS

[__] SIM / [X] NÃO

SUMÁRIO

1. DAS DISPOSIÇÕES GERAIS
2. DO OBJETO
3. DOS RECURSOS ORÇAMENTÁRIOS
4. DO CREDENCIAMENTO
5. DAS CONDIÇÕES PARA PARTICIPAÇÃO
6. DO ENVIO DAS PROPOSTAS E DOS DOCUMENTOS DE HABILITAÇÃO
7. DO PREENCHIMENTO DA PROPOSTA
8. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES
9. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA
10. DA FASE DE JULGAMENTO
11. DA HABILITAÇÃO
12. DOS RECURSOS ADMINISTRATIVOS
13. DA REABERTURA DA SESSÃO PÚBLICA
14. DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO
15. DOS PRAZOS E CONDIÇÕES DE ENTREGA E RECEBIMENTO
16. O TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE
17. DAS OBRIGAÇÕES DA CONTRATADA
18. DAS OBRIGAÇÕES DA CONTRATANTE
19. DO PAGAMENTO
20. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES
21. DA REPACTUAÇÃO, REAJUSTE E REVISÃO DE PREÇO
22. DOS ESCLARECIMENTOS E DA IMPUGNAÇÃO DO ATO CONVOCATÓRIO
23. DAS DISPOSIÇÕES FINAIS

EDITAL DO PREGÃO ELETRÔNICO N.º 94.001/2026-CPL/MP/PGJ

O **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS** pelo presente edital e por intermédio da **PROCURADORIA GERAL DE JUSTIÇA**, cadastrada no CNPJ sob o n.º 04.153.748/0001-85, tendo em vista o que consta do **Processo SEI n.º 2025.007562**, através da **COMISSÃO PERMANENTE DE LICITAÇÃO – CPL**, designada pelo Ato PGJ n.º 165/2025, e alterações, de lavra da Procuradora-Geral de Justiça, torna público que realizará licitação, na modalidade **PREGÃO, na forma ELETRÔNICA, com critério de julgamento MENOR PREÇO GLOBAL**, com modo de disputa "**ABERTO"**, nos termos da Lei nº 14.133, de 2021, do Ato PGJ n.º 008/2024 e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

O contrato correspondente, ou o instrumento que vier a substituí-lo, será regido pela Lei nº 14.133, de 2021 e suas alterações.

PROCESSO SEI	**2025.007562**
Recebimento das propostas	a partir da data de publicação do aviso no PNCP
Abertura das propostas	às 10h do dia **19/01/2026** (horário de Brasília)
Licitação exclusiva para ME/EPP	**( ) SIM (*X*) NÃO**
Endereço eletrônico	https://www.gov.br/compras/pt-br
Código UASG	925849

1. DAS DISPOSIÇÕES GERAIS

1.1. O pregão será realizado em sessão pública, por meio da utilização de recursos da tecnologia da informação – *internet*, utilizando-se, para tanto, de métodos de autenticação de acesso e recursos de criptografia, garantindo segurança em todas as fases do certame.

1.2. Os trabalhos serão conduzidos por servidor público integrante da **COMISSÃO PERMANENTE DE LICITAÇÃO** deste Órgão, por ato interno, denominado(a) PREGOEIRO(A), e membros da equipe de apoio, previamente credenciados no aplicativo https://www.gov.br/compras/pt-br.

1.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública, observarão rigorosamente o horário de **Brasília – DF**, e, dessa forma, serão registradas no sistema eletrônico e na documentação relativa ao certame.

2. DO OBJETO

2.1. O objeto da presente licitação é a escolha da proposta mais vantajosa para a **contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses**, de acordo com as condições constantes do Edital e seus anexos.

2.2. Por tratar-se de solução integrada, onde o funcionamento efetivo e satisfatório depende de cada um dos seus itens e serviços em conjunto, como um todo, o objeto da presente licitação será organizado em **LOTE ÚNICO**, de acordo com as especificações constantes do **TERMO DE REFERÊNCIA N.º 28.2025.DTIC.2002143.2025.007562**, conforme tabela abaixo:

ITEM	DESCRIÇÃO	QUANTIDADE
01	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9	4
02	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU	1
03	SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX	5
04	SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU	1
05	LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE	50
06	SOFTWARE DE BACKUP DE DADOS	1
07	EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	1
08	SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	1
09	SWITCH CORE	2

2.3. No presente certame não haverá itens com participação exclusiva à microempresas e empresas de pequeno porte, nos termos do art. 48 da Lei Complementar nº 123, de 14 de dezembro de 2006

2.4. O critério de julgamento adotado será o **menor preço GLOBAL**, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.

2.4.1. Em observância ao disposto no §1º do art. 82 da Lei Federal nº 14.133/2021, o critério de julgamento de menor preço GLOBAL foi adotado, pois, por se tratar de uma solução integrada, a licitação por itens não se revela vantajosa técnica e economicamente, no presente caso.

2.4.2. Não obstante, na fase de aceitação da proposta, serão observados, como critério de aceitabilidade, os preços unitários máximos estimados para cada item.

2.5. O objeto da futura contratação compreenderá, sobretudo, as especificações constantes do **TERMO DE REFERÊNCIA Nº 28.2025.DTIC.2002143.2025.007562**, Anexo I deste Edital, sem prejuízo das demais prescrições figuradas no mencionado documento, bem assim na Minuta do Contrato Administrativo Nº 68.2025.DCCON - CONTRATOS.2031978.2025.007562, Anexo II do Edital.

2.6. Os valores apresentados nos orçamentos e/ou propostas de preço deverão considerar inclusas todas as despesas relativas a frete, taxas, análises, amostras, impostos, licenças, encargos sociais, ou outras que possam influir direta ou indiretamente nos custos.

2.7. Integra a presente licitação, como parte indissolúvel deste Edital:

a) Anexo I — Termo de Referência nº 28.2025.DTIC.2002143.2025.007562;

b) Anexo II — Minuta de Contrato Administrativo Nº 69.2025.DCCON - CONTRATOS.2033432.2025.007562;

c) Anexo III — Modelo de Declarações Complementares;

d) Anexo IV — Modelo de Proposta de Preços;

e) Anexo V — Modelo de Solicitação de Cadastramento – SEFAZ/AM;

f) Anexo VI — Modelo de Credenciamento para Vistoria Técnica;

g) Anexo VII — Modelo de - Atestado de Vistoria Técnica; e

h) Anexo VIII — Modelo de Dispensa de Vistoria Técnica.

3. DOS RECURSOS ORÇAMENTÁRIOS

3.1. A despesa decorrente da contratação do objeto deste Pregão, quando efetivada, deverá recair por conta dos recursos específicos consignados no orçamento da PROCURADORIA-GERAL DE JUSTIÇA DO ESTADO DO AMAZONAS, nas seguintes classificações orçamentárias:

3.1.1. **Fonte de Recurso:** 1.500.100 - Recursos não Vinculados de Impostos, **Programa de Trabalho:** 03.091.3234.2536.0001 - Aparelhamento de Unidades Administrativas e Operacionais, **Elemento:** 4490.52 - Equipamentos e Material Permanente. **Subelemento:** 4490.52.55 - Tecnologia da Informação**.**

4. DO CREDENCIAMENTO

4.1. As empresas interessadas em participar do certame deverão providenciar, previamente, o credenciamento perante oSistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras), por meio de Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil

4.1.1. Para ter acesso ao sistema eletrônico, os interessados em participar deste pregão deverão dispor de chave de identificação e senha pessoal, obtidas junto ao SICAF, onde também deverão informar-se à respeito do seu funcionamento, regulamento e receber instruções detalhadas para sua correta utilização.

4.1.2. O credenciamento da licitante, bem como a sua manutenção, dependerá de registro cadastral atualizado no**SISTEMA DE CADASTRAMENTO UNIFICADO DE FORNECEDORES – SICAF**, em seu nível básico, que também será requisito obrigatório para fins de habilitação.

4.1.3. O credenciamento junto ao provedor do sistema implica a responsabilidade legal da licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes ao pregão eletrônico.

4.2. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou do **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS** (entidade promotora da licitação) por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

4.3. É de responsabilidade do licitante Cadastrado conferir a exatidão dos seus dados cadastrais no SICAF e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

4.3.1. A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação.

5. DAS CONDIÇÕES PARA PARTICIPAÇÃO

5.1. Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação, legalmente constituídos, desde que atendam às condições exigidas deste Edital e seus Anexos, inclusive quanto à documentação exigida, e que estejam com Credenciamento regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF.

5.1.1. **A licitante deverá declarar em campo próprio do sistema eletrônico a condição de microempresa ou empresa de pequeno porte**, para os fins previstos na Lei Complementar nº. 123/06.

5.1.1.1. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 16 da Lei nº 14.133, de 2021, para o agricultor familiar, o produtor rural pessoa física e para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006.

5.1.2. Os interessados deverão atender às condições exigidas no cadastramento no Sicaf até o terceiro dia útil anterior à data prevista para recebimento das propostas.

5.2. O licitante deverá estar devidamente credenciado no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras), por meio de Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil.

5.3. O licitante deverá manifestar, em campo próprio do sistema eletrônico, que cumpre plenamente os requisitos de habilitação, e que sua proposta está em conformidade com as exigências do instrumento convocatório.

5.4. Será exigida do licitante Declaração de Elaboração Independente de Proposta, a qual será feita no campo do sistema *Comprasnet* destinado para tanto e/ou nas Declarações Complementares de Habilitação, conforme Anexo III deste Edital.

5.5. Todos os custos decorrentes da elaboração e apresentação de propostas serão de responsabilidade exclusiva da licitante, não

sendo o **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**, em nenhum caso, responsável pelos mesmos, inclusive, pelas transações que forem efetuadas em nome do participante no Sistema Eletrônico ou por eventual desconexão.

5.6. **Não poderá participar, direta ou indiretamente**, desta licitação ou da execução dos serviços e do fornecimento de bens a eles necessários:

5.6.1. Os interessados que não atendam às condições deste Edital e seus anexos;

5.6.2. Autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados;

5.6.3. Empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários;

5.6.4. Pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

5.6.4.1. O impedimento de que trata o item 5.6.4. será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

5.6.4.2. Nos termos do art. 42 do Ato nº 008/2024/PGJ "*É vedado ao Ministério Público contratar com pessoas físicas ou jurídicas que em regular processo administrativo foram declaradas impedidas de licitar e contratar com a administração pública direta ou indireta, nas esferas federal, estadual ou municipal, assim como com pessoas físicas ou jurídicas que estão impedidas de contratar com o Poder Público em decorrência de condenação judicial por atos de improbidade administrativa*."

5.6.5. Aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

5.6.6. Empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

5.6.7. Pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

5.6.8. Agente público do órgão ou entidade licitante;

5.6.8.1. A vedação de que trata o item 5.6.8 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

5.6.8.2. É vedada a contratação, durante a vigência do contrato, da prestação de serviço por empregados de empresas fornecedoras de mão de obra que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de dirigente do órgão ou entidade contratante ou de agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato (art. 48, parágrafo único, da Lei de Licitações n. 14.133/2021), de membro ou de servidor do MPAM, nela compreendido o ajuste mediante o acolhimento recíproco para a prestação de serviço entre os Ministérios Públicos ou entre esses e órgãos da Administração Pública direta e indireta dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios, bem como é vedada a realização, manutenção, aditamento ou prorrogação de contrato de prestação de serviços com empresa que tenha entre seus empregados colocados à disposição do Ministério Público para o exercício de funções de chefia, pessoas que incidam nas vedações constantes na Resolução n. 177, de 5 de julho de 2017, do Conselho Nacional do Ministério Público. (Art. 42, §4º do Ato nº 008/2024/PGJ)

5.6.9. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

5.6.10. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei n.º 14.133, de 2021.

5.6.11. Interessado que se encontre em processo de Falência, Recuperação Judicial e Extrajudicial (conforme Lei nº. 11.101/05), salvo decisão judicial em contrário (conforme Acordão 1201/2020 - TCU - PLENÁRIO), concurso de credores, insolvência, dissolução, liquidação, fusão, cisão, incorporação, salvo devidamente justificado;

5.6.12. Interessado(s) em regime de consórcio, qualquer que seja sua forma de constituição, em razão da baixa complexidade de execução do objeto.

5.6.13. Empresa estrangeira não autorizada a funcionar no País e que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

5.7. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 5.6.2 e 5.6.3 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

5.8. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

5.9. O disposto nos itens 5.6.2 e 5.6.3 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

5.10. Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da Lei nº 14.133/2021.

5.11. A **declaração falsa** relativa ao cumprimento dos requisitos de habilitação e proposta **sujeitará o licitante às sanções** previstas neste Edital.

5.12. DA VISTORIA TÉCNICA. Considerando que na presente contratação a avaliação prévia do local de execução é relevante para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, o licitante deve atestar, sob pena de desclassificação, que conhece o local e as condições de realização do serviço, assegurado a ele o direito de realização de vistoria prévia.

5.12.1. As empresas LICITANTES PODERÃO realizar, sob o acompanhamento de servidor especialmente designado, vistoria às unidades da Procuradoria-Geral de Justiça, em data e horário previamente acordados segundo a conveniência deste Órgão, com o objetivo de conhecer as instalações onde serão executados os serviços e sanar as dúvidas porventura existentes, a fim de subsidiar a elaboração das propostas a serem submetidas ao certame.

5.12.2. A vistoria deverá ser realizada por representante devidamente credenciado pela empresa LICITANTE, devidamente municiado de documento próprio de credenciamento, conforme ANEXO VI deste Edital;

5.12.3. A comprovação de realização da vistoria será efetuada por meio de apresentação deAtestado de Vistoria Técnica - conforme modelo constante do ANEXO VII deste Edital, que será emitido pelo interessado, assinado por servidor designado da DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - DTIC desta PGJ/AM;

5.12.4. O Atestado de Vistoria Técnica será assinado por servidor do MPAM que acompanhar a vistoria, e deverá ser encaminhada juntamente com a proposta;

5.12.5 As visitas deverão ser previamente agendadas, com 24 (vinte e quatro) horas de antecedência, pelo telefone (92) 3655-0670/0660 – DTIC, no período das 8h às 14h e poderão ser realizadas em até 2 (dois) dias úteis anteriores à data estipulada para abertura da licitação.

5.13. Caso o licitante opte por não realizar vistoria, poderá substituir a declaração exigida no presente item por uma Declaração de Dispensa de Vistoria Técnica assinada pelo seu responsável técnico acerca do conhecimento pleno das condições e peculiaridades da contratação, nos termos do ANEXO VIII deste Edital, que deverá ser encaminhada juntamente com a proposta;

5.14. Não serão aceitas alegações posteriores advindas de desconhecimento das condições prediais, das características do ambiente de prestação dos serviços ou erro orçamentário por parte da futura contratada, quando da execução dos serviços propostos.

6. DO ENVIO DAS PROPOSTAS E DOS DOCUMENTOS DE HABILITAÇÃO

6.1. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço ou o percentual de desconto, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.

6.1.1. Levando-se em conta as nuances do objeto e da inviabilidade de seu parcelamento, somente serão aceitas propostas para o quantitativo total estimado para cada item.

6.2. Caso a fase de habilitação anteceda as fases de apresentação de propostas e lances, os licitantes encaminharão, na forma e no prazo estabelecidos no item anterior, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto nos itens 7.1.1 e 7.12.1 deste Edital.

6.3. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

6.3.1. está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

6.3.2. não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

6.3.3. não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

6.3.4. cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

6.4. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021.

6.5. O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021.

6.5.1. no item exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item;

6.5.2. nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

6.6. A falsidade da declaração de que trata os itens 6.3. ou 6.5. sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

6.7. O envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.

6.8. Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.

6.9. As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1º da LC nº 123, de 2006.

6.10. Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

6.11. Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema.

6.12. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

6.13. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para

apresentação de propostas, após a fase de envio de lances.

6.14. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá às seguintes regras:

6.14.1. a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

6.14.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo estabelecido e o intervalo de que trata o subitem acima.

6.15. O valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

6.15.1. valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço; e

6.15.2. percentual de desconto inferior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por maior desconto.

6.16. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 6.14. possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

6.17. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

7. DO PREENCHIMENTO DA PROPOSTA

7.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos (no que couber):

7.1.1. Valor unitário e total do item;

7.1.2. Marca;

7.1.3. Fabricante;

7.1.4. Descrição detalhada do objeto, contendo as informações similares à especificação do Termo de Referência: indicando, no que for aplicável, o modelo, prazo de validade ou de garantia, número do registro ou inscrição do bem no órgão competente, quando for o caso, **sem identificação da licitante**;

7.1.4.1. Não serão aceitas propostas escritas contendo especificações que não contenham as informações necessárias à perfeita caracterização do objeto e suas especificidades, bem como especificações vagas e incompletas.

7.2. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

7.3. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

7.4. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

7.5. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

7.6. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

7.7. O **prazo de validade da proposta não será inferior a 90 (noventa) dias**, a contar da data de sua apresentação.

7.8. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais/estaduais, quando participarem de licitações públicas.

7.8.1. Caso o critério de julgamento seja o de maior desconto, o preço já decorrente da aplicação do desconto ofertado deverá respeitar os preços máximos previstos no item 7.8.

7.9. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a fiscalização do Tribunal de Contas do Estado do Amazonas e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

7.10. O CNPJ da proponente, empresa cadastrada no SICAF e habilitada na licitação, deverão ser o mesmo para efeito de emissão das notas fiscais e posterior pagamento.

7.11. Serão irrelevantes quaisquer ofertas que não se enquadrem nas especificações exigidas, ou Anexos não solicitados, considerando-se que pelo preço proposto, a empresa obrigar-se-á a executar os serviços/entregar os produtos descritos neste Edital.

7.12. Para efeito de elaboração das propostas, caso haja divergência entre a especificação contida neste Edital e a no sistema SIASG, prevalecerá a descrita neste Edital.

8. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

8.1. A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

8.2. Um vez aberta a sessão, não será mais possível a substituição da proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema.

8.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

8.4. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

8.5. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

8.6. Os licitantes poderão oferecer lances sucessivos, observando as regras estabelecidas no Edital.

8.6.1. Os lances para grupos serão feitos em telas diferentes da tela principal do envio de lances, para cada item do grupo.

8.6.2. O lance vencedor será o menor lance na soma total dos itens do grupo.

8.6.3. O licitante poderá oferecer lance de **valor inferior ou percentual de desconto superior** ao último por ele ofertado e registrado pelo sistema.

8.6.4. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

8.7. O **critério de julgamento adotado será o menor preço GLOBAL**, conforme definido neste Edital e seus anexos.

8.8. **O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser R$ 10,00 (dez reais)**.

8.9. O intervalo entre os lances enviados pelo mesmo licitante não poderá ser inferior a vinte (20) segundos e o intervalo entre lances não poderá ser inferior a três (3) segundos, sob pena de serem automaticamente descartados pelo sistema os respectivos lances (quando implementado).

8.10. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

8.11. O procedimento seguirá de acordo com o modo de disputa adotado.

8.12. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa "**ABERTO**", os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

8.12.1. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

8.12.2. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

8.12.3. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

8.12.4. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

8.12.5. Após o reinício previsto no item supra, os licitantes serão convocados para apresentar lances intermediários.

8.13. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa "**ABERTO E FECHADO**", os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

8.13.1. A etapa de lances da sessão pública terá duração inicial de quinze minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de tempo de até dez minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

8.13.2. Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

8.13.3. No procedimento de que trata o subitem supra, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

8.13.4. Não havendo pelo menos três ofertas nas condições definidas neste item, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

8.13.5. Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

8.14. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa "**FECHADO E ABERTO**", poderão participar da etapa aberta somente os licitantes que apresentarem a proposta de menor preço/ maior percentual de desconto e os das propostas até 10% (dez por cento) superiores/inferiores àquela, em que os licitantes apresentarão lances públicos e sucessivos, até o encerramento da sessão e eventuais prorrogações.

8.14.1. Não havendo pelo menos 3 (três) propostas nas condições definidas no **item 8.14**, poderão os licitantes que apresentaram as três melhores propostas, consideradas as empatadas, oferecer novos lances sucessivos.

8.14.2. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

8.14.3. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

8.14.4. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

8.14.5. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

8.14.6. Após o reinício previsto no subitem supra, os licitantes serão convocados para apresentar lances intermediários.

8.15. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

8.16. Em caso de falha no sistema, os lances em desacordo com os subitens anteriores deverão ser desconsiderados pelo pregoeiro, devendo a ocorrência ser comunicada imediatamente ao Órgão Gestor do Sistemas de Compras do Governo Federal.

8.16.1. Na hipótese do subitem anterior, a ocorrência será registrada em campo próprio do sistema.

8.17. **Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar**.

8.18. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada à identificação do licitante.

8.19. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

8.20. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a 10 (dez) minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

8.21. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da LC nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

8.21.1. Nessas condições, as propostas de micreoempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

8.21.2. A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

8.21.3. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

8.21.4. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

8.22. **Havendo eventual empate** entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021.

8.22.1. Persistindo o empate após as medidas do item 8.23, o sistema fará um sorteio eletrônico das propostas empatadas, a ser realizado em ato público, para o qual todos os licitantes serão convocados, vedado qualquer outro processo, nos termos da **Instrução Normativa SEGES/ME n.º 73, de 2022.**

8.23. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, o pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

8.23.1. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

8.23.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

8.24. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

9. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

9.1. O pregoeiro solicitará ao licitante melhor classificado que, **no prazo máximo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada**, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

9.1.1. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo

9.2. Na proposta vencedora a ser enviada posteriormente deverá constar, conforme modelo do **Anexo IV**:

a) Os valores, os preços e os custos utilizados terão como expressão monetária a moeda corrente nacional (art. 13º, I, da Lei nº 14.133/2021). Ocorrendo divergência entre os preços unitários e o preço total, prevalecerão os primeiros; no caso de divergência entre os valores numéricos e os valores expressos por extenso, prevalecerão estes últimos.

a.1.) Não será admitido nos preços o fracionamento de centavo que ultrapassar duas casas decimais, desprezando-se sumariamente a fração remanescente;

a.2.) No preço deverão estar incluídas todas as despesas que influam no custo, tais como: impostos, transportes, seguros, taxas e outras despesas necessárias ao fornecimento dos materiais e à execução dos serviços correspondentes;

a.3.) Ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo licitante ou seu representante legal;

a.4.) Não se admitirá, na proposta de preços, custos identificados mediante o uso da expressão "verba" ou de unidades genéricas.

b) **Prazo de validade da proposta de, no mínimo, 90 (noventa) dias corridos**, a contar da data;

c) Especificações claras, completas e minuciosas, com detalhes do objeto ofertado, inclusive marca, modelo, tipo e referência, no que couber, observadas as especificações mínimas e quantitativos contidos neste Edital e anexos;

d) A oferta deverá ser firme e precisa, limitada, rigorosamente, ao objeto deste Edital, sem conter alternativas de preço ou de qualquer outra condição que induza o julgamento a mais de um resultado, sob pena de desclassificação;

e) Prazo de entrega da solução: **Até 60 (sessenta) dias corridos**, contados da assinatura do Contrato, consoante **Item 4.1 do Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562**, *Anexo I* e parte integrando deste Edital;

f) **Prazo de garantia/assistência técnica: pelo período de 60 (sessenta) meses, conforme dispõe o Item 1.1 do Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562**, *Anexo I* e parte integrando deste Edital; **.**

g) Os seguintes dados da licitante: Razão Social, endereço, telefone/fax, número do CNPJ/MF, *e-mail*, se houver, Banco,

agência, número da conta-corrente e praça de pagamento;

h) Nome, CNPJ ou CPF dos **3 (três) principais integrantes do quadro societário da licitante,** assim compreendidos aqueles que detenham maior parcela das cotas societárias ou o poder de gestão da sociedade;

i) Contato para fins de faturamento: (indicar o nome, cargo, endereço, telefone, fax, *e-mail* de contato do responsável pelo recebimento das futuras notas de empenho)**.**

j) Quando solicitada pelo Pregoeiro, **documentação técnica (manuais, catálogos, prospectos, links da fabricante)**, com as características detalhadas (marca, modelo, cor, tipo de material e medidas - no que couber) e imagens ilustrativas dos produtos propostos, que possibilitem a completa averiguação de conformidade com as especificações, visando facilitar a avaliação a ser realizada por técnicos deste Órgão.

9.3. As **Declarações Complementares, referentes ao Anexo III do Edital**, observado as exigências mínimas do Termo de Referência, deverão ser efetuadas no momento da elaboração e envio da proposta pelos fornecedores, em seu próprio conteúdo ou documento apartado, sendo elas que:

a) Cumpre plenamente os requisitos de habilitação, ciente de que responde pela veracidade das informações prestadas, na forma da lei;

b) Em atenção **item 5.6.** e **art. 14.º e seus incisos da Lei n.º 14.133/2021**, não está impedida de participar direta ou indiretamente desta licitação, e ainda, que não possue sócios, diretores ou gerentes, que sejam cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do Ministério Público do Estado do Amazonas e de sua CPL;

c) Recebeu o edital e todos os documentos que o integram, dispondo de todos os elementos e informações necessários à elaboração da proposta de preços com total e completo conhecimento do objeto da licitação;

d) Os documentos e declarações apresentados são fiéis e verdadeiros;

e) Caso seja vencedor do certame e não cadastrado no SISTEMA DE ADMINISTRAÇÃO FINANCEIRA E CONTABILIDADE da SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ-AM, encaminhará a CONTRATANTE os documentos necessários para efetuar o referido cadastramento no prazo de 05 (cinco) dias úteis, a contar da adjudicação, sob pena de perder o direito de preferência à contratação em favor dos demais licitantes subsequentes, sem prejuízo da possibilidade de responder a procedimento administrativo de responsabilização por eventual retardamento da licitação;

f) O preço inclui além do lucro, todos os custos e despesas, com tributos incidentes e encargos devidos, materiais, serviços, transporte, a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas, bem como quaisquer outras despesas diretas e indiretas incidentes na prestação de serviços;

g) Apresentará, quando da contratação, documento que indique o pessoal técnico operacional, das instalações e do aparelhamento adequado e disponíveis para a realização do objeto da licitação, bem como a qualificação de cada membro da equipe técnica que se responsabilizará pelos trabalhos;

h) Submete-se e concorda integralmente com os termos do presente Edital, bem como com seus elementos e especificações, comprometendo-me a cumpri-los fielmente, inclusive no que se refere à fiscalização e ao controle técnico a serem exercidos por profissional expressamente designado para tal finalidade; e

i) A proposta apresentada para participar do presente Pregão foi elaborada de maneira independente por esta licitante e o seu conteúdo não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer outro participante potencial ou de fato, por qualquer meio ou por qualquer pessoa.

9.4. A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do contrato e aplicação de eventual sanção à Contratada, se for o caso.

9.4.1. Todas as especificações do objeto contidas na proposta, tais como marca, modelo, tipo, fabricante e procedência, vinculam a Contratada.

9.5. A proposta deverá obedecer aos termos deste Edital e seus Anexos, não sendo considerada aquela que não corresponda às especificações ali contidas ou que estabeleça vínculo à proposta de outro licitante.

9.6. As propostas que contenham a descrição do objeto, o valor e os documentos complementares estarão disponíveis na *internet*, após a homologação.

10. DA FASE DE JULGAMENTO

10.1. Encerrada a etapa de negociação, o pregoeiro verificará se a licitante provisoriamente classificada em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no **item 5.6.** do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

a) SICAF;

b) Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/ceis); e

c) Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep).

10.1.1. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei n° 8.429, de 1992.

10.1.2. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas. (IN nº 3/2018, art. 29, *caput*)

10.1.3.1.A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros. (IN nº 3/2018, art. 29, §1º).

10.1.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação. (IN nº 3/2018, art. 29, §2º).

10.1.3.3. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

10.1.3. Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

10.1.4. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com os **itens 2.3 e 6.5.** deste edital.

10.1.5. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto nos **itens 10.4 e 10.5** deste Edital.

10.2. A proposta e documentação, se necessário, **será analisada pela equipe da DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - DTIC**, para fins de verificação do atendimento às características e exigências reclamadas no edital e anexos.

10.3. **Será desclassificada a proposta ou lance vencedor que, ressalvado o disposto no subitem 10.7. deste Edital**:

10.3.1. contiver vícios insanáveis;

10.3.2. não obedecer às especificações técnicas contidas no Edital e seus anexos;

10.3.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

10.3.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

10.3.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável;

10.3.6. Também será DESCLASSIFICADA a licitante que no momento do preenchimento do campo de ***"Descrição detalhada do objeto ofertado"*** no Sistema Comprasnet identifique sua empresa, o que não se confunde com a proposta inicial juntada ao Sistema e a proposta final e reajustada após convocação pelo Pregoeiro.

10.4. No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

10.4.1. A inexequibilidade, na hipótese de que trata o ***caput***, só será considerada após diligência do pregoeiro, que comprove:

10.4.1 1. que o custo do licitante ultrapassa o valor da proposta; e

10.4.1.2. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

10.5. Em contratação de serviços de engenharia, além das disposições acima, a análise de exequibilidade e sobrepreço considerará o seguinte:

10.5.1. Nos regimes de execução por tarefa, empreitada por preço global ou empreitada integral, semi-integrada ou integrada, a caracterização do sobrepreço se dará pela superação do valor global estimado;

10.5.2. No regime de empreitada por preço unitário, a caracterização do sobrepreço se dará pela superação do valor global estimado e pela superação de custo unitário tido como relevante, conforme planilha anexa ao edital;

10.5.3. No caso de serviços de engenharia, serão consideradas inexequíveis as propostas cujos valores forem inferiores a 75% (setenta e cinco por cento) do valor orçado pela Administração, independentemente do regime de execução.

10.5.4. Será exigida garantia adicional do licitante vencedor cuja proposta for inferior a 85% (oitenta e cinco por cento) do valor orçado pela Administração, equivalente à diferença entre este último e o valor da proposta, sem prejuízo das demais garantias exigíveis de acordo com a Lei.

10.6. Caso o custo global estimado do objeto licitado tenha sido decomposto em seus respectivos custos unitários por meio de Planilha de Custos e Formação de Preços elaborada pela Administração, o licitante classificado em primeiro lugar será convocado para apresentar Planilha por ele elaborada, com os respectivos valores adequados ao valor final da sua proposta, sob pena de não aceitação da proposta.

10.6.1. Em se tratando de serviços de engenharia, o licitante vencedor será convocado a apresentar à Administração, por meio eletrônico, as planilhas com indicação dos quantitativos e dos custos unitários, seguindo o modelo elaborado pela Administração, bem como com detalhamento das Bonificações e Despesas Indiretas (BDI) e dos Encargos Sociais (ES), com os respectivos valores adequados ao valor final da proposta vencedora, admitida a utilização dos preços unitários, no caso de empreitada por preço global, empreitada integral, contratação semi-integrada e contratação integrada, exclusivamente para eventuais adequações indispensáveis no cronograma físico-financeiro e para balizar excepcional aditamento posterior do contrato.

10.7. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço.

10.7.1. Verificada a presença de erros sanáveis na proposta de preços, o Pregoeiro ou Administração poderá realizar diligência junto à Licitante para a devida correção apenas das falhas apontadas, **limitado a 3 (três) oportunidades**, vedada a juntada de documento novo.

10.7.2. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas.

10.8. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, **24 (vinte e quatro)** horas de antecedência, e a ocorrência será registrada em ata, caso não seja informada na sessão a nova data de reabertura.

10.9. O Pregoeiro poderá convocar o licitante para enviar documento complementar, por meio de funcionalidade disponível no sistema, **no prazo máximo de 02 (duas) horas, sob pena de não aceitação da proposta**.

10.9.1. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no "chat" pelo licitante, antes de findo o prazo.

10.9.2. Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se os que contenham as características do material ofertado, tais como marca, modelo, tipo, fabricante e procedência, além de outras informações pertinentes, a exemplo de catálogos, folhetos ou propostas, encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pelo Pregoeiro, sem prejuízo do seu ulterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta.

10.10. **DA APRESENTAÇÃO DE AMOSTRAS.** Caso o Termo de Referência exija a apresentação de amostra, ou quando solicitado pelo Pregoeiro, o licitante classificado em primeiro lugar deverá apresentá-la, conforme disciplinado no Termo de Referência e Edital, sob pena de não aceitação da proposta.

10.10.1. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a avaliação das amostras, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

10.10.2. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

10.10.3 No caso de não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita pelo Pregoeiro, ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

10.10.4. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), o Pregoeiro analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da(s) amostra(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência.

10.10.5. Se o Termo de Referência não dispor sobre o trâmite da apresentação da amostra, caso seja solicitada a apresentação pelo Pregoeiro, o licitante classificado em primeiro lugar deve apresentá-la, sob pena de não aceitação da proposta, no local a ser indicado e dentro de **05 (cinco) dias úteis** contados da solicitação, observando-se:

10.10.5.1. Para avaliação da qualidade, os bens recebidos serão sujeitos à testes de aceitação. Após o qual, emitirá um relatório completo dos testes efetuados, devidamente assinado. Quando não estabelecido o procedimento no Termo de Referência, os testes serão constituídos das seguintes fases:

a) Abertura das embalagens;

b) Comprovação de que os materiais atendem às especificações mínimas exigidas ou superiores oferecidas;

c) Colocação de amostra dos bens em funcionamento; e

d) Testes funcionais de configuração e desempenho deles.

10.10.5.2. Por meio de mensagem no sistema, será divulgado o local e horário da realização do procedimento para a avaliação das amostras, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

10.10.5.3. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

10.10.5.4. No caso de não haver entrega da amostra ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

10.10.5.5. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), o Pregoeiro analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da(s) amostra(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência.

10.10.5.6. Os exemplares colocados à disposição da Administração serão tratados como protótipos, podendo ser manuseados e desmontados pela equipe técnica responsável pela análise, não gerando direito a ressarcimento.

10.10.5.7. Após a divulgação do resultado final da licitação, as amostras entregues deverão ser **recolhidas pelos licitantes no prazo de 10 (dez) dias corridos,** após o qual poderão ser descartadas ou incorporadas pela Administração, sem direito a ressarcimento.

10.10.5.8. Os licitantes deverão colocar à disposição da Administração todas as condições indispensáveis à realização de testes e fornecer, sem ônus, os manuais impressos em língua portuguesa, necessários ao seu perfeito manuseio, quando for o caso.

10.11. Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

10.12. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a sua continuidade.

10.13. Nos itens não exclusivos para a participação de microempresas e empresas de pequeno porte, sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso.

10.14. A apresentação da proposta implicará a plena aceitação, por parte do licitante, de todas as condições estabelecidas neste Edital e seus anexos, bem como, todas as especificações do objeto contidas na proposta vinculam a Contratada.

10.15. Quando da proposta de preços não constar quaisquer das declarações complementares, os prazos previstos, quer sejam os de garantia, validade dos produtos, validade da proposta ou de entrega, entender-se-á que estão aceitos os constantes do Edital.

10.16. Encerrada a análise quanto à aceitação da proposta, o pregoeiro verificará a habilitação do licitante, observado o disposto neste Edital.

10.17. Decorrido o prazo de validade das propostas, sem convocação para contratação, ficam as licitantes liberadas dos compromissos assumidos, podendo ser consultado acerca da manutenção dos preços ofertados.

11. DA HABILITAÇÃO

11.1. Os documentos previstos no Termo de Referência e neste Edital, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.

11.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira poderá ser substituída pelo registro cadastral no Sicaf.

11.2. Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

11.2.1. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato ou da ata de registro de preços, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

11.3. Quando permitida a participação de consórcio de empresas, a habilitação técnica, quando exigida, será feita por meio do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, quando exigida, será observado o somatório dos valores de cada consorciado.

11.3.1. Se o consórcio não for formado integralmente por microempresas ou empresas de pequeno porte e o termo de referência exigir requisitos de habilitação econômico-financeira, haverá um acréscimo de 10% para o consórcio em relação ao valor exigido para os licitantes individuais.

11.4. **Todos os documentos enviados eletronicamente deverão ser enviados em original, ou por cópia autenticada, devidamente assinado(s) pelo(s) representante(s) legal(is) no dia subsequente ao do resultado da habilitação, impreterivelmente, sob pena de desclassificação**, observado o disposto no **item 23.8.** e seguintes, à Comissão Permanente de Licitação da Procuradoria-Geral de Justiça do Estado do Amazonas, Av. Coronel Teixeira, 7.995, Nova Esperança II, CEP: 69037-473.

11.4.1. Caso a autenticação do documento ou o próprio documento esteja em formato digital, com assinatura por certificado digital, padrão ICP-Brasil, ou ainda torne possível sua convalidação em sítio eletrônico de autoridade certificadora oficial e/ou cartório digital respectivo, a licitante está dispensada da obrigação do item anterior.

11.5. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei nº 14.133/2021.

11.6. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133/2021).

11.7. Será verificado se o licitante apresentou no sistema, sob pena de inabilitação, a declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

11.8. O licitante deverá apresentar, sob pena de desclassificação, declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

11.9. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

11.9.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir.

11.10. É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

11.10.1. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

11.11. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

11.11.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de **02 (duas) horas**, prorrogável por igual período, contado da solicitação do pregoeiro.

11.11.2. Na hipótese de a fase de habilitação anteceder a fase de apresentação de propostas e lances, os licitantes encaminharão, por meio do sistema, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto.

11.12. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

11.12.1. Os documentos relativos à regularidade fiscal que constem do Termo de Referência somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

11.12.2. Respeitada a exceção do subitem anterior, relativa à regularidade fiscal, quando a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, a verificação ou exigência do presente subitem ocorrerá em relação a todos os licitantes.

11.13. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (Lei 14.133/21, art. 64):

11.13.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

11.13.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

11.14. Na análise dos documentos de habilitação, o Pregoeiro ou a comissão de contratação poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

11.15. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital.

11.16. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

11.17. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, e não como condição para participação na licitação (art. 4º do Decreto nº 8.538/2015).

11.18. Quando a fase de habilitação anteceder a de julgamento e já tiver sido encerrada, não caberá exclusão de licitante por motivo relacionado à habilitação, salvo em razão de fatos supervenientes ou só conhecidos após o julgamento.

11.19. Os documentos necessários à habilitação deverão estar com prazo vigente, à exceção daqueles que por sua natureza, não contenham validade, e poderão ser apresentados em original, por qualquer processo de cópia autenticada por tabelião de notas ou por servidor da CPL, ou por publicação em órgãos da imprensa oficial, **não sendo aceitos "protocolos" ou solicitação de documento em substituição aos documentos requeridos neste Edital**.

11.20. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

11.20.1. Serão aceitos registros de CNPJ de licitante matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

11.21. Ressalvado o disposto no subitem **6.3.**, os licitantes deverão encaminhar, nos termos deste Edital, a documentação relacionada nos itens a seguir, para fins de habilitação.

11.22. Relativos à Habilitação Jurídica:

11.22.1. No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

11.22.2. Em se tratando de microempreendedor individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio http://www.portaldoempreendedor.gov.br;

11.22.3. No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

11.22.4. Inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência;

11.22.5. No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

11.22.6. No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização;

11.22.7. Os documentos relativos à Habilitação Jurídica indicados, deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

11.23. Relativo à Regularidade Fiscal e Trabalhista:

11.23.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso.

11.23.2. Prova de regularidade perante a Fazenda federal, estadual e/ou municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei.

11.23.3. Prova de regularidade relativa à Seguridade Social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei;

11.23.4. Prova de regularidade perante a Justiça do Trabalho;

11.23.5. Declaração de cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal, conforme declaração do sistema;

11.23.6. Caso o licitante detentor do menor preço seja qualificado como microempresa ou empresa de pequeno porte deverá apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição, sob pena de inabilitação.

11.23.7. A aceitação de certidões emitidas via *internet* ficará sujeita à confirmação de sua validade mediante consulta *on line* ao cadastro emissor respectivo.

11.23.8. Caso o licitante seja considerado isento dos tributos estaduais/municipais relacionados ao objeto licitatório, deverá comprovar tal condição mediante declaração da Fazenda Estadual do seu domicílio ou sede, ou outra equivalente, na forma da lei;

11.23.9. Os documentos referidos nos subitens acima poderão ser substituídos ou supridos, no todo ou em parte, por outros meios hábeis a comprovar a regularidade do licitante, inclusive por meio eletrônico (§1.º, art. 68, da Lei 14.133/21);

11.23.10. A comprovação de atendimento do disposto nos subitens 11.23.2, 11.23.3 e 11.23.11. deverá ser feita na forma da legislação específica (§2.º, art. 68, da Lei 14.133/21);

11.24. Relativos à Qualificação Econômico-Financeira:

11.24.1. Balanço patrimonial e demonstrações contábeis dos 2 (dois) últimos exercícios sociais, já exigíveis e apresentados na forma da lei, podendo ser apresentado de acordo com o Sistema Público de Escrituração Digital (SPED – Decreto Federal n.º 6.022/2007), que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta;

11.24.1.1. O Balanço apresentado deverá cumprir as seguintes formalidades:

a) Assinatura do contador e do titular ou representante legal da empresa no balanço patrimonial e DRE (pode ser feita digitalmente);

b) Prova de registro na Junta Comercial ou Cartório (devidamente carimbado, com etiqueta, chancela da Junta Comercial ou código de registro).

11.24.1.2. No caso de fornecimento de bens para pronta entrega, não será exigido da licitante qualificada como microempresa ou empresa de pequeno porte, a apresentação de balanço patrimonial do último exercício financeiro. (Art. 3º do Decreto nº 8.538, de 2015);

11.24.1.3. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e ficarão autorizadas a substituir os demonstrativos contábeis pelo balanço de abertura;

11.24.1.4. Quando solicitado ou autorizado pelo Pregoeiro, será permitido apresentação de balanço intermediário, desde que se decorra de lei ou contrato social/estatuto social da Licitante.

11.24.1.5. A comprovação da situação financeira da empresa será constatada mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um) resultantes da aplicação das fórmulas e Patrimônio Líquido mínimo de 10% do valor estimado da proposta de preços ou do item pertinente.

11.24.3. Certidões Negativas de Falência e Recuperação Judicial (conforme Lei nº 11.101/05), expedida pela Central de Certidões do Tribunal de Justiça ou órgão equivalente do domicílio ou da sede do licitante, **expedida até 90 (noventa) dias antes da abertura desta licitação**, quando do documento não constar data expressa de validade;

11.24.3.1 Onde não houver **CENTRAL DE CERTIDÕES DO TRIBUNAL DE JUSTIÇA**, deverá ser apresentada Certidão emitida pela **SECRETARIA DO TRIBUNAL DE JUSTIÇA** ou órgão equivalente do domicílio ou da sede do licitante constando a quantidade de Cartórios Oficiais de Distribuição de Pedidos de Falência e Recuperação Judicial (conforme Lei nº 11.101/05), devendo ser apresentadas Certidões expedidas na quantidade de cartórios indicadas no respectivo documento, no prazo referido no item **11.24.3.**;

11.24.3.2. Caso os prazos de validade não constem expressamente das certidões, serão considerados para esse fim, o prazo descrito no subitem **11.24.3**. deste instrumento convocatório.

11.24.4. Os documentos referidos no item **11.24. e subitens** limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos

11.25. Relativos à Qualificação Técnica

11.25.2. **Apresentação de Atestado de Capacidade Técnica** (Art. 67, II, da Lei 14.133/21) fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado, que comprove(m) que a empresa licitante tenha executado/entregue, a contento, serviços/materiais de natureza e vulto compatíveis com o presente objeto, que permitam estabelecer, por comparação, proximidade de características funcionais técnicas, dimensionais, quantitativas e qualitativas com o objeto do presente Edital, sendo aceitável a soma de atestados para a comprovação desse quantitativo, conforme Termo de Referência**.**

11.25.1.1. Para fins de comprovação de aptidão, serão considerados compatíveis com objeto, os atestados de capacidade técnica que comprovem o fornecimento concomitante do objeto licitado ou do item vencido.

11.25.1.2. No caso de pessoa jurídica de direito público, o(s) atestado(s) ou certidão (ões) deverá (ão) ser assinado(s) pelo

responsável do setor competente do órgão;

11.25.1.3. No caso de pessoa jurídica de direito privado, o(s) atestado(s) deverá(ão) conter dados suficientes para identificação civil do declarante, com referência ao cargo/função que ocupa na empresa.

11.25.1.4. A ausência de apresentação de atestado claro, legível e idôneo, em não conformidade com este Edital, será motivo de inabilitação, a critério do Pregoeiro.

11.26. Disposições Gerais da Habilitação:

11.26.1. O licitante enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado: (a) da prova de inscrição nos cadastros de contribuintes estadual e municipal.

11.26.2. Se a documentação de habilitação não estiver completa e correta ou contrariar qualquer dispositivo deste Edital e seus Anexos, **o pregoeiro considerará o proponente inabilitado**, sendo convocado outro licitante, observada a ordem de classificação, e assim **sucessivamente**, sem prejuízo das sanções legais cabíveis.

11.26.3. Sob pena de inabilitação os documentos apresentados deverão estar em nome da licitante, com o nº do CNPJ e o endereço respectivo, conforme segue:

11.26.3.1. se a licitante for a matriz, todos os documentos deverão estar em nome da matriz, e

11.26.3.2. se a licitante for a filial, todos os documentos deverão estar em nome da filial.

11.11.3.3. no caso dos subitens anteriores, serão dispensados da filial aqueles documentos que COMPROVADAMENTE, forem emitidos SOMENTE em nome da matriz, e vice-versa.

11.26.4. Caso os prazos de validade não constem expressamente das certidões apresentadas, será considerado para esse fim, o prazo descrito no subitem **11.24.3**. deste instrumento convocatório.

11.27. Havendo alguma restrição na comprovação da regularidade fiscal para microempresas e empresas de pequeno porte, lhes será assegurado o prazo de 05 (cinco) dias úteis, a contar do momento em que o licitante for declarado vencedor, prorrogáveis por igual período, a requerimento da interessada e a critério da Administração Pública, para a regularização da documentação, pagamento ou parcelamento do débito e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.

11.27.1. A não-regularização fiscal e trabalhista no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação. Se, na ordem de classificação, seguir-se outra microempresa, empresa de pequeno porte ou sociedade cooperativa com alguma restrição na documentação fiscal e trabalhista, será concedido o mesmo prazo para regularização.

11.28. Para fins de julgamento da habilitação no certame, considerar-se-á vigente o documento com prazo de validade, pelo menos, até a data de abertura da licitação.

11.29. Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a continuidade da mesma.

11.30. Nos itens não exclusivos a microempresas e empresas de pequeno porte, em havendo inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45, da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

11.31. O licitante provisoriamente vencedor em um item, que estiver concorrendo em outro item, ficará obrigado a comprovar os requisitos de habilitação cumulativamente, isto é, somando as exigências do item em que venceu às do item em que estiver concorrendo, e assim sucessivamente, sob pena de inabilitação, além da aplicação das sanções cabíveis.

11.31.1. Não havendo a comprovação cumulativa dos requisitos de habilitação, a inabilitação recairá sobre o(s) item(ns) de menor(es) valor(es) cuja retirada(s) seja(m) suficiente(s) para a habilitação do licitante nos remanescentes.

11.32. Atendidas as exigências habilitatórias fixadas neste Edital, o licitante será declarado **vencedor**, sendo-lhe adjudicado o objeto do certame, caso não haja interposição de recursos, encaminhando-se, em seguida os autos à autoridade competente para homologação.

11.33. Da sessão pública será lavrada ata circunstanciada, que mencionará todos os licitantes, a classificação dos lances, bem como as ocorrências que interessarem ao julgamento desta licitação.

12. DOS RECURSOS ADMINISTRATIVOS

12.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

12.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.

12.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

12.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

12.3.2. o prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos.

12.3.2. o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

12.3.3. na hipótese de adoção da inversão de fases prevista no§ 1º do art. 17 da Lei nº 14.133, de 2021, o prazo para apresentação das razões recursais será iniciado na data de intimação da ata de julgamento.

12.3.4. Os recursos deverão ser encaminhados em campo próprio do sistema.

12.3.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de **3 (três) dias úteis**, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

12.4. Os recursos interpostos fora do prazo não serão conhecidos.

12.5. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de**3 (três) dias úteis**, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

12.6. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão

final da autoridade competente.

12.7. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

12.8. Os autos do processo permanecerão com vista franqueada aos interessados na **COMISSÃO PERMANENTE DE LICITAÇÃO**, localizada na Av. Coronel Teixeira, n.º 7.995, Nova Esperança, CEP.: 69037-473, nos dias úteis, no horário das 8h às 14h (horário local).

12.8.1. Os interessados poderão solicitar cópia dos autos por meio do e-mail licitacao@mpam.mp.br

12.9. Não serão providos recursos de caráter protelatório, fundada em mera insatisfação da licitante, podendo ainda ser aplicado, supletiva e subsidiariamente, no que couberem, as regras previstas na Lei n.º 13.105/2015 (Código de Processo Civil).

12.10. A alegação de preço inexequível por parte de uma das licitantes com relação à proposta de preços de outra licitante deverá ser devidamente comprovada.

12.11. A sessão pública do pregão somente será concluída após declarado o vencedor do certame e encerrado o prazo para manifestação de intenção de interposição de recurso, cabendo aos licitantes permanecerem conectados ao sistema até o final desta etapa.

12.12. Decididos os recursos, a autoridade competente fará a adjudicação do objeto da licitação ao licitante vencedor.

13. DA REABERTURA DA SESSÃO PÚBLICA

13.1. A sessão pública poderá ser reaberta:

13.1.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

13.1.2. Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal e trabalhista, nos termos do art. 43, §1º da LC nº 123/2006. Nessas hipóteses, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

13.2. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

13.2.1. A convocação se dará por meio do sistema eletrônico (“chat”) ou ainda, *e-mail*, de acordo com a fase do procedimento licitatório.

13.2.2. A convocação feita por *e-mail* dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

14. DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

14.1. O objeto da licitação será adjudicado e homologado ao licitante declarado vencedor pela autoridade competente.

14.2. Homologado o resultado, o adjudicatário, quando convocado a comparecer, terá o **prazo máximo de 5 (cinco) dias úteis**, para celebrar o contrato ou retirar o instrumento equivalente, devendo manter as condições de habilitação exibidas na licitação.

14.2.1. Se o vencedor do certame não apresentar situação regular no ato da assinatura do contrato (ou retirada do instrumento equivalente), ou recusar-se a assiná-lo, ou sobrevier fato impeditivo de sua celebração, a sessão será retomada e os demais licitantes chamados, procedendo-se na forma do item **10.11**., sem prejuízo das sanções cabíveis.

14.2.2. O vencedor do certame deverá apresentar ao órgão interessado, antes da assinatura do contrato (ou retirada do instrumento equivalente), nova proposta de preços escrita, com a devida recomposição dos custos unitários decorrentes da diminuição dos valores na fase de lances.

14.3. A homologação do resultado desta licitação não implicará direito à contratação.

15. DOS PRAZOS E CONDIÇÕES DE ENTREGA E RECEBIMENTO

15.1. As informações suficientes à execução do objeto constituem os **ITENS 4 e 6** do **TERMO DE REFERÊNCIA Nº 28.2025.DTIC.2002143.2025.007562**, Anexo I deste Edital.

15.2. O recebimento dos materiais/serviços será realizado pela fiscalização da CONTRATANTE.

16. O TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

16.1. Após a homologação da licitação, em sendo realizada a contratação, será firmado Termo de Contrato ou emitido instrumento equivalente.

16.1.1. O adjudicatário **terá o prazo de 5 (cinco) dias úteis**, contados a partir da data de sua convocação, para assinar o Termo de Contrato ou aceitar o instrumento equivalente, conforme o caso (Nota de Empenho/Carta Contrato/Autorização), sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

16.1.1.1. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato ou aceite do instrumento equivalente, a Administração poderá encaminhá-lo para assinatura ou aceite da adjudicatária, mediante correspondência eletrônica no *e-mail* constante da proposta, para que seja assinado eletronicamente pelo Sistema SEI ou aceito no prazo de 5 (cinco) dias, a contar da data de seu recebimento.

16.1.1.2. O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração;

16.1.1.3. Nos termos do art. 6º, do Decreto n º 40.674/2019, o termo contratual ou instrumento equivalente poderá ser assinado por certificação digital ou mediante assinatura eletrônica via Sistema Eletrônico de Informação - SEI, conforme

disposição do ATO Nº 141/2017/PGJ;

16.1.1.3.1. O uso da senha de acesso ao Sistema Eletrônico de Informação - SEI é de **inteira e exclusiva responsabilidade da licitante**, incluindo qualquer acesso efetuado diretamente ou por seu representante, não cabendo ao MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS, promotora da licitação, **qualquer responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.**

16.1.1.4. Para fins do atendimento do disposto no item anterior, antes da assinatura da Ata de Registro de Preços – ARP, será solicitado do representante da fornecedora o preenchimento de cadastro disponível no endereço eletrônico: https://sei.mpam.mp.br/sei/controlador_externo.php?acao=usuario_externo_logar&id_orgao_acesso_externo=0 e envio dos seguintes documentos:

I – Documento de identidade;

II – Cadastro de Pessoa Física – CPF;

III – Comprovante de residência atualizado;

IV – Ato constitutivo e suas alterações, devidamente registrados; e

V – Ato de nomeação ou eleição de dirigentes ou procuração, quando for o caso, devidamente registrados.

16.1.1.5. Será dispensado da apresentação dos documentos referidos o representante que já os tiver enviado durante a sessão pública do pregão.

16.1.1.6. Ao assinar o termo contratual ou instrumento equivalente, a empresa adjudicatária obriga-se a fornecer/executar os bens/serviços a ela adjudicados, conforme especificações e condições contidas neste Edital, em seus Anexos e também na proposta apresentada, prevalecendo, no caso de divergência, as especificações e condições do Edital;

16.2. O aceite da Nota de Empenho ou do instrumento equivalente, emitida à empresa adjudicada, implica no reconhecimento de que:

16.2.1 referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 14.133, de 2021;

16.2.2. a CONTRATADA se vincula à sua proposta e às previsões contidas no Edital e seus Anexos;

16.2.3. a CONTRATADA reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 137 e 138 da Lei nº 14.133, de 2021, e reconhece os direitos da Administração previsto no artigo 139 da mesma Lei.

16.3. Previamente à contratação, a Administração realizará consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018, e nos termos do art. 6º, III, da Lei nº 10.522, de 19 de julho de 2002, consulta prévia ao CADIN.

16.4. Na assinatura do contrato ou da Ata de Registro de Preços, será exigida a comprovação das condições de habilitação consignadas no Edital, que deverão ser mantidas pelo licitante durante a vigência do contrato ou da Ata de Registro de Preços.

16.5. Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no Edital ou se recusar a assinar o contrato ou a Ata de Registro de Preços, a Administração, sem prejuízo da aplicação das sanções das demais cominações legais cabíveis a esse licitante, poderá convocar outro licitante, respeitada a ordem de classificação, para, após a comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o Contrato ou a Ata de Registro de Preços.

16.6. **DA GARANTIA CONTRATUAL**. Nos termos do art. 96 da Lei n.º 14.133/2021, para segurança do integral cumprimento do contrato, a **CONTRATADA** apresentará garantia de **5% (cinco por cento)** do valor total do contrato, observadas as disposições da Cláusula Décima Quarta da Minuta de Contrato Administrativo Nº69.2025.DCCON - CONTRATOS.2033432.2025.007562, Anexo II deste Edital.

17. DAS OBRIGAÇÕES DA CONTRATADA

17.1. As obrigações da CONTRATADA constituem o **Item 7.1 do Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562**, bem como a **Cláusula Décima Primeira da Minuta de Contrato Administrativo Nº 69.2025.DCCON - CONTRATOS.2033432.2025.007562,** *Anexos I e II* deste Edital, respectivamente.

17.2. Se a licitante vencedora não apresentar situação de regularidade documental, no ato da emissão da nota de empenho, ou recusar-se injustificadamente a receber a nota de empenho no prazo estabelecido, os demais licitantes serão convocados observada a ordem de classificação, e assim sucessivamente, sem prejuízo da aplicação das sanções cabíveis.

17.2.1. O prazo de convocação poderá ser prorrogado uma vez, por igual período, quando solicitado pela vencedora durante o seu transcurso, desde que ocorra motivo justificado e aceito pela Administração.

17.3. A empresa deverá encaminhar, quando solicitado, via *e-mail*, os seguintes dados: Banco, agência e número da conta corrente, endereço, telefone e representante legal da empresa, com o número do CNPJ e Inscrição Estadual ou Inscrição Municipal.

18. DAS OBRIGAÇÕES DA CONTRATANTE

18.1. As obrigações da CONTRATANTE constituem o **Item 7.2 do Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562**, bem como a **Cláusula Décima da Minuta de Contrato Administrativo Nº 69.2025.DCCON - CONTRATOS.2033432.2025.007562**, *Anexos I e II* deste Edital, respectivamente.

19. DO PAGAMENTO

19.1 O pagamento resultante da contratação do objeto será efetuado de acordo com o **Item 10** do **Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562**, bem como a Cláusula Décima Sétima da **Minuta de Contrato Administrativo Nº 69.2025.DCCON - CONTRATOS.2033432.2025.007562**, *Anexos I e II* deste Edital, respectivamente, em consonância, também, com a proposta de preços aceita pela Administração.

19.2. O pagamento devido à CONTRATADA será creditado em conta corrente por meio de ordem bancária, efetuado mediante

apresentação de nota fiscal/fatura atestada e visada pelos órgãos de fiscalização e acompanhamento do fornecimento do material.

19.2.1. Os prazos e condições de pagamento são as estabelecidos no Art. 140 do Ato nº 008/2024/PGJ:

I - 10 (dez dias) úteis para a liquidação da despesa, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração;

II - 10 (dez dias) úteis para pagamento, a contar da liquidação da despesa.

19.2.1.1. Para os fins de liquidação, deverá ser observado o disposto no art. 63 da Lei nº 4.320, de 17 de março de 1964, certificando-se do adimplemento da obrigação do contratado nos prazos e forma previstos no contrato.

19.2.1.2. O prazo de que trata o inciso I do caput do Art. 140 do Ato nº 008/2024/PGJ poderá ser excepcionalmente prorrogado, justificadamente, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

19.2.1.3. O prazo para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins de que trata o inciso I do caput e o § 2º do Art. 140 do Ato nº 008/2024/PGJ.

19.2.1.4. Na hipótese de caso fortuito ou força maior que impeça a liquidação ou o pagamento da despesa, o prazo para o pagamento será suspenso até a sua regularização, devendo ser mantida a posição da ordem cronológica que a despesa originalmente estava inscrita.

19.2.1.5. No caso de insuficiência de recursos financeiros disponíveis para quitação integral da obrigação, poderá haver pagamento parcial do crédito, permanecendo o saldo remanescente na mesma posição da ordem cronológica.

19.2.2. As respectivas notas fiscais/faturas, emitidas em conformidade com o Protocolo ICMS 42/2009 (NF-e), deverão estar devidamente discriminadas, em nome da **PROCURADORIA-GERAL DE JUSTIÇA, CNPJ nº 04.153.748/0001-85**, e acompanhada das respectivas Certidões Negativas de Débito para com a Seguridade Social, para com o Fundo de Garantia por Tempo de Serviço, junto à Justiça Trabalhista e, ainda, das certidões de regularidade junto à Fazenda Federal, Estadual e Municipal, conforme descrito no link: https://www.mpam.mp.br/servicos-sp261893274/licitacoes/34-licitacoes/paginas-internas-licitacoes/2148-orientacaopagamentofornecedor;

19.2.3. Deverão constar das Notas Fiscais as especificações dos serviços, o número da Nota de Empenho e do instrumento contratual correspondente, conforme o caso;

19.2.4. Enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência contratual, nenhum pagamento será efetuado à Contratada, sem que isso gere direito a acréscimos de qualquer natureza.

19.3. Qualquer atraso ocorrido na apresentação da nota fiscal/fatura, ou dos documentos exigidos como condição de pagamento por parte da CONTRATADA, importará prorrogação automática do prazo de vencimento da obrigação do Contratante.

19.4. Nenhum pagamento isentará o fornecedor das responsabilidades atinentes ao objeto contratual, nem tampouco implicará a aprovação definitiva da entrega, total ou parcialmente.

19.5. A nota fiscal (atestada) e os documentos exigidos no Edital e no contrato, para fins de liquidação e pagamento das despesas, deverão ser entregues, exclusivamente, no Setor de Protocolo da CONTRATANTE.

19.6. Como condição para emissão da nota de empenho, a licitante vencedora deverá manter as condições de habilitação, cuja confirmação será feita através de consulta ao SICAF ou através da internet nos respectivos sites dos órgãos emissores das certidões de regularidade fiscal.

19.7. Se a licitante vencedora não apresentar situação de regularidade documental, no ato da emissão da nota de empenho, ou se recusar injustificadamente a recebê-la no prazo estabelecido, os demais licitantes serão convocados, observada a ordem de classificação, e assim sucessivamente, sem prejuízo da aplicação das sanções cabíveis.

19.7.1. Como condição inafastável a que seja emitida Nota de Empenho à Fornecedora, esta deverá, também, estar cadastrada junto ao Sistema de Administração Financeira e Contabilidade – Cadastramento de Credores – da Secretaria da Fazendo do Estado do Amazonas – SEFAZ.

19.7.1.1. Com relação ao Cadastramento de Credores, a empresa deverá providenciar o envio dos documentos abaixo elencados ao órgão promotor da licitação (MPAM), durante o certame no próprio Sistema *Comprasnet* na fase de envio da proposta, quando convocado pelo Pregoeiro ou posteriormente após a adjudicação para o endereço eletrônico licitacao@mpam.mp.br, sendo que naquele primeiro momento não será motivo para sua desclassificação:

a) Carta solicitando o cadastramento (conforme **Anexo V)**;

b) Comprovante de inscrição e de situação cadastral emitido pela Receita Federal do Brasil;

c) Cópia legível dos dados bancários (por ex: extrato, cópia reprográfica de cartão bancário etc.);

d) Comprovante de endereço, tais como: conta de água, energia, gás, serviços de internet ou contrato de aluguel.

19.7.1.2. Caso a vencedora não realize o **cadastro em até 5 (cinco) dias úteis** após a homologação do certame, poderá responder a procedimento de apuração de responsabilidade por eventual retardamento da execução do ajuste, com possível aplicação das sanções previstas neste Edital, bem como perda do direito de preferência à contratação em favor dos demais licitantes subsequentes.

20. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

20.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

20.1.1. deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a pregoeiro/a durante o certame;

20.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

20.1.2.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

20.1.2.2. recusar-se a enviar o detalhamento da proposta quando exigível;

20.1.2.3. pedir para ser desclassificado quando encerrada a etapa competitiva; ou

20.1.2.4. deixar de apresentar amostra;

20.1.2.5. apresentar proposta ou amostra em desacordo com as especificações do edital;

20.1.3. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

20.1.3.1. recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

20.1.4. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;

20.1.5. fraudar a licitação;

20.1.6. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

20.1.6.1. agir em conluio ou em desconformidade com a lei;

20.1.6.2. induzir deliberadamente a erro no julgamento;

20.1.6.3. apresentar amostra falsificada ou deteriorada;

20.1.7. praticar atos ilícitos com vistas a frustrar os objetivos da licitação

20.1.8. praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

20.2. Com fulcro na Lei nº 14.133, de 2021, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

20.2.1. advertência;

20.2.2. multa;

20.2.3. impedimento de licitar e contratar e

20.2.4. declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

20.3. Na aplicação das sanções serão considerados:

20.3.1. a natureza e a gravidade da infração cometida.

20.3.2. as peculiaridades do caso concreto

20.3.3. as circunstâncias agravantes ou atenuantes

20.3.4. os danos que dela provierem para a Administração Pública

20.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

20.4. A multa será recolhida em percentual de 0,5% (cinco décimos por cento) a 30% (trinta por cento) incidente sobre o valor do contrato licitado, recolhida no prazo máximo de 5 (cinco) dias úteis, a contar da comunicação oficial.

20.4.1. Para as infrações previstas nos itens 20.1.1., 20.1.2. e 20.1.3., a multa será de 0,5% (cinco décimos por cento) a 15% (quinze por cento) do valor do contrato licitado.

20.4.2. Para as infrações previstas nos itens 20.1.4., 20.1.5., 20.1.6., 20.1.7. e 20.1.8., a multa será de 15% (quinze por cento) a 30% (trinta por cento) do valor do contrato licitado.

20.5. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

20.6. Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

20.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 22.1.1., 22.1.2. e 22.1.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito do **ESTADO DO AMAZONAS**, pelo prazo máximo de 3 (três) anos.

20.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 20.1.4, 20.1.5, 20.1.6, 20.1.7 e 20.1.8, bem como pelas infrações administrativas previstas nos itens 20.1.1, 20.1.2 e 20.1.3 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.

20.9. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 20.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor da Procuradoria-Geral de Justiça.

20.10. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

20.11. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

20.12. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

20.13. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

20.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

20.15. O disposto nos itens acima também se aplica aos integrantes do cadastro de reserva, em pregão para registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente ou com justificativa recusada pela Administração Pública.

20.16. As sanções serão aplicadas pela **AUTORIDADE COMPETENTE**, em processo regular que assegure ao acusado o direito prévio da citação, do contraditório e da ampla defesa, com os recursos a ela inerentes.

20.17. As penalidades serão obrigatoriamente publicadas no Diário Eletrônico do Ministério Público do Estado do Amazonas e

registradas no Sistema de Cadastramento Unificado de Fornecedores – SICAF.

20.18. Se a CONTRATADA, sem justa causa, não cumprir as obrigações assumidas ou infringir preceitos legais, serão aplicadas as sanções previstas no **Item 8 do Termo de Referência n.º 28.2025.DTIC.2002143.2025.007562**, bem como n a s **Cláusulas Décima Nona e Vigésima da Minuta de Contrato Administrativo Nº 69.2025.DCCON - CONTRATOS.2033432.2025.007562,** Anexos I e II, respectivamente, deste instrumento convocatório, segundo a gravidade da falta, observando-se os limites estabelecidos no **subitem 20.4.**

20.19. A inexecução total ou parcial do contrato enseja a sua rescisão pelos motivos legais.

20.20. Se a multa for de valor superior ao valor da garantia prestada, além da perda desta, responderá a CONTRATADA pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela CONTRATANTE ou ainda, quando for o caso, cobrada judicialmente.

20.20.1. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, o Estado ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

20.21. Se, durante o processo de aplicação de penalidade, houver indícios de prática de infração administrativa tipificada pelaLei nº 12.846, de 1º de agosto de 2013, como ato lesivo à Administração Pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização – PAR.

20.22. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

20.23. O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Estadual resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

22.24. O fluxo procedimental quanto ao procedimento preliminar e o processo de apuração de responsabilidade visando a aplicação das sanções administrativas no âmbito do Ministério Público do Estado do Amazonas está disciplinado no Ato PGJ n.º 217/2024 (publicado no DOMPE, Ed. 2874, de 02.07.2024).

21. DA REPACTUAÇÃO, REAJUSTE E REVISÃO DE PREÇO

21.1. A interessada deverá protocolar o seu pedido de repactuação, reajuste e revisão de preços antes da assinatura do contrato ou, nos casos em que este vier a ser substituído por instrumento equivalente, **em até 5 (cinco) dias do recebimento da Nota de Empenho**, sob pena de não apreciação do pedido por intempestividade.

21.1.1. Deverá constar do pedido a planilha de custos e documentos comprovantes da situação superveniente, decorrente de caso fortuito ou de força maior.

21.1.2. A CONTRATADA deverá demonstrar de maneira clara a composição do preço de cada item constante de sua proposta, através de Planilha de Custos contendo, por exemplo: as parcelas relativas à mão de obra direta, demais insumos, encargos em geral, lucro e participação percentual em relação ao preço final.

21.1.3. O pedido deverá vir instruído com os seguintes documentos/informações:

a) Planilha ou equivalente, contendo o custo (preço de custo, impostos, frete, lucro) de cada item constante da proposta inicial em confronto com a nova planilha atualizada, a fim de comprovar a elevação dos encargos do particular;

b) Demonstração de forma cabal que o desequilíbrio decorre de fato superveniente, isto é, ocorrência de evento posterior à apresentação da proposta;

c) Vínculo de causalidade entre o evento ocorrido e a majoração dos encargos da empresa;

d) Comprovação de que o desequilíbrio decorre de fato, imprevisível ou previsível, porém de consequências incalculáveis, apresentado, para tanto TODOS os documentos que comprovem a imprevisibilidade da ocorrência do evento (notas fiscais, cotações e etc.);

e) Memória de cálculo em conformidade com a variação pleiteada, por item;

f) Demonstração de que o desequilíbrio de fato alheio à vontade das partes.

21.2. A não-apresentação da planilha de custos impossibilitará o **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS** de proceder o reequilíbrio, reajuste ou revisão de preços, caso venha a empresa contratada solicitar qualquer uma dessas alterações no contrato.

21.3. A cada pedido de reequilíbrio, reajuste ou revisão de preço, deverá a contratada comprovar e justificar as alterações havidas na planilha apresentada à época da elaboração da proposta, demonstrando a nova composição do preço.

21.4. No caso de o detentor do registro de preços/contratado ser revendedor ou representante comercial deverá demonstrar de maneira clara a composição do preço constante de sua proposta, com descrição das parcelas relativas ao valor de aquisição do produto com notas fiscais de fábrica/indústria, encargos em geral, lucro e participação percentual de cada item em relação ao preço final *(planilha de custos)*.

21.5. **A critério do MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS, poderá ser exigido da contratada, listas de preços expedidas pelos fabricantes**, que conterão, obrigatoriamente, a data de início de sua vigência e numeração sequencial, para instrução de pedidos de revisão de preços.

21.6. Na análise do pedido de reequilíbrio, reajuste ou revisão, dentre outros critérios, o **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS** adotará, para verificação dos preços constantes dos demonstrativos que acompanhem o pedido, pesquisa de mercado dentre empresas de reconhecido porte mercantil, produtoras e /ou comercializadoras, a ser realizada pela própria unidade ou por instituto de pesquisa, utilizando-se, também, de índices setoriais ou outros adotados pelo Governo Estadual, devendo a deliberação de deferimento ou indeferimento da alteração solicitada ser instruída com justificativa da escolha do critério e memória dos respectivos cálculos, para decisão da Administração.

21.7. O percentual de diferença entre os preços de mercado vigentes à época do julgamento da licitação, devidamente apurado, e os propostos pela CONTRATADA/Detentora do registro de preços será mantido durante toda a vigência do registro. **O percentual não poderá ser alterado de forma a configurar reajuste econômico durante a vigência deste registro**.

21.8. A repactuação, reajuste ou revisão do preço, caso deferido, somente terá validade a partir da data da publicação da deliberação na Imprensa Oficial.

21.9. É vedado à contratada interromper o fornecimento ou a prestação do serviço enquanto aguarda o trâmite do

processo de reequilíbrio, reajuste ou revisão de preços, estando, neste caso, sujeita às sanções previstas neste Edital.

21.10. A repactuação, reajuste ou revisão levará em consideração preponderantemente as normas legais federais e estaduais, que são soberanas à previsão do conteúdo exposto neste item.

22. DOS ESCLARECIMENTOS E DA IMPUGNAÇÃO DO ATO CONVOCATÓRIO

22.1. **Até o dia 13/01/2026, 03 (três) dias úteis antes da data designada para a abertura da sessão pública, qualquer pessoa poderá IMPUGNAR** este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, mediante **petição**, que deverá obrigatoriamente (art. 10, caput, da Lei nº 12.527/2011) conter a identificação do Impugnante (CPF/CNPJ).

22.2. Os pedidos de **ESCLARECIMENTOS** referentes a este processo licitatório deverão ser enviados ao Pregoeiro, **até o dia 13/01/2026, 3 (três) dias úteis anteriores à data designada para abertura da sessão pública**, até às 15h (horário de Brasília), exclusivamente por meio eletrônico via internet, no endereço indicado no Edital, mediante **petição**, que deverá obrigatoriamente (art. 10, caput, da Lei nº 12.527/2011) conter a identificação do Impugnante (CPF/CNPJ).

22.3. Os pedidos de impugnações e esclarecimentos, bem como as respectivas respostas, serão divulgados no site https://www.gov.br/compras/pt-br, na área Gestor Público/consultas/pregões/agendados (http://comprasnet.gov.br/acesso.asp?url=/livre/Pregao/lista_pregao_filtro.asp?Opc=0) e no **site oficial do MPAM**. O fornecedor, além do acesso livre, poderá visualizar também no menu principal, no link: "visualizar impugnações /esclarecimentos/avisos".

22.4. A impugnação ou pedido de esclarecimento poderá ser realizada por forma eletrônica, pelo e-mail licitacao@mpam.mp.br, no horário local de expediente da Instituição, até às 15 horas (horário de Brasília) da data limite fixada ou por petição dirigida/protocolada no Prédio-Sede desta PGJ, localizado na Av. Coronel Teixeira, nº 7995 - Nova Esperança, CEP: 69037-473, endereçado à Comissão Permanente de Licitação.

22.5. Acolhida a impugnação ou determinadas as providências requeridas, será designada nova data para realização da sessão pública, salvo quando estas não afetarem a formulação das propostas.

22.6. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

22.6.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos autos do processo de licitação.

22.7. As respostas aos pedidos de esclarecimentos divulgadas pelo sistema vincularão os participantes e a Administração.

23. DAS DISPOSIÇÕES FINAIS

23.1. A **COMISSÃO PERMANENTE DE LICITAÇÃO** prestará todos os esclarecimentos solicitados pelos interessados nesta licitação, estando disponível para atendimento de segunda a sexta-feira, das 9h às 15 horas (horário de Brasília), na Avenida Coronel Teixeira, n.º 7.995, Nova Esperança, Manaus – AM, pelo telefone (92) 3655-0743 ou, ainda, pelo e-mail: licitacao@mpam.mp.br.

23.2. A **Autoridade Competente** designará o pregoeiro que conduzirá esta licitação, necessariamente escolhido dentre os Pregoeiros Oficiais do **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**.

23.3. É facultada ao pregoeiro ou autoridade superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou complementar a instrução do processo.

23.3.1. O pregoeiro, durante as fases de julgamento das propostas e/ou habilitação, deve sanear eventuais erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível aos licitantes, sendo que a vedação à inclusão de novo documento, prevista no art. 64 da Nova Lei de Licitações (Lei 14.133/2021), não alcança documento ausente, comprobatório de condição atendida pelo licitante quando apresentou sua proposta, que não foi juntado com os demais comprovantes de habilitação e/ou da proposta, por equívoco ou falha, o qual deverá ser solicitado e avaliado pelo pregoeiro. (Acórdão TCU 1211/2021 - Plenário, relator Ministro Walton Alencar Rodrigues).

23.3.2. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento de que trata o subitem anterior, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, 24 (vinte e quatro) horas de antecedência, e a ocorrência será registrada em ata.

23.4. A **Autoridade Competente** para determinar a contratação poderá revogar a licitação por razões de interesse público derivado de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo anulá-la por ilegalidade, de ofício ou por provocação de qualquer pessoa, mediante ato escrito e fundamentado.

23.4.1. No caso de revogação ou anulação do procedimento licitatório, ficará assegurada oportunidade de ampla e prévia manifestação dos interessados, na forma da Lei.

23.4.2. A anulação pode ser declarada a qualquer tempo.

23.4.3. As licitantes não terão direito a indenização em decorrência de anulação do procedimento licitatório, ressalvado o direito do FORNECEDOR de boa-fé de ser ressarcida pelos encargos que tiver suportado em eventual cumprimento da obrigação decorrente da execução do objeto deste certame.

23.5. Os proponentes assumem todos os custos de preparação e apresentação de sua proposta e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

23.6. **Após apresentação da proposta, não caberá desistência, salvo por motivo justo decorrente de fato superveniente e aceito pelo pregoeiro, sob pena de abertura de procedimento apuratório em face da conduta do licitante**.

23.7. Quando todos os licitantes forem inabilitados ou todas as propostas forem desclassificadas, o Pregoeiro poderá fixar aos licitantes o prazo de 3 (três) dias úteis para apresentar nova documentação ou nova proposta escoimada das causas que ensejaram a inabilitação ou desclassificação das empresas.

23.8. Em caso de licitante vencedor sediado fora da cidade de Manaus, cujo envio de documentos e demais solicitações ensejem utilização de serviços postais, será obrigatória a apresentação de cópia do comprovante de envio dos itens solicitados, como forma de confirmação do atendimento aos prazos previstos em cada subitem.

23.8.1. O comprovante poderá ser digitalizado e enviado para o e-mail: licitacao@mpam.mp.br.

23.8.2. O descumprimento dos prazos para envio dos documentos ou demais solicitações, sem apresentação de justificativa,

ensejará a desclassificação da empresa licitante, sem prejuízo das sanções cabíveis.

23.8.3. Caso a autenticação do documento ou o próprio documento esteja em formato digital, com assinatura por certificado digital, padrão ICP-Brasil, ou ainda torne possível sua convalidação em sítio eletrônico de autoridade certificadora oficial e/ou cartório digital respectivo, a licitante está dispensada da obrigação do item anterior.

23.8.3.1. Os documentos eletrônicos produzidos com a utilização de processo de certificação disponibilizada pela ICP-Brasil, nos termos da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, serão recebidos e presumidos verdadeiros em relação aos signatários, dispensando-se o envio de documentos originais e cópias autenticadas em papel.

23.9. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no horário e local aqui estabelecidos, desde que não haja comunicação do Pregoeiro em contrário.

23.10. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente normal no **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**.

23.11. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível a verificação de suas condições de habilitação e a exata compreensão da sua proposta, durante a realização da sessão pública de pregão.

23.12. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

23.13. Será divulgada ata da sessão pública no sistema eletrônico.

23.14. Nenhuma pessoa física ou jurídica ainda que credenciada poderá representar mais de uma empresa concorrente, sob pena de não participação das empresas representadas.

23.15. A homologação do resultado desta licitação não implicará direito à contratação.

23.16. Em substituição aos respectivos originais todos os documentos poderão ser apresentados em cópia autenticada por Cartório competente ou conferida com o original por servidor da CPL. **Neste último caso, a autenticação administrativa poderá ser feita, preferencialmente, até o dia anterior à data prevista para o recebimento dos envelopes da Proposta e da Documentação**;

23.17. Somente serão aceitos propostas e lances encaminhados pelo sistema eletrônico.

23.18. É de inteira responsabilidade do licitante o acompanhamento do processo referente a este pregão eletrônico, no endereço eletrônico https://www.gov.br/compras/pt-br.

23.19. Para as demais condições de contratação, observar-se-ão as disposições constantes dos Anexos deste Edital.

23.20. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

23.21. Este Edital e seus Anexos poderão ser examinados sem ônus para o interessado, antes da realização da licitação, no formato eletrônico, através de consulta aos sítios https://www.gov.br/compras/pt-br e www.mpam.mp.br, ou através do correio eletrônico da CPL, licitacao@mpam.mp.br.

23.20.1. O Edital e seus anexos também estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico https://www.gov.br/pncp/pt-br.

23.20.1. Poderão ser, também, adquiridos impressos mediante depósito da quantia referente ao custo reprográfico, calculado no produto de R$ 0,50 (cinquenta centavos) por página, depositado na Conta-Corrente n.º 13200-4, Agência 6019-4, do Banco Bradesco S/A (237), em nome do **FUNDO DE APOIO DO MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**.

23.22. Os casos omissos serão resolvidos pelo Pregoeiro, com base no Ato PGJ n.º 008/2024 e na Lei n.º 14.133/21 e alterações.

23.23. As questões decorrentes da execução deste Instrumento, que não possam ser dirimidas administrativamente, serão processadas e julgadas no foro da cidade de Manaus, com exclusão expressa de qualquer outro.

Manaus, 30 de dezembro de 2025.

Sarah Madalena B. Côrtes de Melo

Presidente da Comissão Permanente de Licitação
Ato PGJ n.º 165/2025 - DOMPE, Ed. 3121, de 15.07.2025

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

TERMO DE REFERÊNCIA Nº 28.2025.DTIC.2002143.2025.007562

1. OBJETO DA CONTRATAÇÃO

1.1 Contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais do Ministério Público do Estado do Amazonas (MPAM).

1.2 Justificativa para a Contratação

Em 2019, foi celebrado o Contrato Administrativo n. 006/2019 - MP/PGJ (SEI0299031), para o Sistema de Automação da Justiça para o Ministério Público - SAJ-MP. Paralelamente, foi adquirida uma solução de software e hardware para processamento e armazenamento de dados que suportasse as demandas requeridas pelo SAJ-MP e demais sistemas computacionais da instituição - Solução Nutanix de Hiperconvergência, através do Contrato Administrativo n. 010/2018 - MP/PGJ (SEI 0210232).

Em 2020, para aumentar a capacidade de processamento e armazenamento, foi adquirido mais um servidor que fora incorporado à solução de Nutanix de Hiperconvergência, através do Contrato Administrativo n. 020/2020 - MP/PGJ, SEI 0572982.

A infraestrutura de hardware e software adquirida foi instalada no espaço físico mencionado e desde então segue em operação.

Esta é a infraestrutura física e computacional sobre a qual se mantêm os sistemas computacionais do MPAM, atualmente em situação crítica, com equipamentos que já ultrapassaram o período de suporte ativo pelos fabricantes (end of life), tornando-se obsoletos do ponto de vista técnico e funcional. Essa condição, como já mencionado, implica riscos relevantes à operação institucional, tais como falhas operacionais, indisponibilidade de sistemas e impossibilidade de atualização tecnológica.

Além disso, as aplicações institucionais em uso pelo MPAM estão em constante evolução, exigindo maior desempenho, escalabilidade e disponibilidade de recursos computacionais. A atual infraestrutura hiperconvergente, embora eficaz em sua concepção, já não atende plenamente às demandas atuais e futuras, especialmente diante da necessidade de implantação de novos sistemas e da manutenção dos já existentes.

Diante desse cenário, especificamos a contratação de uma solução plataforma NUTANIX, com equipamentos em garantia técnica e alinhados às necessidades imediatas do órgão, de forma a promover a continuidade dos serviços e a proteção de dados institucionais.

2. FORMA DE CONTRATAÇÃO

2.1 Tipo de contratação

2.1.1 A contratação será realizada por meio de licitação.

2.2 Modalidade da licitação

2.2.1 A modalidade adotada será o Pregão, na forma eletrônica, nos termos da legislação vigente.

2.3 Justificativa para não adoção do Sistema de Registro de Preços

2.3.1 A presente contratação refere-se a serviços de natureza contínua, com necessidade de execução imediata, regular e ininterrupta, cujas quantidades e especificações estão previamente definidas no Termo de Referência. Tais características não se compatibilizam com o modelo de contratação por demanda variável previsto no Sistema de Registro de Preços.

2.3.2 A demanda é certa, contínua e previamente dimensionada, tratando-se de prestação direta e específica ao contratante. Diante disso, a forma de execução contratual exige vínculo estável e unitário durante todo o período de vigência, não sendo adequada a contratação por meio de adesões esporádicas ou fracionadas.

2.3.3 Ressalta-se, ainda, que o uso do SRP é facultativo, conforme previsto no art. 82 da Lei nº 14.133/2021, sendo recomendado apenas quando se verificar vantagem para a Administração, o que não se configura no caso em questão.

2.4 Critério de julgamento da proposta

2.4.1 Será adotado o critério de julgamento pelo menor preço.

2.5 Critério de adjudicação

2.5.1 A adjudicação será realizada pelo critério de menor preço **global**.

2.6 Consórcios

2.6.1 Fica vedada a participação de empresas em consórcio nesta licitação. A natureza dos serviços – homogêneos, integrados e de execução contínua – não apresenta volume financeiro de alta monta ou risco elevado que justifique a união de empresas. Além disso, a formação de consórcios poderia acarretar dificuldades na gestão e fiscalização contratual, bem como possível elevação de custos, contrariando os princípios da vantajosidade e da eficiência.

2.7 Previsão de subcontratação

2.7.1 É vedada a subcontratação dos serviços objeto desta contratação. Considerando a natureza sensível e estratégica das atividades, as quais exigem controle direto e permanente da contratada, a subcontratação representaria risco à continuidade, à segurança da informação e à qualidade dos serviços prestados. Tal vedação está amparada no art. 122, § 2º, da Lei nº

14.133/2021, sendo medida necessária para preservar a eficiência e a efetividade da execução contratual.

2.8 Aplicação de tratamento diferenciado para ME/EPP/MEI (microempresa e afins)

2.8.1 Será assegurado o tratamento diferenciado às Microempresas (ME), Empresas de Pequeno Porte (EPP) e Microempreendedores Individuais (MEI) conforme previsto na legislação vigente, mediante comprovação de enquadramento no momento da habilitação, nos termos e condições a estabelecidas no edital.

2.9 Aplicação de direito de preferência

2.9.1 Em caso de empate ficto entre propostas, será assegurado o exercício do direito de preferência às ME, EPP e MEI, conforme disposto nos arts. 44 e 45 da Lei Complementar nº 123/2006, e no art. 62, inciso III, da Lei nº 14.133/2021. Os prazos e procedimentos para o exercício do referido direito serão disciplinados no instrumento convocatório.

3. REQUISITOS DO FORNECEDOR

3.1 Da necessidade de vistoria técnica

3.3.1 As empresas LICITANTES DEVERÃO realizar, sob o acompanhamento de servidor especialmente designado, vistoria às unidades da Procuradoria-Geral de Justiça, em data e horário previamente acordados segundo a conveniência deste Órgão, com o objetivo de conhecer as instalações onde serão executados os serviços e sanar as dúvidas porventura existentes, a fim de subsidiar a elaboração das propostas a serem submetidas ao certame.

3.3.1.1 A vistoria deverá ser realizada por representante devidamente credenciado pela empresa LICITANTE, devidamente municiado de documento próprio de credenciamento;

3.3.1.2 A comprovação de realização da vistoria será efetuada por meio de apresentação deAtestado de Realização de Vistoria Técnica, que será emitido pelo interessado, ssinado por servidor designado da DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - DTIC desta PGJ/AM, e apresentado oportunamente, à sua habilitação;

3.3.1.3 O Atestado de Realização de Vistoria Técnica será assinado por servidor do MPAM que acompanhar a vistoria, e deverá ser encaminhada juntamente com a proposta;

3.3.1.4 As visitas deverão ser previamente agendadas, com 24 (vinte e quatro) horas de antecedência, pelo telefone (92) 3655-0670/0660 – DTIC, no período das 8h às 14h e poderão ser realizadas em até 2 (dois) dias úteis anteriores à data estipulada para abertura da licitação.

3.3.2 Caso a LICITANTE renuncie à vistoria técnica, deverá entregar a Declaração de Dispensa de Vistoria, o qual deverá ser preenchido e assinado pelo interessado em participar da licitação, anexando, oportunamente, à sua habilitação.

3.3.3 Não serão aceitas alegações posteriores advindas de desconhecimento das condições prediais, das características do ambiente de prestação dos serviços ou erro orçamentário por parte da futura contratada, quando da execução dos serviços propostos.

3.2 Da capacidade técnica

3.2.1 A licitante deve apresentar, juntamente com os demais documentos de habilitação, atestado de capacidade técnica expedido(s) em seu nome e respectivo CNPJ, fornecido por pessoas jurídicas de direito público ou privado, que comprovem já ter fornecido solução de datacenter, contemplando infraestrutura integrada de hardware e software, serviço de implantação, configuração e transferência de conhecimento, similares ao objeto deste Termo.

3.2.2 A licitante deverá apresentar na qualificação técnica, documento que indique o pessoal técnico operacional, das instalações e do aparelhamento adequado e disponíveis para a realização do objeto da licitação, bem como a qualificação de cada membro da equipe técnica que se responsabilizará pelos trabalhos. (art. 67, III da Lei 14.133/21).

3.2.3 Os atestados apresentados poderão ser objeto de diligência a critério do CONTRATANTE, para verificação da autenticidade do conteúdo. Caso seja encontrada divergência entre o especificado nos documentos e o apurado em eventual diligência, além da desclassificação no presente processo licitatório, fica sujeita a licitante às penalidades cabíveis.

3.3 Apresentação de amostras

3.3.1 A critério da autoridade competente, não será exigida a apresentação de amostras.

4. DA FORMALIZAÇÃO E PRAZO DE VIGÊNCIA DO CONTRATO

A CONTRATANTE formalizará um contrato administrativo observando as seguintes condições:

4.1 Do prazo

4.1.1 A CONTRATADA deverá em, **no máximo, 60 (sessenta) dias corridos**, contados a partir da assinatura do contrato, finalizar a entrega de todos os itens do objeto especificado, com funcionamento e funcionalidades da solução de Datacenter completamente operacionais, totalmente ativadas e disponíveis na estrutura da CONTRATADA, conforme descritas neste Termo.

4.2 Das condições de fornecimento

4.2.1 A CONTRATADA será responsável pelo transporte dos produtos, desde o local de sua fabricação/embalagem, conforme o caso, até o local de entrega, na sede da PROCURADORIA GERAL DE JUSTIÇA, a qual ocorrerá em dias úteis, no horário das 14h às 17h, no seguinte endereço:

Av. Coronel Teixeira, nº 7.995, Nova Esperança II **CEP. 69037-473, Manaus-AM**

4.2.2 A entrega dos produtos deverá ser previamente agendada com o SETOR DE PATRIMÔNIO E MATERIAL – SPAT pelo telefone (92) 3655-0767.

4.2.3 Os produtos deverão ser entregues em perfeitas condições, conforme a quantidade e especificações pactuadas, observando o Edital, a Proposta da CONTRATADA e este Termo de Referência, devendo, também, ser acondicionado adequadamente, em seu invólucro original, que deverão ser entregues devidamente acompanhados da respectiva nota fiscal, na qual constarão os valores discriminados dos itens que integram o conjunto, assim como as indicações referentes a: marca, modelo, procedência e prazo de garantia ou validade.

4.2.4 Os produtos devem estar em plena fabricação, não sendo aceitos aqueles com avisos de end-of-sale, end-of-support ou end-of-life emitidos pelo fabricante.

4.3 Da vigência do contrato

4.3.1 O Contrato terá vigência de **60 (sessenta) meses**, contados da data de publicação do extrato no Diário Oficial do MPAM, sendo resguardados os direitos relacionados à garantia e a assistência técnica vinculados aos equipamentos e serviços adquiridos, conforme descrito neste Termo.

5. MODELO DE GESTÃO

5.1 O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133/21, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

5.2 Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

5.3 As comunicações entre a CONTRATANTE e a CONTRATADA devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

5.4 A CONTRATANTE poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

5.5 Após a assinatura do contrato ou instrumento equivalente, a CONTRATANTE poderá convocar o representante da CONTRATADA para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da CONTRATADA, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

5.6 Preposto

5.6.1 A CONTRATADA deverá manter preposto junto à PGJ-AM, aceito pela respectiva FISCALIZAÇÃO, durante o período de vigência do contrato, para representá-la administrativamente, sempre que for necessário, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado, o qual deverá ser indicado mediante declaração de que deverá constar o nome completo, nº do CPF e do documento de identidade, além dos dados relacionados à sua qualificação profissional.

5.6.2 A empresa orientará o seu PREPOSTO quanto à necessidade de acatar as orientações da Administração, inclusive quanto ao cumprimento das Normas Internas e de Segurança e Medicina do Trabalho.

5.6.3. A Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em quea Contratada designará outro para o exercício da atividade.

5.7 Fiscalização

5.7.1 A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos, conforme indicação em portaria específica publicada no Diario Oficial do MPAM.

5.7.2 Compete ao Gestor da Ata/Contrato, além de outras atribuições, nos termos da lei:

a) Acompanhar os prazos de execução e de vigência do contrato, conforme as rotinas e procedimentos estabelecidos pelo MPAM, e as cláusulas do contrato ou instrumento equivalente, comunicando à CONTRATADA e à unidade competente da Administração eventuais atrasos e encaminhando, em tempo hábil, expediente para a prorrogação do Contrato;

b) Coordenar e acompanhar a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração;

c) Acompanhar a manutenção das condições de habilitação da CONTRATADA, para fins de empenho de despesa e pagamento, e anotar os problemas que obstam o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais;

d) Comunicar à Autoridade Competente as ocorrências relacionadas à execução do contrato que ultrapassarem a sua competência;

e) Emitir TERMO DE RECEBIMENTO DEFINITIVO, juntamente com a FISCALIZAÇÃO, comprovando a avaliação do cumprimento das obrigações assumidas pelo CONTRATADO;

f) Receber e conferir as faturas/notas fiscais emitidas pela CONTRATADA, e encaminhar, devidamente certificadas/atestadas ao setor competente, observando, previamente, se a fatura apresentada pela CONTRATADA refere-se ao objeto que foi efetivamente CONTRATADO;

g) Encaminhar o processo à unidade competente para proceder à liquidação da despesa, alertando para a data limite para pagamento das notas fiscais/fatura;

h) Requisitar a prorrogação de contrato, se possível, junto à Autoridade Competente, que deve ser providenciada antes de seu término, reunindo as justificativas necessárias;

i) Elaborar a comunicação à área competente para abertura de nova licitação, antes de findo a prestação de serviços e com antecedência razoável;

j) Cuidar das alterações de interesse da CONTRATADA, que deverão ser por ela formalizadas e devidamente fundamentadas, principalmente em se tratando de pedido de reequilíbrio econômico-financeiro ou repactuação, sendo que, no caso de pedido de prorrogação de prazo, deverá ser comprovado o fato impeditivo da execução, o qual, por sua vez, deverá corresponder àqueles previstos na Lei n. 14.133/21 e alterações, se possível;

k) Esclarecer dúvidas e transmitir instruções ao CONTRATADO, comunicando alterações de prazos, cronogramas de execução e especificações do projeto, inclusive solicitando ao setor competente da Administração, quando necessário a emissão de parecer técnico;

l) Deflagrar e conduzir os procedimentos de fiscalização à CONTRATADA, com base nos termos contratuais, sempre que houver descumprimento de suas cláusulas por culpa da CONTRATADA, acionando as instâncias superiores e/ou os órgãos públicos competentes quando o fato exigir;

m) Verificar se a entrega de materiais ou a prestação do serviço está sendo executada em conformidade com o pactuado, no tocante a prazo, especificações, preço e quantidade;

n) Rejeitar equipamentos e serviços que estejam em desacordo com as especificações do objeto contratado;

o) Zelar pelo efetivo cumprimento das obrigações contratuais assumidas e pela qualidade dos produtos fornecidos e dos serviços prestados;

p) Notificar a CONTRATADA em qualquer ocorrência desconforme com as cláusulas contratuais, sempre por escrito, com prova

de recebimento da notificação (procedimento formal, com prazo);

q) Verificar a regularidade fiscal, trabalhista e previdenciária da contratada para fins de pagamento; e

r) Orientar a CONTRATADA, por intermédio do preposto, sobre a correta execução do Contrato e, pelo mesmo meio, levar ao seu conhecimento as situações temerárias, recomendando medidas e estabelecendo prazo de resolução.

5.7.3 Compete ao Fiscal Técnico, além de outras atribuições, nos termos da lei:

a) Acompanhar e fiscalizar a execução do contrato nos aspectos técnicos da solução, conforme o respectivo regramento técnico aplicável;

b) Zelar pelo efetivo cumprimento das obrigações contratuais assumidas e pela qualidade dos produtos fornecidos e dos serviços prestados, de modo a assegurar os melhores resultados para a Administração;

c) Ler atentamente o Termo de Contrato e anotar em registro próprio todas as ocorrências relacionadas à sua execução, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados;

d) Esclarecer dúvidas do preposto/representante da CONTRATADA que estiverem sob a sua alçada, encaminhando às áreas competentes os problemas que surgirem quando lhe faltar competência;

e) Notificar a CONTRATADA para a correção da execução do contrato, determinando prazo para a correção, quando identificada qualquer inexatidão ou irregularidade;

f) Informar ao Gestor do Contrato, em tempo hábil, irregularidades que possam demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso;

g) Comunicar ao Gestor do Contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual;

h) Avaliar a qualidade dos serviços realizados ou dos itens entregues e justificativas, de acordo com os critérios de aceitação definidos em contrato; e

i) Orientar a CONTRATADA, por intermédio do preposto, sobre a correta execução do contrato e, pelo mesmo meio, levar ao seu conhecimento as situações temerárias, recomendando medidas e estabelecendo prazo de resolução.

6. ENTREGA DO OBJETO

6.1 Do recebimento provisório e definitivo

6.1.1 O recebimento dos produtos será conduzido por uma COMISSÃO especialmente designada para essa finalidade. Essa comissão será composta por, no mínimo, três servidores ou empregados públicos, em conformidade com o disposto no Art. 117, §1º e Art. 140, inciso II da Lei n.º 14.133/21, conforme estabelecido neste subitem.

6.1.2 O RECEBIMENTO PROVISÓRIO será realizado pelo SETOR DE PATRIMÔNIO E MATERIAL - SPAT no ato da entrega da totalidade dos produtos empenhados, devidamente acompanhados da nota fiscal. Constitui-se de uma inspeção quantitativa, para posterior verificação de sua conformidade com as especificações do Termo de Referência, e Ata de Registro de Preços.

a) O RECEBIMENTO PROVISÓRIO não constitui aceitação dos mesmos.

6.1.3 O RECEBIMENTO DEFINITIVO será realizado por FISCAL TÉCNICO ou COMISSÃO especialmente designada, no prazo máximo de 30 (trinta) dias, a contar do recebimento provisório, para verificação da conformidade dos equipamentos com as condições, especificações e obrigações contratuais.

a) É condição para RECEBIMENTO DEFINITIVO o fornecimento do TERMO DE GARANTIA E ASSISTÊNCIA TÉCNICA, informando que os referidos produtos estão cobertos por garantia de fábrica, de acordo com as exigências constantes neste instrumento;

b) O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais;

c) Uma vez constatado o cumprimento das obrigações de fornecimento, o TERMO DE RECEBIMENTO DEFINITIVO será emitido, que consistirá na declaração formal de que os itens fornecidos atendem aos requisitos estabelecidos no contrato, comprovando o atendimento das exigências contratuais.

6.1.4 Para avaliação da adequação às exigências contratuais e qualidade, o FISCAL TÉCNICO ou COMISSÃO submeterá os equipamentos recebidos a testes de aceitação, para aferição da boa execução do objeto contratado, após o qual, emitirá um relatório completo dos testes efetuados, devidamente assinado. Os testes serão constituídos das seguintes fases:

a) Abertura das embalagens;

b) Comprovação de que o equipamento/solução atende às especificações mínimas exigidas ou superiores oferecidas;

c) Testes funcionais de configuração e desempenho dos mesmos.

6.1.5 Os itens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência, seus Anexos e na proposta, sem prejuízo da aplicação das penalidades, cabendo à CONTRATADA o dever de substituir os itens que não estejam de acordo com as especificações, observando-se o disposto no Art. 140, §1º da Lei n.º 14.133/21.

6.1.6 O RECEBIMENTO PROVISÓRIO ou DEFINITIVO do objeto não exclui a responsabilidade civil a ele relativa, nem a ético-profissional, pela perfeita execução do objeto deste Termo.

6.1.7 As não conformidades e desvios de qualidade observados serão descritos em relatório, e não serão recebidos definitivamente, devendo a pendência ser completamente sanada pela CONTRATADA, em no máximo 15 (quinze) dias consecutivos, contados da notificação da CONTRATANTE.

6.1.8 Se, a qualquer tempo, vier a ser constatado que o material fornecido o foi em desacordo com as especificações e, em decorrência desse fato, observar-se qualquer tipo de dano ao equipamento onde está sendo utilizado, o reparo do equipamento ou, se for o caso, a sua substituição, será de inteira responsabilidade da CONTRATADA, nos termos da lei pertinente.

7. DAS OBRIGAÇÕES DO CONTRATANTE E DA CONTRATADA

7.1 Obrigações da CONTRATADA

7.1.1 A CONTRATADA deverá cumprir todas as obrigações constantes neste termo de referência, minuta de contrato e seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando:

7.1.2 Apresentar, no prazo de até 10 (dez) dias corridos, contados a partir da assinatura do Contrato ou do recebimento da Nota

de Empenho e da Autorização de Fornecimento de Materiais/Serviços:

7.1.2.1 Indicação formal do preposto da CONTRATADA apto a representá-la junto à CONTRATANTE, que deverá responder pela fiel execução do contrato, designado para acompanhar sua execução e atuar como interlocutor principal junto à CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

a) A indicação do preposto deverá ser acompanhada de seus dados pessoais, (no mínimo o nome completo e CPF do funcionário da empresa) e dados de contrato, como e-mail, telefone, whatsapp e outros.

7.1.2.2 Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste Termo de Referência.

7.1.3 Efetuar a entrega do objeto contratado, dentro do prazo e de acordo com as especificações constantes deste Termo de Referência, observando as prescrições e as recomendações do fabricante, a legislação estadual ou municipal, se houver, bem como outras normas correlatas, ainda que não estejam explicitamente citadas neste documento e seus anexos.

7.1.4 Apresentar, no prazo de até 10 (dez) dias úteis, contados a partir da entrega do objeto, o correspondente TERMO DE GARANTIA E ASSISTÊNCIA TÉCNICA, para os equipamentos/softwares/licenças fornecidos incluindo seus números de série, com o prazo de garantia solicitado neste Termo de Referência.

7.1.5 Não transferir a outrem, no todo ou em parte, o objeto deste Termo, sem prévia e expressa anuência da CONTRATANTE, não sendo aceita a transferência de responsabilidade para outras entidades, sejam fabricantes, técnicos, subempreiteiros ou quaisquer outros.

7.1.6 Comunicar imediatamente à CONTRATANTE, formalmente, toda e qualquer anormalidade que dificulte ou impossibilite a execução do objeto deste Termo e prestar os esclarecimentos julgados necessários.

7.1.7 Aceitar todas as decisões, métodos de inspeção, verificação e controle, obrigando-se a fornecer todos os dados, elementos e explicações que a CONTRATANTE julgar necessário.

7.1.7.1 A ação de fiscalização não exonera a CONTRATADA de suas responsabilidades contratuais.

7.1.8 Manter contato e realizar o planejamento dos serviços com o CONTRATANTE de forma a executar quaisquer tarefas ou ajustes inerentes ao objeto contratado.

7.1.9 Acatar as observações feitas pela FISCALIZAÇÃO da CONTRATANTE quanto à execução dos serviços.

7.1.10 Atender prontamente quaisquer orientações e exigências da equipe de FISCALIZAÇÃO do contrato ou autoridade superior (art. 137, II, da Lei n.º 14.133/21, e prestar todo esclarecimento ou informação por eles solicitados, inerentes à execução do objeto contratual;

7.1.10.1 A CONTRATADA deverá responder por escrito, no prazo máximo de até 2 (dois) dias consecutivos, a quaisquer comunicações e/ou esclarecimentos requisitados pela CONTRATANTE, pertinentes à execução do contrato e que venham a ser solicitados pelo MPAM.

7.1.11 A CONTRATADA deverá responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com Código de Defesa do Consumidor, Lei nº 8.078/90, e às demais normas pertinentes.

7.1.12 Apresentar justificativa por escrito, devidamente comprovada, nos casos de ocorrência de fato superveniente, excepcional ou imprevisível, estranho à vontade das partes, e de impedimento de execução por fato ou ato de terceiro reconhecido pela CONTRATANTE em documento contemporâneo a sua ocorrência, quando não puder cumprir os prazos estipulados para a execução, total ou parcial, do objeto deste Termo.

7.1.12.1 Nos casos de eventual atraso na entrega do objeto, comunicar à CONTRATANTE antes de expirar tal prazo, quaisquer problemas que impossibilitem o cumprimento do prazo previsto, com a devida comprovação.

7.1.13 Substituir, reparar, corrigir, remover, refazer ou reconstituir, às suas expensas, no todo ou em parte, no prazo fixado pela FISCALIZAÇÃO, os itens que não atendam às especificações exigidas e foram rejeitados, os que se verifiquem imperfeições, vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.

7.1.14 Responsabilizar-se por falhas na execução dos serviços que venham a se tornar aparentes em data posterior à sua entrega, ainda que tenha havido aceitação do mesmo.

7.1.15 Responsabilizar-se pela garantia e assistência técnica *on-site* dos itens, caso o fabricante e/ou assistência técnica autorizada por este não puder fazê-lo ou se recusar.

7.1.16 Manter, durante toda a execução do contrato, todas as condições de habilitação e qualificação exigidas na respectiva licitação, em compatibilidade com as obrigações assumidas.

7.1.17 Responder pela idoneidade moral e técnica dos seus empregados, sendo única, integral e exclusivamente responsável, em qualquer caso, por todos os danos e prejuízos, de qualquer natureza, causados, direta ou indiretamente, à CONTRATANTE ou a terceiros, provenientes da execução dos serviços objeto deste termo de referência, quaisquer que tenham sido as medidas preventivas adotadas, respondendo por si e seus procuradores.

7.1.18 Responsabilizar-se por obter todas as franquias, licenças, aprovações e demais exigências de órgãos competentes, inclusive responsabilizando-se por todos os ônus decorrentes.

7.1.19 A inobservância das especificações constantes deste termo de referência implicará a não aceitação parcial ou total dos serviços, devendo a CONTRATADA refazer as partes recusadas sem direito a indenização.

7.2. Obrigações da CONTRATANTE

7.2.1 Acompanhar e fiscalizar, como lhe aprouver e no seu exclusivo interesse, na forma prevista na Lei n.º 14.133/21, exigindo o cumprimento de todas as obrigações assumidas, de acordo com o contrato e seus anexos.

7.2.2 Nomear GESTOR e FISCALIZAÇÃO técnica e administrativa, para acompanhar e fiscalizar, a execução dos contratos.

7.2.3 As ações de fiscalização não excluem nem reduzem a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios ou emprego de material inadequado ou de qualidade inferior.

7.2.4 Fornecer à CONTRATADA as informações necessárias à fiel execução do objeto deste termo de referência.

7.2.5 Permitir o acesso, acompanhar e fiscalizar a execução do contrato, verificando a conformidade da prestação dos serviços e regular a entrega dos itens, de forma a assegurar o perfeito cumprimento do contrato.

7.2.6 Anotar em registro próprio e notificar a CONTRATADA, por escrito, a ocorrência de eventuais imperfeições, defeitos de fabricação, e avarias nos itens, fixando prazo para a sua reposição.

7.2.7 Rejeitar, no todo ou em parte, serviço ou fornecimento executado em desacordo com o contrato.

7.2.8 Efetuar regularmente o pagamento da CONTRATADA, dentro dos critérios estabelecidos neste termo de referência e no contrato, quanto aos serviços devidamente realizados, por meio de Ordem Bancária, após o atesto das notas fiscais/faturas pelo comitê responsável.

8. DAS PENALIDADES

8.1 O descumprimento de quaisquer das obrigações relacionadas à prestação do serviço, salvo nos casos devidamente justificados e comprovados, a critério da CONTRATANTE, sujeitará a CONTRATADA às sanções previstas na Lei Federal n.º 14.133/2021, sem prejuízo das responsabilidades civil e criminal, garantindo-se o direito ampla defesa e ao contraditório, quais sejam:

I. Advertência: Será aplicada no caso de atraso no cumprimento dos prazos para apresentação de uma solução definitiva para um problema com solução provisória, ainda que mantidos os níveis de serviço acordados com tal solução provisória, bem como, nos casos de atraso no encaminhamento do diagnóstico da ocorrência e comprovação da correção após a solução definitiva do problema e nos casos de repetidos descumprimentos dos acordos de nível de serviço que gerem impacto ao funcionamento do MPAM.

II. Multa, nos seguintes termos:

Item	Penalidade	Sanção	Limite
1	Atraso injustificado na entrega do objeto contratado, ou pelo não cumprimento dos prazos estabelecidos no Edital	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor total da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
2	Atraso injustificado na regularização pertinente quando da recusa do objeto fornecido, na fase de **RECEBIMENTO**.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor total da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
3	Recusa em substituir o produto defeituoso, que vier a ser rejeitado, ou que na execução dos serviços de garantia e assistência técnica, apontem a necessidade de troca;	Multa de mora diária de **1% (um por cento)** sobre o valor da Nota de Empenho	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
4	Deixar de utilizar peças, componentes ou insumos originais ou certificados pelo fabricante, novos e de primeiro uso.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho. Por ocorrência	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
5	Atraso injustificado para efetiva recolocação do produto em seu pleno estado de funcionamento, conforme condições de GARANTIA E ASSISTÊNCIA TÉCNICA deste Termo.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
6	Deixar de fornecer equipamento backup nos casos em que não for possível recuperar os produtos dentro dos prazos de atendimento previstos.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
7	Atraso injustificado para a substituição de determinado item (equipamento, serviço, software, licença), no atendimento de chamado de garantia e assistência técnica.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da CONTRATADA às sanções correlatas.
8	Atraso injustificado para a análise e correção dos itens (equipamento, serviço, software, licença), no atendimento de chamado de garantia e assistência técnica.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 10º (décimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 11.º (décimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
9	Atraso injustificado para o fornecimento do TERMO DE GARANTIA E ASSISTÊNCIA TÉCNICA.	Multa de mora diária de **0,3% (três décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 10º (décimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 11.º (décimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.

Item	Penalidade	Sanção	Limite
10	Atraso injustificado na resposta aos pedidos de esclarecimentos de ordem técnica.	Multa de mora diária de **0,2% (dois décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 10º (décimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 11.º (décimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
11	Deixar de cumprir qualquer outra obrigação não prevista neste Termo de Referência	Multa de mora diária de **1% (um por cento)** sobre o valor da Nota de Empenho	Limitada a sua aplicação até **15% (quinze por cento)**.
12	Quando, sem justificativa aceita pela **CONTRATANTE**, o vencedor não providenciar o devido cadastramento junto ao Sistema de Administração Financeira e Contabilidade – Cadastramento de Credores da SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ-AM, na forma prevista no Edital.	Multa de 2**,5% (dois inteiros e cinco décimos por cento)** sobre o valor total da proposta.	Não se aplica.
13	Inexecução parcial do objeto contratado.	Multa de até **30% (trinta por cento)** sobre o valor da Nota de Empenho, sem prejuízo das demais sanções previstas.	Não se aplica.
14	Inexecução total do objeto.	Multa de até **30% (trinta por cento**) sobre o valor total do contrato, sem prejuízo das demais sanções previstas.	Não se aplica.

III. Com fundamento no artigo 156, inciso III, da Lei n.º 14.133/2021, ficará impedido de licitar e contratar, pelo prazo de até 3 (três) anos, sem prejuízo de multa de até 10% (dez por cento) do valor estimado para a contratação e demais cominações legais, nos seguintes casos:

a) Apresentar documentação falsa;

b) Ensejar o retardamento da execução do objeto;

c) Comportar-se de modo inidôneo;

d) Não manter a proposta;

e) Deixar de entregar a documentação exigida no certame, e quando esta conduta caracterizar fraude à licitação pública;

f) Cometer fraude fiscal;

g) Fazer declaração falsa.

8.2. Para fins da subcondição da alínea "c" do item III, reputar-se-ão inidôneos atos como os descritos nos arts. 337-F, 337-H, 337-I, 337-J, 337-K e 337-M do Código Penal.

8.3 A sanção de impedimento de licitar e contratar prevista no item III também aplicável em quaisquer das hipóteses previstas como infração administrativa deste Termo de Referência.

8.4 Serão descontados dos pagamentos porventura devidos à CONTRATADA as importâncias alusivas a multas, ou efetuar sua cobrança mediante inscrição na dívida ativa do Estado, ou por qualquer outra forma prevista em lei.

8.5 Caso a CONTRATANTE determine, a multa deverá ser recolhida no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

8.6 Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a CONTRATANTE poderá cobrar o valor remanescente judicialmente.

8.7 A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

8.8 Se, durante o processo de aplicação de penalidade, houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846/2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou processo administrativo.

8.9 A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846/2013, seguirão seu rito normal na unidade administrativa.

9. ACORDO DE NÍVEL DE SERVIÇO (SLA)

9.1 Os chamados de suporte técnico serão classificados conforme o nível de severidade, com base no impacto causado no ambiente computacional da CONTRATANTE, conforme as tabelas a seguir:

9.1.1 Impacto:

Nível	Descrição do Impacto
1	Serviços totalmente indisponíveis
2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos
3	Acesso aos aplicativos

9.1.2 Níveis de Severidade:

Modalidade	Prazo	Níveis de Severidade		
		1	2	3
Remoto	Início do Atendimento	1 hora	4 horas	8 horas
	Solução do Contorno	8 horas	12 horas	24 horas

9.2 Quando for necessário atendimento presencial, a CONTRATADA deverá disponibilizar técnicos para resolver os problemas no local. Preferencialmente, essas atividades devem ser previamente acordadas entre as partes, exceto em casos de severidade máxima ou evidente indisponibilidade da infraestrutura da CONTRATANTE.

9.3 O início do atendimento será considerado a partir da abertura do chamado técnico.

9.4 O atendimento será considerado encerrado quando a solução estiver disponível e funcionando perfeitamente no local de instalação.

9.5 Durante toda a vigência do contrato, a CONTRATANTE poderá abrir chamados ilimitados para suporte técnico.

9.6 A CONTRATADA será integralmente responsável por quaisquer danos ou prejuízos causados ao patrimônio da CONTRATANTE ou de terceiros, decorrentes de ações ou omissões de seus colaboradores durante a execução dos serviços solicitados.

9.7 Qualquer atividade relacionada a configurações, ajustes ou parametrizações após a implantação deverá ser precedida da abertura de um chamado técnico.

9.8 Caso a atividade seja realizada de forma proativa, a CONTRATADA deverá comunicar à CONTRATANTE, via e-mail, justificando a execução antecipada.

9.9 Se alguma atividade exigir a interrupção da solução, a CONTRATANTE deverá ser imediatamente notificada para autorizar ou reagendar a execução.

9.10 Atualizações que impliquem indisponibilidade do ambiente devem ser previamente agendadas com a equipe técnica da CONTRATANTE.

9.11 A CONTRATADA deverá manter uma Central de Atendimento em português (Brasil), operando 24 horas por dia, 7 dias por semana, durante todo o ano (24x7x365), para abertura de chamados e demais comunicações.

9.12 A CONTRATANTE poderá solicitar serviços específicos por meio dos seguintes canais de comunicação:

a) E-mail;

b) Telefone 0800;

c) Sistema de Chamados Web.

9.13 O serviço será considerado concluído somente após a confirmação da área técnica da CONTRATANTE quanto à sua execução satisfatória.

9.14 O encerramento de solicitações técnicas dependerá da anuência de ambas as partes: CONTRATADA e CONTRATANTE.

9.15 A CONTRATADA manterá um cadastro com os nomes das pessoas indicadas pela CONTRATANTE autorizadas a abrir e encerrar chamados.

9.16 O prazo para encerramento do atendimento não poderá ultrapassar os limites estabelecidos para cada nível de criticidade.

9.17 Considera-se suporte técnico as atividades que requerem acompanhamento por parte de um técnico da CONTRATANTE.

9.18 Quando for necessário atendimento local, o cronograma de execução deverá ser acordado entre as partes.

9.19 A CONTRATADA deverá iniciar o atendimento conforme os prazos definidos para cada nível de criticidade.

9.20 A manutenção corretiva inclui os serviços necessários para restaurar o funcionamento adequado dos equipamentos, com fornecimento de peças conforme especificações do fabricante, em caso de falhas ou defeitos de hardware.

9.21 A CONTRATADA deverá realizar os serviços de manutenção com ferramentas próprias e técnicos especializados, devidamente identificados.

9.22 O suporte técnico compreende ações para restabelecer o funcionamento correto das soluções contratadas, incluindo configuração, habilitação, implementação, manutenção e colocação em produção de funcionalidades.

9.23 Caso seja necessária a atualização de firmware, a CONTRATADA deverá fornecer o pacote de software e realizar a atualização.

9.24 Considerando que a resolução de problemas de software pode envolver o desenvolvimento de patches, admite-se a adoção de soluções de contorno (workaround) até a implementação da solução definitiva.

9.25 O período para solução de ocorrências de software será contado entre a formalização e o encerramento efetivo da ocorrência, seja com solução definitiva ou provisória.

9.26 Para ocorrências de hardware não resolvidas dentro do prazo, a CONTRATADA deverá substituir o equipamento ou módulo defeituoso em até 72 (setenta e duas) horas úteis. Após a substituição, deverá ser entregue um documento com as descrições e números de série dos equipamentos substituídos e novos.

9.27 A substituição definitiva de hardware deverá ser feita com equipamento novo, original, recomendado pelo fabricante, com configuração igual ou superior à do substituído.

9.28 Durante a substituição, a CONTRATADA deverá entregar documento contendo a descrição e número de série do equipamento defeituoso e do novo equipamento.

9.29 O prazo para solução de ocorrências de hardware será contado entre a formalização e o encerramento efetivo da ocorrência. Quando houver substituição, o encerramento será considerado apenas após o novo equipamento entrar em operação.

9.30 Para cálculo do tempo de atendimento, serão desconsiderados os períodos em que a CONTRATANTE estiver responsável por ações necessárias à análise e solução da ocorrência.

9.31 Não haverá limitação quanto ao número de técnicos da CONTRATANTE autorizados a abrir chamados, desde que previamente registrados como pontos de contato.

9.32 Durante o período de garantia, a CONTRATADA deverá fornecer todas as atualizações de software (versões, releases, patches), firmware ou microcódigos dos hardwares cobertos pela manutenção, sem custo adicional.

10. FORMA DE PAGAMENTO

10.1 O pagamento será realizado à CONTRATADA de forma integral e condicionado ao marco da emissão do Termo de Recebimento Definitivo do objeto assinado por ambas partes;

10.2 O pagamento devido à CONTRATADA será creditado em conta-corrente por meio de ordem bancária, efetuado mediante apresentação de DANFE com o devido “atesto” de recebimento pela fiscalização da PGJ.

10.2.1 O documento fiscal, emitido em conformidade com o Protocolo ICMS 42/2009 (NF-e), deverá estar devidamente discriminado, em nome da PROCURADORIA-GERAL DE JUSTIÇA, CNPJ n.º 04.153.748/0001-85, e acompanhada das respectivas Certidões Negativas de Débito para com a Seguridade Social, para com o Fundo de Garantia por Tempo de Serviço, junto à Justiça Trabalhista e, ainda, das certidões de regularidade junto à Fazenda Federal, Estadual e Municipal, conforme o disposto no artigo 68 da Lei nº 14.133/2021, bem como da formalização do pedido de pagamento e do recibo a PGJ;

10.2.2 Deverão constar do documento fiscal as especificações dos produtos, o número da Nota de Empenho e da Ata/Contrato, conforme o caso; e

10.2.3 Enquanto pendente de liquidação, por obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência contratual, nenhum pagamento será efetuado à Contratada, sem que isso gere direito a acréscimos de qualquer natureza.

10.2.4 Na emissão da nota fiscal/fatura, a CONTRATADA deverá atentar para as orientações de retenção tributária na legislação aplicável.

10.3 Qualquer atraso ocorrido na apresentação do DANFE, ou dos documentos exigidos como condição de pagamento por parte da Contratada, importará prorrogação automática do prazo de vencimento da obrigação do Contratante.

10.4 Nenhum pagamento isentará o fornecedor das responsabilidades atinentes ao objeto contratual, nem tampouco implicará a aprovação definitiva da entrega, total ou parcialmente.

10.5 O documento fiscal, devidamente atestado, e os documentos exigidos neste Termo, no Edital e na Ata/Contrato, para fins de liquidação e pagamento das despesas, deverão ser entregues no Setor de Protocolo da Contratante (email: protocolo@mpam.mp.br) e na Diretoria de Tecnologia da Informação e Comunicação (e-mail: dtic@mpam.mp.br).

10.6 Como condição para emissão da Nota de Empenho, a licitante vencedora manterá a condição de habilitação, cuja confirmação será feita através de consulta ao SICAF ou através da *internet* nos respectivos *sites* dos órgãos emissores das certidões de regularidade fiscal.

10.7 Como condição inafastável a que seja emitida Nota de Empenho à Contratada, esta deverá, também, estar cadastrada junto ao Sistema de Administração Financeira e Contabilidade – Cadastramento de Credores – da Secretaria da Fazenda do Estado do Amazonas – SEFAZ.

11. ESPECIFICAÇÕES TÉCNICAS DO OBJETO

11.1 O objeto deste Termo compreende a contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais do Ministério Público do Estado do Amazonas (MPAM).

11.2 Por tratar-se de solução integrada, onde o funcionamento efetivo e satisfatório depende de cada um dos seus itens em conjunto, como um todo, ou seja, o simples funcionamento de itens separadamente não tem nenhuma funcionalidade, conforme indicado no Estudo Técnico Preliminar (ETP), a contratação terá lote único, organizado conforme tabela a seguir:

ITEM	DESCRIÇÃO	QU
01	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9	
02	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU	
03	SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX	
04	SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU	
05	LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE	
06	SOFTWARE DE BACKUP DE DADOS	
07	EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	
08	SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	
09	SWITCH CORE	

11.3 Nas especificações técnicas mínimas apresentadas a seguir, os termos "possui", "permite", "suporta" e "é" implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo "ou" implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo "e" implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções citadas.

11.4 A CONTRATADA não poderá oferecer serviço inferior as especificações apresentadas neste Termo, sendo permitido, porém, a oferta de serviço superior as especificações mínimas apresentadas, de acordo com a conveniência da CONTRATADA e aprovação do CONTRATANTE.

11.5 Toda documentação gerada durante a prestação dos serviços será de propriedade do CONTRATANTE, em virtude de sua elaboração tomar por base informações críticas do funcionamento intrínseco à sua infraestrutura, que afetam diretamente a segurança do CONTRATANTE.

11.6 A CONTRATADA deverá guardar inteiro sigilo dos serviços contratados e dos dados processados, bem como de toda e qualquer documentação gerada, reconhecendo serem esses de propriedade e uso exclusivo do CONTRATANTE, sendo vedada sua cessão, locação ou venda a terceiros.

11.7 CONTRATADA deverá manter o CONTRATANTE atualizado sobre todos os fluxos adotados para a execução das atividades objeto da contratação durante o período contratual, bem como sobre a forma de automatização de quaisquer serviços, documentando todos os procedimentos detalhadamente para que possam servir de base para a continuidade dos serviços independentemente da metodologia que possa ser adotada.

11.8 ITEM 01 - EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9

11.8.1 Características Gerais

11.8.1.1 A infraestrutura deverá ser composta por appliances Nutanix com integração completa entre hardware e software, armazenamento e rede, entregando uma solução hiperconvergente pronta para operação.

11.8.1.2 Serão aceitos apenas appliances homologados pela Nutanix para uso com o Nutanix AOS (Acropolis Operating System) e Nutanix AHV (Acropolis Hypervisor) ou outro hipervisor suportado pela plataforma.

11.8.1.3 Caso necessário, será permitida a entrega de equipamentos ou recursos adicionais para atender aos requisitos mínimos, desde que todos os componentes estejam integrados e certificados pela Nutanix.

11.8.1.4 É permitida a entrega de múltiplos nós em um único chassi, desde que compatível com a arquitetura Nutanix.

11.8.1.5 A solução deve incluir a ferramenta unificada de monitoração, em sua ultima versão ou equivalente, que oferece gerenciamento centralizado e interface gráfica para monitoramento, atualizações e operação da infraestrutura, incluindo:

11.8.1.5.1 Atualização de BIOS, firmware, hipervisor e SDS;

11.8.1.5.2 Visualização do hardware físico;

11.8.1.5.3 Diagnóstico, inventário e expansão de nós.

11.8.1.6 Caso alguma funcionalidade não esteja disponível na ferramenta unificada ou equivalente para monitoramento ou atualização, a CONTRATADA deverá realizar este serviço de forma remota/on-line ou presencial.

11.8.1.7 Todas as atualizações devem ser homologadas pela Nutanix e aplicadas conforme as melhores práticas da fabricante. Esta ferramenta deve ser gráfica, com suporte a apresentação de visões do hardware físico dos nós, suporte a troca de drives, com controle do inventário, com ferramenta de diagnóstico e com módulo para a adição de novos nós.

11.8.1.8 A arquitetura deve garantir alta disponibilidade (HA) e resiliência a falhas, com suporte a recuperação de desastres (DR).

11.8.1.9 Os appliances devem permitir expansão modular e não disruptiva dos serviços de rede e aplicações, com detecção automática de novos nós.

11.8.1.10 Deve centralizar o armazenamento de dados em discos compartilhados, redundantes.

11.8.1.11 Cada nó deverá conter armazenamento dedicado para o sistema operacional da plataforma.

11.8.1.12 A solução deve estar preparada para ambientes de virtualização em alta disponibilidade, conforme as práticas recomendadas pela Nutanix.

11.8.1.13 Deve suportar software de virtualização para consolidação de servidores e recuperação automática em caso de falhas físicas, minimizando o downtime.

11.8.1.14 A entrega deve ser feita com todos os componentes física e logicamente integrados, sem ponto único de falha, com acesso imediato ao ambiente via sistema de gestão da plataforma após energização e conexão.

11.8.1.15 A instalação deve ser compatível com racks padrão de 19 polegadas, incluindo todos os acessórios necessários para montagem no ambiente da CONTRATANTE.

11.8.1.16 O equipamento deve integrar a linha de produtos Nutanix da família “NX”, assegurando total compatibilidade com atual ambiente e possibilidade de expansão das zonas de disponibilidade já estabelecidas, conforme informações disponibilizadas no endereço eletrônico oficial da fabricante: https://www.nutanix.com/products/hardwareplatforms/specsheet?platformProvider=Nutanix

11.8.2 Configuração do Nó ou Chassi

11.8.2.1 Serão admitidas ofertas de chassis que comportam múltiplos servidores (nós/nodes), para o atendimento da especificação técnica.

11.8.2.2 Cada nó, ou chassi, deverá possuir ventiladores e fontes redundantes para a operação adequada dos equipamentos.

11.8.2.3 Todas as fontes de alimentação deverão ser acompanhadas de seus respectivos cabos de energia compatíveis.

11.8.3 Características de Processamento por Nó

11.8.3.1 Cada servidor deverá possuir, no mínimo, 02 (dois) processadores com arquitetura x86, voltados ao uso em servidores, contendo as seguintes características mínimas:

11.8.3.1.1 12 (doze) núcleos físicos e 24 (vinte e quatro) threads por processador;

11.8.3.1.2 Frequência de clock nominal de, no mínimo, 2,4 GHz;

11.8.3.1.3 Controladora de memória integrada com suporte à tecnologia DDR5 ou superior.

11.8.3.2 Será admitida a entrega de processadores de geração superior ao modelo originalmente especificado, desde que mantenham no mínimo a mesma quantidade de núcleos e threads, independentemente de demais especificações.

11.8.4 Especificações de Memória por Nó

11.8.4.1 Cada servidor deverá ser fornecido com, no mínimo, 1536 GB (um mil quinhentos e trinta e seis gigabytes) de memória RAM, distribuída uniformemente entre os processadores, utilizando módulos DDR5 ou superior.

11.8.5 Especificações de Rede por Nó

11.8.5.1 Cada servidor deverá ser entregue com as seguintes interfaces de rede:

11.8.5.1.1 Mínimo de 2 (duas) interfaces de 25/10 GbE SFP28, integradas em uma placa de rede;

11.8.5.1.2 Mínimo de 1 (uma) interface exclusiva de gerenciamento Ethernet 1000Base-T.

11.8.5.2 A interface de gerenciamento deverá vir acompanhada de cabos UTP categoria 6 (ou superior), com comprimento mínimo de 5 (cinco) metros e conectores RJ-45.

11.8.6 Especificações de Armazenamento por Nó

11.8.6.1 Cada servidor deverá ser entregue com a seguinte configuração mínima de discos:

11.8.6.1.1 04 (quatro) unidades de SSD NVMe, ou SSD SAS/SATA, com capacidade mínima de 3,84 TB por unidade (volumetria bruta);

11.8.6.1.2 08 (oito) unidades de disco rígido (HDD), com capacidade mínima de 12 TB por unidade (volumetria bruta).

11.9 ITEM 02 - EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU

11.9.1 Características Gerais

11.9.1.1 A solução deverá ser composta exclusivamente por appliances de nuvem privada, com integração total entre recursos de computação, armazenamento e rede, entregues como infraestrutura unificada.

11.9.1.2 Serão aceitos apenas appliances homologados para uso com a solução de armazenamento definido por software (Software Defined Storage – SDS) ofertada.

11.9.1.3 A entrega de equipamentos ou recursos adicionais será aceita, desde que necessária para o atendimento aos requisitos mínimos e que todos os componentes estejam devidamente integrados.

11.9.1.4 É permitida a entrega de múltiplos nós consolidados em um único chassi modular.

11.9.1.5 A solução deverá incluir ferramenta unificada de gerenciamento e atualização, com capacidade de monitorar e atualizar BIOS, firmwares, hypervisor e componentes do SDS. Caso não realize todos os procedimentos listados, a CONTRATADA deverá garantir a execução dessas tarefas online e / ou presencial.

11.9.1.6 A ferramenta de gestão deverá ser gráfica, com visualização física dos nós, suporte à substituição de drives, inventário automatizado, diagnóstico integrado e capacidade de adicionar novos nós ao cluster.

11.9.1.7 A arquitetura deverá contemplar alta disponibilidade nativa e recursos para recuperação de desastres (DR), de forma a garantir continuidade dos serviços mesmo em caso de falhas parciais.

11.9.1.8 Os equipamentos devem possuir arquitetura modular, permitindo expansão de capacidade com inclusão de novos appliances sem interrupção dos serviços.

11.9.1.9 O armazenamento deverá ser centralizado, com discos compartilhados e redundância nativa.

11.9.1.10 Cada servidor deverá conter unidade de armazenamento dedicada ao sistema operacional da plataforma e aos softwares de virtualização , processamento gráfico e calculo aritmético.

11.9.1.11 A infraestrutura deverá estar preparada para suportar ambientes virtualizados de alta disponibilidade, de acordo com as boas práticas do fabricante da solução.

11.9.1.12 A solução deverá oferecer suporte a consolidação de servidores e recuperação automática em caso de falhas de hardware.

11.9.1.13 A entrega deverá ocorrer com a solução fisicamente e logicamente pré-integrada, sem ponto único de falha, com acesso imediato à plataforma após energização e conexão física.

11.9.1.14 A instalação deverá ser compatível com racks padrão de 19"(dezenove polegadas), com todos os acessórios de fixação inclusos.

11.9.1.15 O equipamento deve integrar a linha de produtos Nutanix da família “NX”, assegurando total compatibilidade com atual ambiente e possibilidade de expansão das zonas de disponibilidade já estabelecidas, conforme informações disponibilizadas no endereço eletrônico oficial da fabricante: https://www.nutanix.com/products/hardwareplatforms/specsheet?platformProvider=Nutanix

11.9.2 Configuração do Nó ou Chassi

11.9.2.1 Serão admitidas ofertas de chassis que comportam múltiplos servidores (nós/nodes), para o atendimento da especificação técnica.

11.9.2.2 Cada nó ou chassi deverá possuir ventiladores e fontes de alimentação redundantes.

11.9.2.3 Cada fonte deverá ser entregue com seu respectivo cabo de energia.

11.9.3 Características de Processamento por Nó

11.9.3.1 Cada servidor deverá possuir, no mínimo, dois processadores com arquitetura x86, dedicados a ambientes de datacenter, com as seguintes características mínimas:

11.9.3.2 12 (doze) núcleos físicos e 24 (vinte e quatro) threads por processador;

11.9.3.3 Frequência mínima de 2,4 GHz;

11.9.3.4 Controladora de memória integrada DDR5 ou superior.

11.9.3.5 A substituição por processadores mais recentes será aceita, desde que observadas as quantidades mínimas de núcleos e threads.

11.9.4 Especificações de Memória por Nó

11.9.4.1 Cada servidor deverá ser entregue com no mínimo 1024 GB (um mil e vinte e quatro gigabytes) de memória RAM, utilizando módulos DDR4 ou superior, distribuídos de forma equilibrada entre os processadores.

11.9.5 Especificações de Rede por Nó

11.9.5.1 Cada servidor deverá conter no mínimo:

11.9.5.1.1 2 (duas)interfaces de rede 25/10 GbE SFP28;

11.9.5.1.2 1 (uma) interface de gerenciamento 1000Base-T;

11.9.5.1.3 A interface de gerenciamento deverá ser acompanhada de cabos UTP Cat-6 ou superior, com 5 metros de comprimento e conectores RJ-45.

11.9.6 Especificações de Armazenamento por Nó

11.9.6.1 Cada servidor deverá ser fornecido com a seguinte configuração de discos:

11.9.6.1.1 2 discos SSD NVMe, SAS ou SATA, com capacidade mínima de 3,84 TB cada (volumetria bruta);

11.9.6.1.2 4 discos HDD com capacidade mínima de 12 TB cada (volumetria bruta).

11.9.7 Especificações de Processamento Gráfico e Cálculo Aritmético

11.9.7.1 Cada servidor deverá conter uma placa gráfica com as seguintes características mínimas:

11.9.7.1.1 48 GB de memória GDDR6 de GPU;

11.9.7.1.2 Interconexão PCIe Gen4 com largura de banda de 64 GB/s;

11.9.7.1.3 Suporte a DirectX 12.075, Shader Model 5.175, OpenGL 4.686 e Vulkan 1.186;

11.9.7.1.4 Compatibilidade com NVIDIA vPC/vApps, NVIDIA RTX Virtual Workstation e NVIDIA Virtual Compute Server;

11.9.7.1.5 Consumo máximo de 350W.

11.10 ITEM 03 – SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX

11.10.1 Camada de Armazenamento da Solução:

11.10.1.1 A solução deverá contar com camada de armazenamento compartilhada entre todos os servidores e appliances descritos neste Termo, utilizando tecnologia de armazenamento definido por software (Software Defined Storage – SDS).

11.10.1.2 A arquitetura de armazenamento deverá ser otimizada para ambientes virtuais, com escalabilidade contínua e elástica, permitindo expansão de capacidade pela adição de novos nós/appliances sem necessidade de licenciamento adicional de virtualização.

11.10.1.3 Não serão aceitas soluções baseadas em tecnologia RAID para redundância de dados.

11.10.1.4 A solução deverá suportar as tecnologias de compressão e desduplicação de dados inline, near-line ou pós-processada, com o objetivo de otimização do armazenamento.

11.10.1.5 A solução deverá prover recursos de QoS (Quality of Service), para controle do volume de I/Os de VMs.

11.10.1.6 Deverá permitir uso de técnicas de Erasure Coding para otimização de aplicações com baixa sensibilidade à latência de escrita.

11.10.1.7 A solução deverá permitir a expansão do cluster através da adição de nós/servidores que incrementem tão somente a capacidade de armazenamento, sem a necessidade de emprego de licenças de virtualização nesses nós/servidores;

11.10.1.8 A substituição de discos defeituosos deverá ocorrer sem impacto nas operações de leitura e escrita das aplicações.

11.10.1.9 A falha de um nó da solução não poderá comprometer a disponibilidade da camada de armazenamento das VMs.

11.10.1.10 A criptografia deverá ser aplicada em nível de cluster ou volume, via hardware ou software, com KMS nativo. Caso não possua, será aceita entrega de servidor redundante externo com essa funcionalidade.

11.10.1.11 A distribuição dos dados deverá ocorrer de forma automática e uniforme dentro do cluster.

11.10.1.12 A solução deverá permitir criação de cópias no tempo (snapshots) sem movimentação dos dados originais e com redirecionamento de escritas subsequentes.

11.10.1.13 Deverá suportar clonagem de instâncias virtuais a partir de snapshots, sem movimentação dos dados.

11.10.1.14 Acesso ao armazenamento deverá ser possível via iSCSI por instâncias físicas ou virtuais externas ao cluster, garantindo suporte a aplicações de alta disponibilidade.

11.10.2 Tecnologia de Replicação e Proteção de Dados:

11.10.2.1 Deverá ser fornecida funcionalidade de replicação local realizando clones e snapshots com proteção contínua dos dados da máquina virtual;

11.10.2.2 A solução deve prover as funcionalidades de Thin Provisioning e Serviços de Cópias de dados;

11.10.2.3 Deverá permitir a configuração de um grupo ou domínio de proteção de instâncias virtuais, que poderão ser protegidas por cópias point-in-time, bem como replicadas para um cluster remoto;

11.10.2.4 Deverá permitir a união de máquinas virtuais em um único grupo de proteção.

11.10.2.5 Deverá proteger, por cópias point-in-time, simultaneamente todas as máquinas virtuais pertencentes ao grupo;

11.10.2.6 Deverá contemplar, também, a proteção nativa de máquinas virtuais consistentes com aplicações, onde há proteção dos dados em memória a partir da movimentação das operações de escrita para disco, de sistemas operacionais Linux e Windows. Caso a plataforma de nuvem privada não permita executar esta funcionalidade nativamente, a CONTRATADA deverá atender este requisito compondo com outra solução.

11.10.2.7 Deverá permitir a configuração de uma entidade capaz de centralizar todo o fluxo do tráfego replicado entre clusters distintos, convergindo assim os recursos para um único ponto focal. Esse recurso centralizado deverá posteriormente redirecionar o tráfego corretamente para os equipamentos específicos do cluster de contingência;

11.10.2.8 Deverá permitir ajustar o consumo de banda em replicações;

11.10.2.9 Deverá permitir a existência de frequências distintas de replicação para instâncias virtuais em grupos diferentes;

11.10.3 Gerenciamento Integrado:

11.10.3.1 A solução deve oferecer solução de gerenciamento integrado, licenciado para gerenciar inclusive múltiplos clusters.

11.10.3.2 Monitoração automática e periódica da solução, com o envio de notificações preventivamente em caso de falhas, notificando o suporte do fornecedor a tomar medidas preventivas e acordadas com a CONTRATANTE a fim de evitar tempo de inatividade e impactos na produção.

11.10.3.3 Deve oferecer portal de acesso do próprio fornecedor para download de atualizações e de softwares agregados.

11.10.3.4 A ferramenta de gerenciamento, local, deve fornecer um dashboard reportando a utilização dos recursos do cluster como CPU, Memória, Armazenamento, IOPS do cluster, largura de banda do cluster, latência do cluster e informações sobre o virtualizador empregado e os alertas de saúde.

11.10.3.5 A solução deve fornecer atualização de todos os componentes (Firmware, e softwares de virtualização que fazem parte da solução) em forma de pacote com instalação assistida.

11.10.3.6 Contemplar as funcionalidades como:

11.10.3.6.1 Emissão de relatório avançados do ambiente;

11.10.3.6.2 Personalização da console principal;

11.10.3.6.3 Planejamento e previsão de capacidade;

11.10.3.6.4 Detecção de ineficiência de cargas de trabalho e dimensionamento ideal;

11.10.3.6.5 Planejamento de capacidade ou cargas de trabalho ao longo do tempo;

11.10.3.6.6 Permitir automação de operações de gerência do ambiente

11.10.4 Provisionamento de Containers:

11.10.4.1 Deverá ser entregue uma plataforma de provisionamento de containers, integrada, a plataforma de virtualização.

11.10.4.2 A plataforma deverá permitir a criação de múltiplo clusters.

11.10.4.3 A fabricante da solução deverá, comprovadamente, pertencer a categoria de membro da CNCF (Cloud Native Computing Foundation).

11.10.4.4 Seleção de sistemas operacionais, bem como suas distintas versões de microcódigo para implementação automática, sendo compatível com sistemas Linux.

11.10.4.5 Seleção das configurações de rede do cluster de containers ou microserviços.

11.10.4.6 Seleção do tipo de armazenamento persistente a ser empregado em containers.

11.10.4.7 Seleção da quantidade de nós dos tipos “Control Plane” e “Workers” que serão implementados simultaneamente.

11.10.4.8 A plataforma de containers deverá permitir a criação de alertas, facilitando a gestão do cluster.

11.10.4.9 Deverá ter suporte a implementação de clusters de plataformas de containers, similares a Kubernetes, NCI,

baremetal, public cloud.

11.10.4.10 A plataforma de containers deverá possuir integração para o acesso através de RBAC, permitindo seu uso completo através de acesso administrativo e permitindo seu uso parcial através de acesso controlado aos demais usuários.

11.10.4.11 Suporte implementação de clusters de plataformas de containers, similares a Kubernetes com suporte a Bring-Your-Own-OS: Rocky Linux, Ubuntu, RHEL e similares.

11.10.4.12 Permitir a configuração de clusters com alta-disponibilidade para os “Control Plane” nodes, com ou sem balanceador de carga;

11.10.4.13 Prover armazenamento persistente através de integração com Container Storage Interface (CSI), para armazenamento de blocos e arquivos. Também deverá ser possível configurar armazenamento de arquivos compatível com protocolo Simple Storage Service;

11.10.4.14 Deverá fornecer um mecanismo de monitoramento que aciona alertas no cluster Kubernetes;

11.10.4.15 Oferecer as seguintes funcionalidades em ambiente Kubernetes:

11.10.4.15.1 Gerenciamento de Dados;

11.10.4.15.2 Proteção e Restauração de Dados;

11.10.4.15.3 Aceleração da Entrega de Aplicativos;

11.10.4.15.4 Gerenciamento de Autoatendimento de Aplicativos;

11.10.4.15.5 Automação e Monitoramento de Infraestrutura;

11.10.4.15.6 Padronização de Políticas de Governança e Conformidade;

11.10.4.16 Para a estratégia de criação de cópias dos dados para ambiente de containers Kubernetes, a solução deverá permitir:

11.10.4.16.1 Fornecimento de software para “worker nodes” Kubernetes, garantindo o suporte unificado e conjunto da solução como um todo;

11.10.4.16.2 Plataformas de container baseadas em Kubernetes.

11.10.4.16.3 Permitira realização de copias e armazenamento em repositório externo.

11.10.4.16.4 Movimentação das imagens de backup para compartilhamentos NFS por meio de solução de armazenamento compatível com protocolo S3, permitindo que o repositório NFS seja utilizado como backend de Object Storage.

11.10.4.16.5 Capacidade de restaurar o Namespace para seu local original e para um novo Namespace.

11.10.5 Segurança de Rede:

11.10.5.1 Suportar microssegmentação para prover controle granular e governança de todo o tráfego de entrada e saída de uma máquina virtual (VM), grupos de máquinas virtuais (VMs) e containers.

11.10.5.2 Permitir a associação de políticas de rede a VMs e conteiners em vez de segmentos de rede específicos (por exemplo VLANs) ou identificadores (endereços IP ou MAC).

11.10.5.3 Prover visualização de tráfego e relacionamentos com a descoberta automática dos fluxos entre as máquinas virtuais e containers.

11.10.5.4 Permitir políticas de segurança centradas na carga de trabalho em vez de uma abordagem centrada na rede, permitindo examinar o tráfego de, e para as VMs, independentemente de como as configurações de rede mudam e onde residem no data center

11.10.5.5 Políticas aplicadas por categorias de VMs e containers.

11.10.5.6 Permitir isolamento de conteiners e VMs comprometidas, colocando-a em quarentena.

11.10.5.7 - Permitir restrição de tráfego entre camadas de aplicação.

11.10.5.8 Atualização automática de políticas.

11.10.5.9 Integração com ferramentas de terceiros como IDS/IPS e load balancer.

11.10.6 Licenciamento do Software de Virtualização:

11.10.6.1 Entrega do licenciamento completo da plataforma de virtualização, versão mais avançada.

11.10.6.2 Suporte à criação de VMs com múltiplas interfaces de rede e múltiplas arquiteturas (32/64 bits).

11.10.6.3 Permitir provisionamento aos principais sistemas operacionais (Windows Server 2022, CentOS 8, Ubuntu 20, RHEL 9) ou superiores.

11.10.6.4 Alocação dinâmica de recursos (CPU/RAM).

11.10.6.5 Hypervisor deverá estar instalado em unidade flash dedicada.

11.10.6.6 Suporte a GPU virtual ou passthrough nativo.

11.10.6.7 Suporte a BIOS/UEFI, snapshots, exportação OVA.

11.10.6.8 Deverá permitir o provisionamento de máquinas virtuais, e grupos de máquinas virtuais, em equipamentos específicos com o propósito de respeitar licenciamentos de aplicações. Em caso de falha do equipamento, a máquina virtual não deverá ser migrada para outro equipamento remanescente;

11.10.6.9 Alta resiliência a falhas de nós/discos.

11.10.6.10 Armazenamento distribuído e gerenciado via console web.

11.10.6.11 Deverá permitir a inicialização, a reinicialização, o reset, o desligamento da VM e o desligamento do sistema operacional dela;

11.10.6.12 Suportar a tecnologia de snapshot nativos do Hypervisor;

11.10.6.13 Permitir a adição de novos servidores no cluster;

11.10.6.14 Permitir criar uma área de armazenamento compartilhada, distribuída e otimizada para ambientes virtuais;

11.10.6.15 Permitir o agrupamento dos volumes lógicos de todos os servidores no cluster provendo uma área de armazenamento comum para o ambiente virtual;

11.10.6.16 Possuir mecanismo de redundância e proteção de dados nativo que armazena cópias dos dados em diversos

discos e hosts do cluster de forma transparente;

11.10.6.17 Deverá ser fornecido licenciamento do software de virtualização na versão mais completa para todos os servidores do ambiente de armazenamento distribuído.

11.10.6.18 Deverá contemplar pelo menos 20 (vinte) núcleos de processamento virtuais (vCPU) ou físicos (pCPU) de solução para gestão de base de dados como serviço (DBaaS).

11.10.6.19 Deverá ser totalmente compatível com a solução ofertada para atendimento aos requisitos deste termo de referência.

11.10.6.20 Permitir automatizar as tarefas para provisionamento, emprego de correções de software (patching), gerenciamento do ciclo de vida, clonagem, atualização dos dados em bases clonadas (refresh), proteção contínua e recuperação de bases de dados.

11.10.6.21 Deverá ser compatível pelo menos com Oracle, Microsoft SQL, PostgreSQL, MariaDB, MongoDB e MySQL.

11.10.6.22 Permitir o uso de uma chave SSH pública para acesso ao servidor de banco de dados com opção através do upload de um arquivo e através da inserção direta da chave em campo de texto.

11.10.6.23 A solução deverá permitir registrar bancos de dados existentes para emprego de proteção contínua capturando e mantendo snapshots e registros (logs) transacionais da base de dados de origem conforme definições contidas no agendamento.

11.10.6.24 A mesma tecnologia deverá permitir a clonagem de bases de dados.

11.10.6.25 Durante a clonagem, a solução deverá permitir a escolha para o administrador utilizar um servidor de banco de dados registrado ou criar um novo servidor.

11.10.6.26 Permitir que o administrador realize o clone de uma base de dados a partir de um snapshot.

11.10.6.27 Permitir que o administrador realize o clone de uma base de dados dentro de uma política de proteção contínua, ou seja, clonar uma base de dados em determinado dia, hora, minuto e segundo.

11.10.6.28 Permitir a definição de agendamento da periodicidade para realizar a atualização (refresh) dos dados da base clonada através do estado atual na base de dados de origem.

11.10.6.29 Permitir a definição de uma data para remoção ou exclusão do clone.

11.10.6.30 Permitir a execução de scripts ou comandos de pré e pós clonagem.

11.10.6.31 Deverá ser possível definir as políticas de retenção dos snapshots diários, semanais, mensais e trimestrais.

11.11 ITEM 04 – SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU

11.11.1 Software para Processamento Gráfico e Cálculo Aritmético:

11.11.1.1 Permitir a seleção, implantação e gestão de modelos de IA Generativa (LLMs) provenientes da Hugging Face e NVIDIA, bem como a importação de modelos personalizados ou treinados pelo contratante em clusters Kubernetes.

11.11.1.10 Permitir a criação de um endpoint de inferência e o compartilhamento dele com desenvolvedores para incorporar em seus aplicativos de IA. Permitir gerenciar e validar esses endpoints para garantir que eles estejam configurados corretamente.

11.11.1.11 Permitir o acesso a um endpoint de inferência por um aplicativo usando chaves de API. O gerenciamento de chaves de API deverá permitir o fornecimento e revogação do acesso à API para garantir controles de segurança de acesso adequados.

11.11.1.12 Permitir o controle de acesso baseado em função (RBAC), para fornecer permissões de acesso personalizadas aos usuários com base em suas funções atribuídas.

11.11.1.13 Possuir uma interface de usuário simples e dinâmica que simplifique o processo de implantação.

11.11.1.14 Possuir um painel dinâmico que permita monitorar a integridade da implantação com ferramentas de monitoramento em tempo real que identifiquem gargalos, rastreiem o desempenho e solucionem problemas.

11.11.1.15 Suportar a instalação e o funcionamento em estruturas sem qualquer conexão com a Internet (dark-site ou air-gapped).

11.12 ITEM 05 - LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE

11.12.1 A solução deverá incluir unidade de subscrição de software para armazenamento de objetos e arquivos, licenciada por terabyte (TB), com suporte técnico durante 60 (sessenta) meses, contemplando ambiente de produção em operação contínua (24x7).

11.12.2. Caso a solução proposta não ofereça suporte nativo a armazenamento de objetos e arquivos, será permitida a utilização de unidade externa dedicada, desde que esta disponha de todos os componentes, funcionalidades e suporte equivalentes à solução principal.

11.12.3. O sistema de armazenamento definido (SDS) deverá otimizar dados utilizando tecnologia de erasure coding na camada de capacidade, de modo a garantir eficiência e resiliência no armazenamento de arquivos e objetos.

11.12.4. A solução deverá permitir a recuperação granular de arquivos pelos usuários, sem necessidade de intervenção do administrador.

11.12.4.1 Para o protocolo SMB, a restauração deverá ocorrer por meio da funcionalidade “Versões Prévias” da pasta de destino.

11.12.4.2 Para o protocolo NFS, a recuperação deverá ser possível pela listagem do subdiretório oculto (snapshot).

11.12.5. O sistema deverá integrar-se a softwares antivírus de terceiros por meio do protocolo ICAP (Internet Content Adaptation Protocol), possibilitando varredura em tempo real de arquivos compartilhados via SMB sempre que forem abertos, modificados ou encerrados.

11.12.6. A interface de gerenciamento deverá exibir o estado dos arquivos após a varredura antivírus, incluindo status como limpo, em quarentena ou deletado, além do histórico de eventos correspondentes.

11.12.7. A interface de gerenciamento deverá também exibir relatórios detalhados contendo a lista de arquivos analisados, ameaças detectadas e arquivos colocados em quarentena.

11.12.8. A interface de gerenciamento deverá permitir ações diretas sobre os arquivos, incluindo:

11.12.8.1. Reexecução de varredura (Rescan);

11.12.8.2. Remoção de arquivos da quarentena;

11.12.8.3. Exclusão permanente de arquivos em quarentena.

11.12.9. A solução deverá possibilitar a configuração de ambiente de detecção avançada de intrusão (AIDE), capaz de identificar e corrigir automaticamente desvios na configuração de segurança do servidor de arquivos, sem necessidade de intervenção manual.

11.12.10. Deverá ser possível configurar políticas de senha forte (strong password) para o acesso à linha de comando (CLI) do servidor de arquivos.

11.12.11. O sistema deverá suportar configuração de qualidade de serviço (QoS), utilizando valores DSCP para diferenciação de códigos de serviço em rede.

11.12.12. Deverá suportar o protocolo NFS v4.2, otimizando as operações de entrada/saída (I/O) e reduzindo o consumo de rede.

11.12.13. A solução deverá contemplar as seguintes funcionalidades para compartilhamento de arquivos via protocolo SMB:

11.12.14. Autenticação integrada ao Active Directory.

11.12.15. Enumeração baseada em acesso (ABE), exibindo apenas pastas e arquivos aos quais o usuário possui permissão.

11.12.16. Assinatura digital de pacotes SMB (SMB Signing), garantindo autenticidade e integridade das transmissões.

11.12.17. Criptografia em nível de pasta (SMB Encryption), assegurando a confidencialidade dos dados.

11.12.18. Organização de compartilhamentos em um único espaço de nomes (Single Namespace), suportando ambientes locais ou geograficamente distribuídos, por meio do protocolo DFS-N (DFS Namespaces).

11.12.19. Suporte à autenticação via Active Directory e LDAP, além de acesso não gerenciado a compartilhamentos NFSv4 (autenticação LDAP) e NFSv3.

11.12.20. Suporte a acesso multiprotocolo (SMB e NFS) sobre o mesmo compartilhamento, preservando permissões via Windows ACLs e Unix mode bits.

11.12.21. Suporte a Home Shares por diretório, permitindo o provisionamento automático de pastas pessoais de usuário.

11.12.22. Suporte à aplicação de cotas de uso do sistema de arquivos, com notificações (soft limit) e bloqueio (hard limit), configuráveis por usuário, grupo ou diretório no momento da criação (Directory Level Quotas).

11.12.23. O módulo de armazenamento de objetos deverá possuir API REST compatível com AWS S3, apta a lidar com petabytes de dados não estruturados, atendendo casos de uso como backup, retenção de longo prazo e aplicações nativas de nuvem.

11.12.24. Deverá permitir que os usuários armazenem e gerenciem dados não estruturados em arquitetura de nuvem privada escalável.

11.12.25. A solução deverá permitir a gestão de objetos via interface gráfica de administração e via API REST compatível com S3, mediante autorização prévia do administrador.

11.12.26. Suportar integração com serviços de diretório (Microsoft Active Directory e OpenLDAP), possibilitando o controle de acesso a objetos.

11.12.27. Permitir o compartilhamento de buckets com usuários portadores de chaves de acesso, com delegação de permissões de leitura e escrita conforme o nível definido.

11.12.28. Exibir a listagem de buckets compartilhados, indicando os respectivos usuários com acesso.

11.12.29. Permitir o gerenciamento de buckets e objetos por meio de APIs REST compatíveis com a solução de gerenciamento central ou S3, mediante autorização administrativa.

11.12.30. Suportar o versionamento de múltiplas versões de um mesmo objeto dentro de um bucket.

11.12.31. Possibilitar a definição de regras de ciclo de vida, como exclusão automática de objetos ou versões após período determinado (dias, meses ou anos).

11.12.32. Implementar mecanismo de proteção contra exclusão ou alteração de objetos, com base em políticas de retenção WORM (Write-Once-Read-Many).

11.12.33. Disponibilizar painel de monitoramento de desempenho, apresentando requisições por segundo, taxa de banda (MB/s) e tempo médio de leitura (GET).

11.12.34. Suportar políticas de cotas de utilização, notificando usuários conforme o consumo de espaço ou número de buckets criados.

11.12.35. Suportar o envio de notificações em tempo real — como criação, deleção, leitura, gravação ou alteração de permissões — para fins de auditoria e retenção, compatível com servidores syslog ou sistemas equivalentes.

11.13 ITEM 06 - SOFTWARE DE BACKUP DE DADOS

11.13.1 Características Gerais do Licenciamento:

11.13.1.1 Aquisição de 200 (duzentas) licenças pelo período de 05 (cinco) anos ou 60 (sessenta) meses.

11.13.1.2 Não deverão existir limites quanto ao uso de agentes, conectores, repositórios de armazenamento, hosts físicos e outras tecnologias agregadas a arquitetura da solução especificada.

11.13.1.3 Ser a última versão disponível, não será aceita a utilização de versões anteriores para cobrir algum item desse descritivo técnico.

11.13.1.4 Mostrar na console de gerenciamento a quantidade de licenças adquiridas e utilizadas.

11.13.1.5 Caso a solução ofertada necessite de algum banco de dados, o mesmo deverá ser fornecido devidamente licenciado sem nenhum custo extra.

11.13.1.6 A solução deve ser compatível com o Item 07 Equipamento de Armazenamento de Dados de Backup on-premises.

11.13.2 Cópia e Restauração de Dados:

11.13.2.1 Permitir o controle da banda utilizada durante a operação de cópia de proteção dos backups.

11.13.2.2 Ser capaz de realizar cópia de arquivos abertos sem que a consistência deles seja comprometida.

11.13.2.3 Possuir a opção de priorização de tarefas de proteção com opção de resumo da cópia caso uma atividade de menor prioridade seja colocada em estado de espera por uma tarefa de maior prioridade.

11.13.2.4 Possuir a funcionalidade de paralelizar a gravação dos dados em dispositivos de armazenamento (funcionalidade conhecida como multiplexação).

11.13.2.5 Ser capaz de enviar alertas através de e-mail com o objetivo de reportar eventos ocorridos na operação e configuração da solução.

11.13.2.6 Ser capaz de enviar traps SNMP (Simple Network Management Protocol) com o objetivo de reportar eventos ocorridos na operação da solução.

11.13.2.7 Possuir a funcionalidade de agendamento automático de tarefas de cópia.

11.13.2.8 Para um mesmo dado armazenado deve haver a possibilidade de configuração de diferentes períodos de retenção.

11.13.3 Gerenciamento das Operações de Proteção e Restauração:

11.13.3.1 Possuir interface única, que seja capaz de gerenciar e executar operações de proteção e recuperação dos sistemas operacionais Windows, Unix e Linux; ambiente de virtualização Acropolis Operating System; aplicações, Microsoft Active Directory e banco de dados Microsoft SQL Server, PostgreSQL e Oracle.

11.13.3.2 O acesso administrativo ao console do servidor de gerenciamento da solução poderá ser feito através de ferramenta disponibilizada no próprio software (console gráfico) ou através de navegador Web.

11.13.3.3 Implementar distribuição automática de carga entre os movimentadores de dados, ou seja, os dados oriundos dos clientes de backup deverão ser distribuídos de forma automática entre os servidores de cópia, e em caso de falha de um dos servidores, o cliente automaticamente irá encaminhar seus dados para o outro servidor de cópia ativo. Esta funcionalidade deverá ser nativa do produto, e não pode ser construída com o uso de soluções baseadas em softwares de cluster de terceiros.

11.13.3.4 A base de dados para armazenamento do catálogo deverá possuir mecanismo de proteção (backup) das informações armazenadas no catálogo e funcionalidades de recuperação rápida do catálogo em caso de desastre.

11.13.4 Criptografia dos Dados Protegidos

11.13.4.1 Implementar criptografia de dados na origem (cliente de backup), de uma forma que seja garantido que o dado que trafegará na rede de modo criptografado.

11.13.4.2 Deverá implementar no mínimo chaves de criptografia de 128 bits ou 256 bits.

11.13.5 Desduplicação dos Dados Protegidos

11.13.5.1 Permitir uso da tecnologia de desduplicação de dados para toda a capacidade licenciada, eliminando blocos repetidos, para cópias e arquivamento em disco e movimentação de dados desduplicados, independentemente do quantitativo de dispositivos de armazenamento que compõem a infraestrutura da CONTRATANTE.

11.13.5.2 Implementar desduplicação de blocos na origem (client-side desduplication), de forma que o cliente envie apenas novos blocos de dados criados e/ou modificados a partir da última cópia total completa;

11.13.5.3 Implementar desduplicação de dados nos servidores de armazenamento (target desduplication), de forma que tais servidores tratem adequadamente blocos repetidos enviados pelos clientes, evitando assim o armazenamento de blocos redundantes;

11.13.5.4 Implementar desduplicação de dados em tarefas de cópia;

11.13.5.5 Implementar desduplicação e compressão em uma mesma tarefa;

11.13.5.6 Permitir a restauração granular de arquivos ou sistemas de arquivos a partir de cópias em disco ou fita. Em caso de backup armazenado em disco a recuperação granular poderá ser feito utilizando-se cópias que possam estar desduplicados;

11.13.6 Alertas e Relatórios da Proteção de Dados

11.13.6.1 Quantidade de rotinas de backup concluídos nas últimas 24 horas, nos últimos 30 dias e nos últimos 12 meses.

11.13.6.2 Quantidade de recuperações efetuadas nas últimas 24 horas, nos últimos 30 dias e nos últimos 12 meses.

11.13.6.3 Resumo de rotinas de backup concluídos com sucesso, com erro ou não concluídos.

11.13.6.4 Mostrar o total de licenças adquiridas e o total de licenças utilizadas e caso ocorra uma nova aquisição de licenças as novas licenças deverão constar nesse relatório.

11.13.6.5 Enviar os seguintes alertas via e-mail: rotina de backup finalizada com sucesso, rotina de backup finalizada com erro e rotina de backup com problema.

11.13.7 Fornecimento de licenciamento do Sistema Operacional

11.13.7.1 Fornecimento de licenciamento do sistema operacional Microsoft Windows Server Datacenter, baseado em núcleo (core-based licensing , para 48 cores físicos).

11.13.7.2 As licenças deverão ser entregues em formato eletrônico, acompanhadas de instruções para instalação e ativação, devendo incluir garantia mínima de 60 (sessenta) meses ou suporte técnico equivalente.

11.13.7.3 O licenciamento deverá ser compatível com servidores físicos e virtuais , observando o licenciamento mínimo exigido pela fabricante.

11.13.7.4 As licenças fornecidas deverão ser originais, legítimas e adquiridas por meio de canal autorizado da Microsoft, com comprovação documental no momento da entrega.

11.13.7.5 As licenças deverão ser entregues em formato eletrônico, acompanhadas de instruções para instalação e ativação, incluindo garantia mínima de 60 (sessenta) meses ou suporte técnico equivalente.

11.13.7.6 O item deverá ser plenamente compatível com a infraestrutura tecnológica do MPAM, em especial com ambientes físicos e virtuais já existentes.

11.13.7.7 Incluir Software Assurance (SA), garantindo direito a atualizações, suporte técnico estendido e benefícios de mobilidade de licenças durante todo o período contratual;

11.14 ITEM 07 - EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES

11.14.1 Características gerais:

11.14.1.1 Deverá corresponder a um sistema inteligente dedicado ao armazenamento de backups em disco, com funcionalidades integradas de criptografia, compressão, desduplicação e replicação dos dados já desduplicados;

11.14.1.2 O equipamento deve estar listado no site oficial do fabricante como um appliance ou sistema de armazenamento de backup em disco, em produção ativa;

11.14.1.3 O hardware e o software devem ser do mesmo fabricante. Não serão aceitas soluções customizadas especificamente para esta licitação, nem combinações OEM, equipamentos usados, recondicionados, de demonstração ou gateways;

11.14.1.4 O equipamento deve ser novo, sem uso anterior, pertencente à linha mais recente do fabricante, em produção contínua e sem previsão de fim de suporte (EOSL) nos próximos cinco anos a partir da data de abertura da licitação;

11.14.1.5 Soluções baseadas exclusivamente em software (appliances virtuais) não serão aceitas;

11.14.1.6 Deve ser compatível com montagem em racks padrão de 19”, acompanhado de trilhos, cabos, conectores, manuais e todos os itens necessários para instalação, configuração e operação completa;

11.14.1.7 Para soluções com arquitetura Scale-Out:

11.14.1.7.1 Deve permitir conexão com outros sistemas do mesmo fabricante para expansão de desempenho e capacidade;

11.14.1.7.2 Deve operar em modo ativo-ativo (alta disponibilidade com balanceamento de carga), redirecionando automaticamente os backups em caso de falha de um dos sistemas;

11.14.1.8 Para soluções com arquitetura Scale-Up:

11.14.1.8.1 Deve incluir duas controladoras, operando em modo ativo-ativo ou ativo-passivo, garantindo continuidade das operações de backup em caso de falha de uma das controladoras.

11.14.2 Requisitos de disponibilidade:

11.14.2.1 Deve possuir tolerância a falhas em componentes como discos, fontes de alimentação e ventiladores;

11.14.2.2 Deve contar com mecanismos que assegurem a integridade dos dados mesmo em casos de interrupção abrupta ou desligamento acidental;

11.14.2.3 Deve incluir proteção de cache de escrita para evitar perda de dados em caso de falha de energia;

11.14.2.4 Deve ser entregue com arranjos RAID-6, RAID-DP ou equivalente, com tolerância a falha de até dois discos e pelo menos um disco hot-spare por grupo RAID;

11.14.2.5 Os discos devem ser hot-pluggable e hot-swappable, permitindo substituição sem interrupção do sistema;

11.14.2.6 Deve oferecer monitoramento remoto pelo fabricante, com recursos como Call-Home para detecção proativa de falhas ou pré-falhas.

11.14.3 - Capacidade, desempenho e conectividade:

11.14.3.1 Deve oferecer no mínimo 100 TB (cem terabytes) úteis, sem considerar compressão, desduplicação ou espaço reservado ao sistema;

11.14.4 Para soluções Scale-Out:

11.14.4.1 Deve atingir taxa mínima de 5 TB/hora (cinco terabytes por hora) para operações de backups, sem considerar desduplicação;

11.14.4.2 Capacidade de ampliar a solução previamente fornecida, através da interconexão de módulos similares ou não, do mesmo fabricante. Para a expansão, volumes em nuvem, off-site, replicação ou similar para o atendimento a este requisito não serão aceitos, mantendo a característica de desduplicação global da solução.

11.14.4.3 A criptografia deve ser feita via hardware. Caso seja por software, a taxa de transferência deve ser 30% superior à mínima exigida, considerando apenas a desduplicação.

11.14.5 Para soluções Scale-Up:

11.14.5.1 Deve permitir expansão para pelo menos 500 TB (quinhentos terabytes) de capacidade útil, sem considerar compressão ou desduplicação, por meio de gavetas de discos, sem troca ou upgrade das controladoras originais, mantendo a desduplicação global;

11.14.5.2 Deve atingir taxa mínima de 15 TB/hora (quinze terabytes por hora) para operações de backup, considerando apenas a desduplicação;

11.14.5.3 A criptografia deve ser realizada por hardware. Se for por software, a taxa de transferência deve ser 30% superior à exigida, considerando apenas a desduplicação;

11.14.5.4 Deve incluir no mínimo duas interfaces de rede de 25 Gbps com conectores SFP28 para backup via LAN, fornecidos com o equipamento;

11.14.5.5 Deve incluir pelo menos duas interfaces de 1 GbE com conectores UTP CAT6 para gerenciamento, também fornecidos;

11.14.5.6 Deve possuir ao menos uma porta IPMI/iLO/iDRAC ou equivalente;

11.14.5.7 Interfaces adicionais devem ser fornecidas conforme as melhores práticas do fabricante para garantir o desempenho requerido;

11.14.5.8 Fornecer a quantidade necessária de discos para atingimento da performance mínima solicitada, ou seja, se a solução requerer mais discos além dos necessários para atender a capacidade solicitada no item 8.3.1, discos adicionais deverão ser fornecidos. Não é obrigatório o licenciamento de capacidade desses discos adicionais

11.14.5.9 Comprovar a taxa de transferência através da ferramenta de dimensionamento do fabricante da solução, desconsiderando o uso de ferramentas/protocolos de otimizações na origem no seu dimensionamento, caso a solução ofertada não seja fornecida com todos os discos possíveis para sua capacidade total.

11.15 ITEM 08 - SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES

11.15.1 Características gerais

11.15.1.1 Permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, de maneira perpétua, irrestrita e sem necessidade de licenciamentos ou ônus adicionais;

11.15.1.2 -Possuir licenças na modalidade de uso perpétuo para todo para o completo atendimento das especificações técnicas do equipamento, ou seja, o equipamento deverá continuar a operar normalmente mesmo após o período de manutenção e assistência técnica contratado;

11.15.1.3 Para soluções com arquitetura Scale-Out:

11.15.1.3.1 A desduplicação de dados deve ser mantida de forma global em todo o ambiente de armazenamento, independentemente da quantidade de dispositivos interligados;

11.15.1.4 Para soluções com arquitetura Scale-Up:

11.15.1.4.1 A desduplicação global deve ser preservada em todo o conjunto de armazenamento.

11.15.2 Requisitos de compatibilidade:

11.15.2.1 O software deve ser homologado e plenamente compatível com o com o software de backup fornecido no ITEM 06 - SOFTWARE DE BACKUP DE DADOS;

11.15.2.2 Deve permitir leitura e gravação simultâneas via protocolos CIFS, NFS e OST;

11.15.2.3 Deve oferecer suporte aos protocolos de monitoramento SNMP e Syslog;

11.15.2.4 Deve possibilitar que aplicações como Oracle (via RMAN) e Microsoft SQL realizem backups tipo Stream Based (Oracle Stream Backup) e “database dump” diretamente no equipamento, por meio de CIFS e NFS, sem uso de software de backup, evitando o consumo de licenças e sem necessidade de licenciamento por volume (TB) ou por servidor (CPU, Core, Tier). Caso essa funcionalidade exija licenciamento, todos os itens necessários devem ser incluídos na proposta.

11.15.3 - Funcionalidades operacionais:

11.15.3.1 Deve permitir a execução simultânea de processos de backup e restore;

11.15.3.2 Deve dispor de interface de gerenciamento baseada em navegador (WEB);

11.15.3.3 A desduplicação deve ser global, mesmo com volumes lógicos distintos, identificando dados redundantes entre diferentes fontes de backup e armazenando-os apenas uma vez;

11.15.3.4 A desduplicação deve ocorrer em conjunto com os processos de backup e restore, sem necessidade de janelas específicas;

11.15.3.5 Deve incluir mecanismos nativos para verificação da integridade dos dados desduplicados, com capacidade de correção automática em caso de inconsistência, sem uso de scripts externos;

11.15.3.6 Deve permitir replicação de dados via rede IP (LAN/WAN), de forma assíncrona, entre sistemas compatíveis do mesmo fabricante, utilizando desduplicação para otimizar o uso da banda;

11.15.3.7 Deve suportar topologias de replicação como 1:1, 1:N, N:1 e o cascateamento de equipamentos;

11.15.3.8 Deve integrar-se ao Microsoft Active Directory 2012 ou superior, para autenticação e controle de acesso;

11.15.3.9 Os dados armazenados devem ser criptografados com algoritmos de no mínimo AES128-SHA ou AES256-SHA;

11.15.3.10 Deve permitir autenticação em dois fatores (2FA), com integração a soluções OTP como Google Authenticator, Microsoft Authenticator ou equivalentes;

11.15.3.11 Caso a solução exija um sistema OTP específico com licenciamento ou hardware dedicado (ex: Common Access Card /Personal Information Verification cards, sistemas de OTP/tokenização licenciados, etc), todos os componentes necessários devem ser fornecidos para pelo menos 5 usuários;

11.15.3.12 Deve oferecer recurso de autorização dupla (Dual Auth) para alterações em configurações de proteção contra ransomware;

11.15.3.13 Deve incluir funcionalidades avançadas de segurança cibernética para proteção contra ransomware, assegurando a integridade dos dados de backup;

11.15.4 Deve possuir mecanismo de imutabilidade dos dados:

11.15.4.1 A proteção deve estar sempre ativa, independente do software de backup, sem necessidade de janelas específicas ou scripts;

11.15.4.2 A proteção deve ser aplicada imediatamente após a desduplicação dos dados, sem depender de agendamento;

11.15.4.3 Deve adotar o conceito de air-gap, tornando os dados protegidos invisíveis à rede e inacessíveis por softwares de backup, independentemente do protocolo utilizado.

11.16 ITEM 09 – SWITCH CORE

11.16.1 Especificações Físicas

11.16.1.1 O equipamento deve contar com, no mínimo, 48 portas SFP28 compatíveis com velocidades de 1, 10 e 25 Gigabit Ethernet.

11.16.1.2 As interfaces devem ser auto-sensíveis, ajustando automaticamente a velocidade conforme o transceiver conectado, sem necessidade de configuração manual.

11.16.1.3 A altura máxima permitida é de 1 unidade de rack (1 RU).

11.16.1.4 Deve ser compatível com racks padrão de 19 polegadas, incluindo os kits de fixação apropriados.

11.16.1.5 As portas SFP28 devem aceitar transceivers dos tipos SFP+ 10GBase-SR, 10GBase-LR, 10GBase-ER, SFP 1000Base-SX, 1000Base-LX, 1000Base-ZX, 1000Base-T e cabos DAC.

11.16.1.6 Devem ser entregues ao menos 10 cabos DAC 25GbE SFP28 com comprimento mínimo de 3 metros, compatíveis com os appliances do item 1.

11.16.1.7 O switch deve possuir pelo menos 6 portas QSFP28 de 100GbE, com suporte a velocidades de 40GbE.

11.16.1.7.1 Deve ser compatível com transceivers 40GBase-SR4 e 40GBase-LR4.

11.16.1.7.2 Deve aceitar transceivers 100GBase-SR4 e 100GBase-LR4.

11.16.1.7.3 Deve suportar cabos DAC.

11.16.1.8 Deve acompanhar pelo menos 1 cabo DAC 100GbE com no mínimo 1 metro de comprimento, para conexão redundante entre switches.

11.16.1.9 A capacidade da matriz de comutação deve ser de no mínimo 4 Tbps.

11.16.1.10 O throughput mínimo exigido é de 1,5 Bpps.

11.16.1.11 O buffer deve ter capacidade mínima de 32 MB.

11.16.1.12 A latência máxima permitida é de 900 nanosegundos.

11.16.1.13 Deve suportar ao menos 160.000 endereços MAC.

11.16.1.14 A tabela ARP deve comportar até 64.000 entradas ou mais.

11.16.1.15 Deve aceitar jumbo frames com tamanho mínimo de 9000 bytes.

11.16.1.16 É obrigatória a presença de pelo menos uma porta RJ-45 para gerenciamento fora de banda.

11.16.1.17 O equipamento deve vir com CPU e memória (RAM e Flash) suficientes para suportar todas as funcionalidades descritas.

11.16.1.18 Fontes de alimentação internas devem ser redundantes e com ajuste automático para 110/220V.

11.16.1.19 O sistema de ventilação deve ser redundante, com fluxo de ar configurável (frontal-traseiro ou traseiro-frontal), sendo fornecido com ventiladores de fluxo frontal-traseiro.

11.16.1.20 Fontes e ventiladores devem ser hot-swappable e redundantes, permitindo substituição sem interrupção.

11.16.1.21 O equipamento deve ser projetado para ambientes de datacenter, com comutação de pacotes de alto desempenho.

11.16.2 - Funcionalidades Gerais

11.16.2.1 LEDs por porta devem indicar status e atividade do link.

11.16.2.2 A arquitetura da solução deve ser baseada em “spine-leaf”, com VxLAN como plano de dados e BGP EVPN como plano de controle.

11.16.2.3 Deve possuir porta de console para configuração via CLI, com conector RJ-45 ou RS-232, incluindo cabos e adaptadores necessários.

11.16.2.4 Gerenciamento via SSHv2 deve ser suportado.

11.16.2.5 O switch deve ter criptografia FIPS 140-2 validada pelo NIST.

11.16.2.6 Deve permitir espelhamento de uma ou mais portas para outra porta específica.

11.16.2.7 Também deve permitir espelhamento para porta remota via tunelamento, mesmo em domínios L2 distintos.

11.16.2.8 Deve implementar Netflow, sFlow ou tecnologia equivalente.

11.16.2.9 Gerenciamento via SNMPv3 deve ser possível.

11.16.2.10 Deve suportar o protocolo Syslog.

11.16.2.11 Deve implementar NTPv4 ou SNTP.

11.16.2.12 Autenticação via RADIUS deve ser suportada.

11.16.2.13 Autenticação via TACACS+ também deve ser suportada.

11.16.2.14 Controle de acesso por porta (IEEE 802.1x) deve estar presente.

11.16.2.15 Deve haver controle de broadcast, multicast e unicast por porta.

11.16.2.16 Deve implementar pelo menos uma fila de saída com prioridade estrita (SP Strict Priority) e divisão de banda ponderada (WRED, WRR ou similar).

11.16.2.17 Deve classificar, marcar e priorizar tráfego com base em IEEE 802.1p CoS.

11.16.2.18 Deve classificar, marcar e priorizar tráfego com base em DSCP (Differentiated Services CodePoint), conforme IETF.

11.16.2.19 Deve permitir classificação de tráfego por IP, portas TCP/UDP e endereços MAC.

11.16.3 - Virtualização de Switch

11.16.3.1 Deve permitir agregação de portas multi-chassi com redundância ativa/ativa sem Spanning Tree, usando MLAG, MC-LAG, M-LAG, VLT (Virtual Link Trunking), Multi-Chassis EtherChannel ou equivalentes.

11.16.3.2 Todos os componentes necessários para alta disponibilidade devem ser fornecidos, incluindo cabos, transceivers e licenças.

11.16.3.3 Em modo virtualizado, os switches devem operar com processamento local, sem tempo de convergência em caso de falha.

11.16.4 - Funcionalidades de Camada 2

11.16.4.1 Suporte a até 4.000 VLANs conforme IEEE 802.1Q.

11.16.4.2 Implementação de VLAN Trunking conforme IEEE 802.1Q, com controle de VLANs permitidas por tronco.

11.16.4.3 Suporte a Link Aggregation (LAG) conforme IEEE 802.3ad.

11.16.4.4 Deve suportar no mínimo 80 grupos LAG com até 16 portas cada.

11.16.4.5 Implementação dos padrões IEEE 802.1d, 802.1s e 802.1w.

11.16.4.6 Deve possuir mecanismo de proteção da root bridge do Spanning Tree.

11.16.4.7 Deve permitir bloqueio de BPDUs em portas em modo fast forwarding, com desativação automática ao recebê-los.

11.16.4.8 Implementação de LLDP e LLDP-MED para descoberta de vizinhos.

11.16.4.9 Suporte a DCB com PFC (IEEE 802.1Qbb), ETS (IEEE 802.1Qaz) e DCBx.

11.16.5 - Funcionalidades de Roteamento

11.16.5.1 Deve realizar roteamento de camada 3 entre VLANs.

11.16.5.2 Suporte ao protocolo OSPFv3.

11.16.5.3 Suporte ao protocolo BGPv4.

11.16.5.4 Capacidade para no mínimo 106.000 rotas IPv4.

11.16.5.5 Capacidade para no mínimo 52.000 rotas IPv6.

11.16.5.6 Operação simultânea com IPv4 e IPv6.

11.16.5.7 Implementação de VRF ou VRF-Light.

11.16.5.8 Suporte a roteamento baseado em políticas (PBR).

11.16.5.9 Implementação do protocolo VRRPv3.

11.17 IMPLANTAÇÃO DA SOLUÇÃO E SERVIÇOS CORRELATOS

11.17.1 A CONTRATADA será responsável por toda a instalação e configuração dos equipamentos, firmwares e softwares, incluindo o fornecimento de quaisquer itens adicionais necessários à sua execução.

11.17.2 A instalação poderá ser realizada integral ou parcialmente pelo fabricante, devendo a CONTRATADA prever esses serviços em sua proposta.

11.17.3 A CONTRATADA deverá disponibilizar técnicos certificados pelo fabricante, habilitados a instalar, operar e configurar os equipamentos fornecidos. Caso a instalação seja conduzida diretamente pelo fabricante, essa exigência estará dispensada.

11.17.4 A CONTRATANTE reserva-se o direito de solicitar a substituição parcial ou total da equipe da CONTRATADA durante a fase de implantação, caso seja constatada a ausência de qualificação técnica adequada.

11.17.5 Deverá ser apresentado cronograma de implantação e proposta de configuração da solução, ambos sujeitos à aprovação da equipe técnica da CONTRATANTE.

11.17.6 Ao final da instalação, deverão ser entregues, em meio digital, os manuais e procedimentos utilizados.

11.17.7 A instalação deverá incluir, no mínimo:

a) Fixação dos equipamentos em rack padrão 19”;

b) Conectorização elétrica e energização dos equipamentos;

c) Atualização de firmwares de todos os componentes (BIOS, Gerência Out of Band, controladoras HBA, interfaces de rede, discos, etc.);

d) Atualizações e releases disponíveis no site oficial;

e) Registro dos equipamentos e licenças no portal do fabricante.

f) Conectorização das interfaces de rede com os respectivos cabos/conectores;

g) Instalação, atualização e configuração dos componentes conforme boas práticas;

h) Integração dos equipamentos à rede do CONTRATANTE;

i) Outras atividades correlatas para garantir a operação da solução no ambiente da CONTRATANTE.

11.17.8 A aceitação dos itens do objeto contratado no ato da sua entrega ao Ministério Público do Estado do Amazonas será considerada como de caráter provisório. A aceitação definitiva dar-se-á após a instalação e configuração dos itens do objeto e a verificação do atendimento às especificações técnicas constantes deste Termo de Referência.

11.17.9 Serão recusados os objetos imprestáveis ou defeituosos, que não atendam as especificações constantes neste termo de referência e/ou que não estejam adequados para uso.

11.17.10 Os itens deverão ser instalados, configurados e ativados pela CONTRATADA em local indicado pelo DTIC do MPAM.

11.17.11 O prazo para conclusão da instalação e configuração dos equipamentos e softwares será de até 30 (trinta) dias, contados a partir da data do recebimento provisório dos mesmos pela DTIC e emissão do termo provisório de recebimento.

11.17.12 Os equipamentos e serviços serão aceitos se, e somente se, houver comprovação de que todos os requisitos técnicos especificados neste Termo de Referência tenham sido atendidos e os itens se encontre em operação plena. Essa comprovação será feita mediante observação direta das características dos equipamentos, consulta à documentação técnica fornecida e verificação dos serviços de instalação e configurações.

11.17.13 Os serviços de instalação, configuração, migração e transferência de conhecimento técnico deverão ser realizados conforme especificado em cada item.

11.17.14 O serviço de instalação e configuração tem a finalidade de garantir que os itens fornecidos estejam operacionais no ambiente de Produção, e de Contingência caso exista.

11.17.15 Todos os serviços de instalação, configuração, migração e transferência de conhecimento técnico deverão ser executados de forma presencial, por especialista(s) técnico(s) certificado(s) nos componentes pelo fabricante dos mesmos com a devida apresentação de certificado(s) técnico(s) emitido(s) pelo fabricante do(s) produto(s).

11.17.16 Os serviços de instalação, configuração, migração e transferência de conhecimento técnico, deverão ser agendados previamente entre as partes, através de e-mail ou telefone, e deverão ser realizados em dias úteis e em horário de expediente do MPAM.

11.17.17 A transferência de conhecimento técnico será feita através de treinamento referente aos componentes do objeto deste Termo de Referência, abrangendo todos os recursos de hardware e software do ambiente, para até 10 (dez) técnicos designados pela CONTRATANTE, cobrindo no mínimo os seguintes tópicos:

a) Instalação.

b) Configuração básica e avançada.

c) Operação básica e avançada.

d) Gerenciamento da solução/expansão.

e) Administração.

f) Solução de problemas (troubleshouting).

g) Laboratório prático baseado na solução/expansão adquirida.

11.17.18 O treinamento deverá ser realizado nas seguintes condições:

a) Deverá ser ministrado em língua portuguesa do Brasil, de forma presencial;

b) Local: Av. Coronel Teixeira, nº 7.995, Nova Esperança II, CEP. 69037-473, Manaus-AM;

c) Carga horária mínima de 30 (trinta) horas, divididas em, no máximo, 4 (quatro) horas diárias;

d) O conteúdo programático deverá ser aprovado pela DTIC antes da realização de cada treinamento.

11.17.19 O material didático e os certificados deverão ser disponibilizados pela CONTRATADA com finalidade específica para ministrar o treinamento à DTIC.

11.17.20 Ao final do treinamento, os participantes deverão estar aptos a operar e administrar as tecnologias referenciadas neste Termo de Referência.

11.17.21 A transferência de conhecimento técnico deverá ocorrer no período correspondente ao recebimento definitivo da expansão, ou em caso de impedimento justificado, em nova data aceita pela fiscalização do contrato.

11.17.22 Caberá ainda a CONTRATADA a execução de todas as atividades, bem como o fornecimento de todos os materiais necessários e suficientes para a instalação e configuração dos equipamentos fornecidos.

11.17.24 O planejamento, instalação, configuração e migração dos equipamentos deverão ser executados por técnicos habilitados e credenciados pelo fabricante.

11.17.25 A CONTRATADA deverá designar um profissional Técnico Responsável para acompanhar a execução dos serviços desde o planejamento até a implantação da expansão.

11.17.26 Antes da implantação dos equipamentos, a equipe técnica da CONTRATADA deverá apresentar o cronograma da implantação contendo: o plano de instalação, plano de contingência e prazos máximos para a realização da mudança.

11.17.27 A CONTRATADA deverá realizar a migração completa do ambiente computacional atualmente em operação para a nova infraestrutura fornecida, incluindo, mas não se limitando a: máquinas virtuais, clusters Kubernetes, bancos de dados, configurações nativas, políticas de segurança, integrações existentes e demais componentes necessários para garantir a continuidade dos serviços. A migração deverá ser executada de forma planejada, segura e sem impacto significativo na disponibilidade dos sistemas, observando as melhores práticas recomendadas pelo fabricante e garantindo a integridade dos dados e das aplicações.

11.17.28 A CONTRATADA deverá prover PDU´s ou réguas smart adequadas para a devida conecção elétrica necessária dos equipamentos específicados neste Termo de Referência.

11.17.29 Após a conclusão das atividades de instalação, configuração, migração e pré-operação, deve ser iniciada a fase de operação assistida do objeto contratado.

11.17.30 A operação assistida terá duração total de 90 (noventa) dias corridos, sendo 15 (dias) dias corridos de forma presencial, e o restante do período podendo ser de forma remota, de modo a assegurar o auxílio e pronta ação corretiva da CONTRATADA necessária em questões relacionadas com a configuração, monitoramento e estabilização da nova solução com o objetivo de garantir o bom funcionamento dos equipamentos e serviços.

11.17.31 Durante a fase de operação assistida, a CONTRATADA deverá atuar de maneira a mitigar os riscos decorrentes da transição tecnológica da plataforma atualmente existente para a nova solução.

11.17.32 As atividades de operação assistida devem ser realizadas somente nas dependências da sede do MPAM em Manaus-AM, em horário de expediente da Procuradoria-Geral, e devem se iniciar logo após a migração tecnológica, testes e ativação dos serviços. Caso seja necessária a consecução de atividades que possam afetar a disponibilidade dos serviços, as atividades de operação assistida podem ser prolongadas após o horário de expediente da Procuradoria-Geral, sem qualquer ônus para o MPAM.

11.17.33 O período de operação assistida deve englobar, dentre outras, as seguintes atividades:

a) Monitoramento de funcionamento e da capacidade dos serviços;

b) Identificação e abertura de chamados técnicos para solução de falhas na solução;

c) Resolução de problemas (troubleshooting);

d) Análise da efetividade de regras e configurações;

e) Simulação de abertura de chamados;

f) Instalação de patches;

g) Execução/revisão de procedimentos de backup e restore de configurações;

h) Geração de relatórios técnicos, administrativos e gerenciais;

12. GARANTIA TÉCNICA

12.1 Todos os equipamentos e softwares utilizados na fornecimento do objeto deverão estar cobertos por suporte, garantia e assistência técnica do fabricante, durante toda a vigência do contrato.

12.2 A garantia dos hardwares deverá ser na modalidade on-site no Datacenter da CONTRATANTE.

12.3 A CONTRATADA é a única responsável pelos equipamentos e softwares disponibilizados na prestação dos serviços fornecidos ao CONTRATANTE, mesmo que tenham sido adquiridos de terceiros.

12.4 A CONTRATADA responderá pela reparação dos danos causados por defeitos relativos ao serviço prestado, conforme descrição e exigências deste Termo. Por isso, deve prezar pela qualidade e eficiência, garantindo que o serviço e as soluções definitivas fornecidas não causem problemas adicionais àqueles apresentados pelo CONTRATANTE, quando do recebimento de alertas ou da abertura dos chamados de suporte técnico.

12.5 Serviços de Suporte Técnico e Manutenção:

12.5.1 Os equipamentos deverão possuir garantia de 60 (sessenta) meses, com suporte 24x7 e prazo de envio de peças até o próximo dia útil após abertura do chamado.

12.5.2 -O CONTRATANTE poderá acionar diretamente o suporte do fabricante, sem necessidade de autorização prévia da CONTRATADA. Não haverá limitação quanto à quantidade de chamados, seja para dúvidas, configurações ou problemas relacionados a hardware e software.

12.5.3 - Chamados poderão ser abertos via telefone 0800, portal web ou e-mail.

12.5.4 - O atendimento telefônico inicial deverá ser realizado em português.

12.5.5 - A contratada deverá garantir acesso completo ao portal do fabricante, incluindo base de conhecimento, atualizações de software e documentação.

12.5.7 - Durante a vigência do suporte, todas as atualizações de firmware e software deverão ser fornecidas sem ônus à CONTRATANTE.

12.5.8 - A contratada deverá apresentar os códigos de serviço (SKU, part number) referentes à garantia do fabricante, com os equipamentos devidamente registrados em nome da contratante.

12.5.9 - É de responsabilidade da contratada garantir a compatibilidade técnica entre todos os componentes da solução durante toda a vigência contratual.

13. DA ELABORAÇÃO

O presente Termo de Referência foi elaborado pela **DIRETORIA DE TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO**, em conformidade com as atribuições legais e regimentais, estando em consonância com as disposições legais e normativas aplicáveis, com a necessidade, interesse e conveniência da Administração, sendo parte integrante do procedimento interno respectivo.

14. DECLARAÇÃO DO SOLICITANTE

Declaro que este Termo de Referência está de acordo com a Lei nº 14.133/2021 e alterações.

ANTOVILA FROTA BEZERRA JUNIOR *Técnico em Computação*	**CARLOS ALEXANDRE DOS SANTOS NOGUEIRA** *Chefe do Setor de Infraestrutura e Telecomunicações*

15. APROVAÇÃO

Solicitamos aprovação do presente Termo de Referência tendo em vista que o mesmo foi elaborado de forma conveniente e oportuna para atender à demanda do Ministério Público do Estado do Amazonas.

EUDO LIMA DE ASSIS JUNIOR
Diretor de Tecnologia da Informação e Comunicação

Documento assinado eletronicamente por **Carlos Alexandre dos Santos Nogueira**, **Chefe do Setor de Infraestrutura e Telecomunicação - SIET**, em 14/11/2025, às 17:00, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Antovila Frota Bezerra Junior**, **Requisitado**, em 14/11/2025, às 17:01, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Eudo de Lima Assis Júnior**, **Diretor de Tecnologia da Informação e Comunicação (DTIC)**, em 16/11/2025, às 22:31, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2002143** e o código CRC **699016BF**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MINUTA DE CONTRATO ADMINISTRATIVO Nº 69.2025.DCCON - CONTRATOS.2033432.2025.007562

Processo SEI n.º 2025.007562
Licitação ou Contratação Direta n.º _____
Contrato Administrativo n.º _____

Termo de Contrato Administrativo que entre si celebram o **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS** e a empresa _____, visando ao o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais da **CONTRATANTE**.

O **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**, por intermédio de sua **PROCURADORIA-GERAL DE JUSTIÇA**, órgão de sua Administração Superior, com sede na cidade de Manaus, Estado do Amazonas, na Avenida Coronel Teixeira, 7.995 – Nova Esperança, 69.037-473, inscrito no CNPJ (MF) sob o n.º 04.153.748/0001-85, doravante denominada **CONTRATANTE**, neste ato representada por seu Subprocurador-Geral de Justiça para Assuntos Administrativos, o Exmo. Sr. **André Virgílio Belota Seffair**, residente e domiciliado em Manaus/AM, inscito no CPF sob o n.º ***.287.772-**, e a empresa _____, inscrita no CNPJ (MF) sob o n.º _____, com sede na _____, _____, daqui por diante denominada **CONTRATADA**, neste ato representada por _____, inscrito no CPF (MF) sob o n.º _____, tendo em vista o que consta no **Processo n.º 2025.007562**, doravante denominado **PROCESSO**, e em consequência do _____, firmam o presente **TERMO DE CONTRATO ADMINISTRATIVO N.º _____** , nos moldes da Lei n.º 14.133/2021 e mediante as cláusulas a seguir estabelecidas:

CLÁUSULA PRIMEIRA – DO OBJETO:

O objeto deste ajuste consiste no fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais da **CONTRATANTE**.

CLÁUSULA SEGUNDA – DO DETALHAMENTO DO OBJETO:

O objeto deste instrumento compreende a contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais da **CONTRATANTE**.

1. Por tratar-se de solução integrada, em que o funcionamento efetivo e satisfatório depende de cada um dos seus itens em conjunto, como um todo, ou seja, o simples funcionamento de itens separadamente não tem nenhuma funcionalidade, conforme indicado no Estudo Técnico Preliminar (ETP), a contratação terá lote único, organizado conforme tabela a seguir:

ITEM	DESCRIÇÃO	QUANTIDADE
01	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9	4
02	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU	1
03	SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX	5
04	SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU	1
05	LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE	50
06	SOFTWARE DE BACKUP DE DADOS	1
07	EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	1
08	SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	1
09	SWITCH CORE	2

2. Nas especificações técnicas mínimas apresentadas a seguir, os termos "possui", "permite", "suporta" e "é" implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo "ou" implica que a

especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo "e" implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções citadas.

3. A **CONTRATADA** não poderá oferecer serviço inferior as especificações apresentadas neste Termo, sendo permitido, porém, a oferta de serviço superior as especificações mínimas apresentadas, de acordo com a conveniência da **CONTRATADA** e aprovação da **CONTRATANTE**.

4. Toda documentação gerada durante a prestação dos serviços será de propriedade da **CONTRATANTE**, em virtude de sua elaboração tomar por base informações críticas do funcionamento intrínseco à sua infraestrutura, que afetam diretamente a segurança da **CONTRATANTE**.

5. A **CONTRATADA** deverá guardar inteiro sigilo dos serviços contratados e dos dados processados, bem como de toda e qualquer documentação gerada, reconhecendo serem esses de propriedade e uso exclusivo da **CONTRATANTE**, sendo vedada sua cessão, locação ou venda a terceiros.

6. **CONTRATADA** deverá manter a **CONTRATANTE** atualizada sobre todos os fluxos adotados para a execução das atividades objeto da contratação durante o período contratual, bem como sobre a forma de automatização de quaisquer serviços, documentando todos os procedimentos detalhadamente para que possam servir de base para a continuidade dos serviços independentemente da metodologia que possa ser adotada.

7. ITEM 01 - EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9

7.1 Características Gerais

7.1.1 A infraestrutura deverá ser composta por appliances Nutanix com integração completa entre hardware e software, armazenamento e rede, entregando uma solução hiperconvergente pronta para operação.

7.1.2 Serão aceitos apenas appliances homologados pela Nutanix para uso com o Nutanix AOS (Acropolis Operating System) e Nutanix AHV (Acropolis Hypervisor) ou outro hipervisor suportado pela plataforma.

7.1.3 Caso necessário, será permitida a entrega de equipamentos ou recursos adicionais para atender aos requisitos mínimos, desde que todos os componentes estejam integrados e certificados pela Nutanix.

7.1.4 É permitida a entrega de múltiplos nós em um único chassi, desde que compatível com a arquitetura Nutanix.

7.1.5 A solução deve incluir a ferramenta Nutanix Prism, em sua ultima versão ou equivalente, que oferece gerenciamento centralizado e interface gráfica para monitoramento, atualizações e operação da infraestrutura, incluindo:

7.1.5.1 Atualização de BIOS, firmware, hipervisor e SDS;

7.1.5.2 Visualização do hardware físico;

7.1.5.3 Diagnóstico, inventário e expansão de nós.

7.1.6 Caso alguma funcionalidade não esteja disponível via Prism ou equivalente para monitoramento ou atualização, a CONTRATADA deverá realizar este serviço de forma remota/on-line ou presencial.

7.1.7 Todas as atualizações devem ser homologadas pela Nutanix e aplicadas conforme as melhores práticas da fabricante. Esta ferramenta deve ser gráfica, com suporte a apresentação de visões do hardware físico dos nós, suporte a troca de drives, com controle do inventário, com ferramenta de diagnóstico e com módulo para a adição de novos nós.

7.1.8 A arquitetura deve garantir alta disponibilidade (HA) e resiliência a falhas, com suporte a recuperação de desastres (DR).

7.1.9 Os appliances devem permitir expansão modular e não disruptiva dos serviços de rede e aplicações, com detecção automática de novos nós.

7.1.10 Deve centralizar o armazenamento de dados em discos compartilhados, redundantes.

7.1.11 Cada nó deverá conter armazenamento dedicado para o sistema operacional da plataforma.

7.1.12 A solução deve estar preparada para ambientes de virtualização em alta disponibilidade, conforme as práticas recomendadas pela Nutanix.

7.1.13 Deve suportar software de virtualização para consolidação de servidores e recuperação automática em caso de falhas físicas, minimizando o downtime.

7.1.14 A entrega deve ser feita com todos os componentes física e logicamente integrados, sem ponto único de falha, com acesso imediato ao ambiente via sistema de gestão da plataforma após energização e conexão.

7.1.15 A instalação deve ser compatível com racks padrão de 19 polegadas, incluindo todos os acessórios necessários para montagem no ambiente da CONTRATANTE.

7.1.16 O equipamento deve integrar a linha de produtos Nutanix da família “NX”, assegurando total compatibilidade com atual ambiente e possibilidade de expansão das zonas de disponibilidade já estabelecidas, conforme informações disponibilizadas no endereço eletrônico oficial da fabricante: https://www.nutanix.com/products/hardwareplatforms/specsheet?platformProvider=Nutanix.

7.2 Configuração do Nó ou Chassi

7.2.1 Serão admitidas ofertas de chassis que comportam múltiplos servidores (nós/nodes), para o atendimento da especificação técnica.

7.2.2 Cada nó, ou chassi, deverá possuir ventiladores e fontes redundantes para a operação adequada dos equipamentos.

7.2.3 Todas as fontes de alimentação deverão ser acompanhadas de seus respectivos cabos de energia compatíveis.

7.3 Características de Processamento por Nó

7.3.1 Cada servidor deverá possuir, no mínimo, 02 (dois) processadores com arquitetura x86, voltados ao uso em servidores, contendo as seguintes características mínimas:

7.3.1.1 12 (doze) núcleos físicos e 24 (vinte e quatro) threads por processador;

7.3.1.2 Frequência de clock nominal de, no mínimo, 2,4 GHz;

7.3.1.3 Controladora de memória integrada com suporte à tecnologia DDR5 ou superior.

7.3.2 Será admitida a entrega de processadores de geração superior ao modelo originalmente especificado, desde que mantenham no mínimo a mesma quantidade de núcleos e threads, independentemente de demais especificações.

7.4 Especificações de Memória por Nó

7.4.1 Cada servidor deverá ser fornecido com, no mínimo, 1.536 GB (um mil quinhentos e trinta e seis gigabytes) de memória RAM, distribuída uniformemente entre os processadores, utilizando módulos DDR5 ou superior.

7.5 Especificações de Rede por Nó

7.5.1 Cada servidor deverá ser entregue com as seguintes interfaces de rede:

7.5.1.1 Mínimo de 2 (duas) interfaces de 25/10 GbE SFP28, integradas em uma placa de rede;

7.5.1.2 Mínimo de 1 (uma) interface exclusiva de gerenciamento Ethernet 1000Base-T.

7.5.2 A interface de gerenciamento deverá vir acompanhada de cabos UTP categoria 6 (ou superior), com comprimento mínimo de 5 (cinco) metros e conectores RJ-45.

7.6 Especificações de Armazenamento por Nó

7.6.1 Cada servidor deverá ser entregue com a seguinte configuração mínima de discos:

7.6.1.1 04 (quatro) unidades de SSD NVMe, ou SSD SAS/SATA, com capacidade mínima de 3,84 TB por unidade (volumetria bruta);

7.6.1.2 08 (oito) unidades de disco rígido (HDD), com capacidade mínima de 12 TB por unidade (volumetria bruta).

8. ITEM 02 - EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU

8.1 Características Gerais

8.1.1 A solução deverá ser composta exclusivamente por appliances de nuvem privada, com integração total entre recursos de computação, armazenamento e rede, entregues como infraestrutura unificada.

8.1.2 Serão aceitos apenas appliances homologados para uso com a solução de armazenamento definido por software (Software Defined Storage – SDS) ofertada.

8.1.3 A entrega de equipamentos ou recursos adicionais será aceita, desde que necessária para o atendimento aos requisitos mínimos e que todos os componentes estejam devidamente integrados.

8.1.4 É permitida a entrega de múltiplos nós consolidados em um único chassi modular.

8.1.5 A solução deverá incluir ferramenta unificada de gerenciamento e atualização, com capacidade de monitorar e atualizar BIOS, firmwares, hypervisor e componentes do SDS. Caso não realize todos os procedimentos listados, a CONTRATADA deverá garantir a execução dessas tarefas presencial ou remotamente.

8.1.6 A ferramenta de gestão deverá ser gráfica, com visualização física dos nós, suporte à substituição de drives, inventário automatizado, diagnóstico integrado e capacidade de adicionar novos nós ao cluster.

8.1.7 A arquitetura deverá contemplar alta disponibilidade nativa e recursos para recuperação de desastres (DR), de forma a garantir continuidade dos serviços mesmo em caso de falhas parciais.

8.1.8 Os equipamentos devem possuir arquitetura modular, permitindo expansão de capacidade com inclusão de novos appliances sem interrupção dos serviços.

8.1.9 O armazenamento deverá ser centralizado, com discos compartilhados e redundância nativa.

8.1.10 Cada servidor deverá conter unidade de armazenamento dedicada ao sistema operacional da plataforma e aos softwares de virtualização e processamento gráfico.

8.1.11 A infraestrutura deverá estar preparada para suportar ambientes virtualizados de alta disponibilidade, de acordo com as boas práticas do fabricante da solução.

8.1.12 A solução deverá oferecer suporte a consolidação de servidores e recuperação automática em caso de falhas físicas.

8.1.13 A entrega deverá ocorrer com a solução fisicamente e logicamente pré-integrada, sem ponto único de falha, com acesso imediato à plataforma após energização e conexão física.

8.1.14 A instalação deverá ser compatível com racks padrão de 19", com todos os acessórios de fixação inclusos.

8.1.15 O equipamento deve integrar a linha de produtos Nutanix da família “NX”, assegurando total compatibilidade com atual ambiente e possibilidade de expansão das zonas de disponibilidade já estabelecidas, conforme informações disponibilizadas no endereço eletrônico oficial da fabricante: https://www.nutanix.com/products/hardwareplatforms/specsheet?platformProvider=Nutanix.

8.2 Configuração do Nó ou Chassi

8.2.1 Serão admitidas ofertas de chassis que comportam múltiplos servidores (nós/nodes), para o atendimento da especificação técnica.

8.2.2 Cada nó ou chassi deverá possuir ventiladores e fontes de alimentação redundantes.

8.2.3 Cada fonte deverá ser entregue com seu respectivo cabo de energia.

8.3 Características de Processamento por Nó

8.3.1 Cada servidor deverá possuir, no mínimo, dois processadores com arquitetura x86, dedicados a ambientes de datacenter, com as seguintes características:

8.3.2 12 (doze) núcleos físicos e 24 (vinte e quatro) threads por processador;

8.3.3 Frequência mínima de 2,4 GHz;

8.3.4 Controladora de memória integrada DDR5 ou superior.

8.3.5 A substituição por processadores mais recentes será aceita, desde que observadas as quantidades mínimas de núcleos e threads.

8.4 Especificações de Memória por Nó

8.4.1 - Cada servidor deverá ser entregue com no mínimo 1.024 GB (um mil e vinte e quatro gigabytes) de memória RAM, utilizando módulos DDR5 ou superior, distribuídos de forma equilibrada entre os processadores.

8.5 Especificações de Rede por Nó

8.5.1 Cada servidor deverá conter no mínimo:

8.5.1.1 2 (duas) interfaces de rede 25/10 GbE SFP28;

8.5.1.2 1 (uma) interface de gerenciamento 1000Base-T;

8.5.1.3 A interface de gerenciamento deverá ser acompanhada de cabos UTP Cat-6 ou superior, com 5 metros de comprimento e conectores RJ-45.

8.6 Especificações de Armazenamento por Nó

8.6.1 Cada servidor deverá ser entregue com:

8.6.1.1 2 discos SSD NVMe, SAS ou SATA, com capacidade mínima de 3,84 TB cada (volumetria bruta);

8.6.1.2 4 discos HDD com capacidade mínima de 12 TB cada (volumetria bruta).

8.7 Especificações de Processamento Gráfico e Cálculo Aritmético

8.7.1 Cada servidor deverá conter uma placa gráfica com as seguintes características:

8.7.1.1 48 GB de memória GDDR6 de GPU;

8.7.1.2 Interconexão PCIe Gen4 com largura de banda de 64 GB/s;

8.7.1.3 Suporte a DirectX 12.075, Shader Model 5.175, OpenGL 4.686 e Vulkan 1.186;

8.7.1.4 Compatibilidade com NVIDIA vPC/vApps, NVIDIA RTX Virtual Workstation e NVIDIA Virtual Compute Server;

8.7.1.5 Consumo máximo de 350W.

9. ITEM 03 – SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX

9.1 Camada de Armazenamento da Solução:

9.1.1 A solução deverá contar com camada de armazenamento compartilhada entre todos os servidores e appliances descritos neste Termo, utilizando tecnologia de armazenamento definido por software (Software Defined Storage – SDS).

9.1.2 A arquitetura de armazenamento deverá ser otimizada para ambientes virtuais, com escalabilidade contínua e elástica, permitindo expansão de capacidade pela adição de novos nós/appliances sem necessidade de licenciamento adicional de virtualização.

9.1.3 Não serão aceitas soluções baseadas em tecnologia RAID para redundância de dados.

9.1.4 A solução deverá suportar as tecnologias de compressão e desduplicação de dados inline, near-line ou pós-processada, com o objetivo de otimização do armazenamento.

9.1.5 A solução deverá prover recursos de QoS (Quality of Service), para controle do volume de I/Os de VMs.

9.1.6 Deverá permitir uso de técnicas de Erasure Coding para otimização de aplicações com baixa sensibilidade à latência de escrita.

9.1.7 A solução deverá permitir a expansão do cluster através da adição de nós/servidores que incrementem tão somente a capacidade de armazenamento, sem a necessidade de emprego de licenças de virtualização nesses nós/servidores;

9.1.8 A substituição de discos defeituosos deverá ocorrer sem impacto nas operações de leitura e escrita das aplicações.

9.1.9 A falha de um nó da solução não poderá comprometer a disponibilidade da camada de armazenamento das VMs.

9.1.10 A criptografia deverá ser aplicada em nível de cluster ou volume, via hardware ou software, com KMS nativo. Caso não possua, será aceita entrega de servidor redundante externo com essa funcionalidade.

9.1.11 A distribuição dos dados deverá ocorrer de forma automática e uniforme dentro do cluster.

9.1.12 A solução deverá permitir criação de cópias no tempo (snapshots) sem movimentação dos dados originais e com redirecionamento de escritas subsequentes.

9.1.13 Deverá suportar clonagem de instâncias virtuais a partir de snapshots, sem movimentação dos dados.

9.1.14 Acesso ao armazenamento deverá ser possível via iSCSI por instâncias físicas ou virtuais externas ao cluster, garantindo suporte a aplicações de alta disponibilidade.

9.2 Tecnologia de Replicação e Proteção de Dados:

9.2.1 Deverá ser fornecida funcionalidade de replicação local realizando clones e snapshots com proteção contínua dos dados da máquina virtual.

9.2.2 A solução deve prover as funcionalidades de Thin Provisioning e Serviços de Cópias de dados.

9.2.3 Deverá permitir a configuração de um grupo ou domínio de proteção de instâncias virtuais, que poderão ser protegidas por cópias point-in-time, bem como replicadas para um cluster remoto.

9.2.4 Deverá permitir a união de máquinas virtuais em um único grupo de proteção.

9.2.5 Deverá proteger, por cópias point-in-time, simultaneamente todas as máquinas virtuais pertencentes ao grupo.

9.2.6 Deverá contemplar, também, a proteção nativa de máquinas virtuais consistentes com aplicações, onde há proteção dos dados em memória a partir da movimentação das operações de escrita para disco, de sistemas operacionais Linux e Windows. Caso a plataforma de nuvem privada não permita executar esta funcionalidade nativamente, a CONTRATADA deverá atender este requisito compondo com outra solução.

9.2.7 Deverá permitir a configuração de uma entidade capaz de centralizar todo o fluxo do tráfego replicado entre clusters distintos, convergindo assim os recursos para um único ponto focal. Esse recurso centralizado deverá posteriormente redirecionar o tráfego corretamente para os equipamentos específicos do cluster de contingência.

9.2.8 Deverá permitir ajustar o consumo de banda em replicações.

9.2.9 Deverá permitir a existência de frequências distintas de replicação para instâncias virtuais em grupos diferentes.

9.3 Gerenciamento Integrado:

9.3.1 A solução deve oferecer solução de gerenciamento integrado, licenciado para gerenciar inclusive múltiplos clusters.

9.3.2 Monitoração automática e periódica da solução, com o envio de notificações preventivamente em caso de falhas, notificando o suporte do fornecedor a tomar medidas preventivas e acordadas com a CONTRATANTE a fim de evitar tempo de inatividade e impactos na produção.

9.3.3 Deve oferecer portal de acesso do próprio fornecedor para download de atualizações e de softwares agregados.

9.3.4 A ferramenta de gerenciamento, local, deve fornecer um dashboard reportando a utilização dos recursos do cluster como CPU, Memória, Armazenamento, IOPS do cluster, largura de banda do cluster, latência do cluster e informações sobre o virtualizador empregado e os alertas de saúde.

9.3.5 A solução deve fornecer atualização de todos os componentes (Firmware, e softwares de virtualização que fazem parte da solução) em forma de pacote com instalação assistida.

9.3.6 Contemplar as funcionalidades como:

9.3.6.1 Emissão de relatório avançados do ambiente;

9.3.6.2 Personalização da console principal;

9.3.6.3 Planejamento e previsão de capacidade;

9.3.6.4 Detecção de ineficiência de cargas de trabalho e dimensionamento ideal;

9.3.6.5 Planejamento de capacidade ou cargas de trabalho ao longo do tempo;

9.3.6.6 Permitir automação de operações de gerência do ambiente.

9.4 Provisionamento de Containers:

9.4.1 Deverá ser entregue uma plataforma de provisionamento de containers, integrada, a plataforma de virtualização.

9.4.2 A plataforma deverá permitir a criação de múltiplo clusters.

9.4.3 A fabricante da solução deverá, comprovadamente, pertencer a categoria de membro da CNCF (Cloud Native Computing Foundation).

9.4.4 Seleção de sistemas operacionais, bem como suas distintas versões de microcódigo para implementação automática, sendo compatível com sistemas Linux.

9.4.5 Seleção das configurações de rede do cluster de containers ou microserviços.

9.4.6 Seleção do tipo de armazenamento persistente a ser empregado em containers.

9.4.7 Seleção da quantidade de nós dos tipos “Control Plane” e “Workers” que serão implementados simultaneamente.

9.4.8 A plataforma de containers deverá permitir a criação de alertas, facilitando a gestão do cluster.

9.4.9 Deverá ter suporte a implementação de clusters de plataformas de containers, similares a Kubernetes, NCI, baremetal, public cloud.

9.4.10 A plataforma de containers deverá possuir integração para o acesso através de RBAC, permitindo seu uso completo através de acesso administrativo e permitindo seu uso parcial através de acesso controlado aos demais usuários.

9.4.11 Suporte implementação de clusters de plataformas de containers, similares a Kubernetes com suporte a Bring-Your-Own-OS: Rocky Linux, Ubuntu, RHEL e similares.

9.4.12 Permitir a configuração de clusters com alta-disponibilidade para os “Control Plane” nodes, com ou sem balanceador de carga;

9.4.13 Prover armazenamento persistente através de integração com Container Storage Interface (CSI), para armazenamento de blocos e arquivos. Também deverá ser possível configurar armazenamento de arquivos compatível com protocolo Simple Storage Service;

9.4.14 Deverá fornecer um mecanismo de monitoramento que aciona alertas no cluster Kubernetes;

9.4.15 Oferecer as seguintes funcionalidades em ambiente Kubernetes:

9.4.15.1 Gerenciamento de Dados;

9.4.15.2 Proteção e Restauração de Dados;

9.4.15.3 Aceleração da Entrega de Aplicativos;

9.4.15.4 Gerenciamento de Autoatendimento de Aplicativos;

9.4.15.5 Automação e Monitoramento de Infraestrutura;

9.4.15.6 Padronização de Políticas de Governança e Conformidade;

9.4.16 Para a estratégia de criação de cópias dos dados para ambiente de containers Kubernetes, a solução deverá permitir:

9.4.16.1 Fornecimento de software para “worker nodes” Kubernetes, garantindo o suporte unificado e conjunto da solução como um todo;

9.4.16.2 Plataformas de container baseadas em Kubernetes.

9.4.16.3 Permitira realização de copias e armazenamento em repositório externo.

9.4.16.4 Movimentação das imagens de backup para compartilhamentos NFS por meio de solução de armazenamento compatível com protocolo S3, permitindo que o repositório NFS seja utilizado como backend de Object Storage.

9.4.16.5 Capacidade de restaurar o Namespace para seu local original e para um novo Namespace.

9.5 Segurança de Rede:

9.5.1 Suportar microssegmentação para prover controle granular e governança de todo o tráfego de entrada e saída de uma máquina virtual (VM), grupos de máquinas virtuais (VMs) e containers.

9.5.2 Permitir a associação de políticas de rede a VMs e conteiners em vez de segmentos de rede específicos (por exemplo VLANs) ou identificadores (endereços IP ou MAC).

9.5.3 Prover visualização de tráfego e relacionamentos com a descoberta automática dos fluxos entre as máquinas virtuais e containers.

9.5.4 Permitir políticas de segurança centradas na carga de trabalho em vez de uma abordagem centrada na rede, permitindo examinar o tráfego de, e para as VMs, independentemente de como as configurações de rede mudam e onde residem no data center

9.5.5 Políticas aplicadas por categorias de VMs e containers.

9.5.6 Permitir isolamento de conteiners e VMs comprometidas, colocando-a em quarentena.

9.5.7 - Permitir restrição de tráfego entre camadas de aplicação.

9.5.8 Atualização automática de políticas.

9.5.9 Integração com ferramentas de terceiros como IDS/IPS e load balancer.

9.6 Licenciamento do Software de Virtualização:

9.6.1 Entrega do licenciamento completo da plataforma de virtualização, versão mais avançada.

9.6.2 Suporte à criação de VMs com múltiplas interfaces de rede e múltiplas arquiteturas (32/64 bits).

9.6.3 Permitir provisionamento aos principais sistemas operacionais (Windows Server 2022, CentOS 8, Ubuntu 20, RHEL 9) ou superiores.

9.6.4 Alocação dinâmica de recursos (CPU/RAM).

9.6.5 Hypervisor deverá estar instalado em unidade flash dedicada.

9.6.6 Suporte a GPU virtual ou passthrough nativo.

9.6.7 Suporte a BIOS/UEFI, snapshots, exportação OVA.

9.6.8 Deverá permitir o provisionamento de máquinas virtuais, e grupos de máquinas virtuais, em equipamentos específicos com o propósito de respeitar licenciamentos de aplicações. Em caso de falha do equipamento, a máquina virtual não deverá ser migrada para outro equipamento remanescente;

9.6.9 Alta resiliência a falhas de nós/discos.

9.6.10 Armazenamento distribuído e gerenciado via console web.

9.6.11 Deverá permitir a inicialização, a reinicialização, o reset, o desligamento da VM e o desligamento do sistema operacional dela;

9.6.12 Suportar a tecnologia de snapshot nativos do Hypervisor;

9.6.13 Permitir a adição de novos servidores no cluster;

9.6.14 Permitir criar uma área de armazenamento compartilhada, distribuída e otimizada para ambientes virtuais;

9.6.15 Permitir o agrupamento dos volumes lógicos de todos os servidores no cluster provendo uma área de armazenamento comum para o ambiente virtual;

9.6.16 Possuir mecanismo de redundância e proteção de dados nativo que armazena cópias dos dados em diversos discos e hosts do cluster de forma transparente;

9.6.17 Deverá ser fornecido licenciamento do software de virtualização na versão mais completa para todos os servidores do ambiente de armazenamento distribuído.

9.6.18 Deverá contemplar pelo menos 20 (vinte) núcleos de processamento virtuais (vCPU) ou físicos (pCPU) de solução para gestão de base de dados como serviço (DBaaS).

9.6.19 Deverá ser totalmente compatível com a solução ofertada para atendimento aos requisitos deste termo de referência.

9.6.20 Permitir automatizar as tarefas para provisionamento, emprego de correções de software (patching), gerenciamento do ciclo de vida, clonagem, atualização dos dados em bases clonadas (refresh), proteção contínua e recuperação de bases de dados.

9.6.21 Deverá ser compatível pelo menos com Oracle, Microsoft SQL, PostgreSQL, MariaDB, MongoDB e MySQL.

9.6.22 Permitir o uso de uma chave SSH pública para acesso ao servidor de banco de dados com opção através do upload de um arquivo e através da inserção direta da chave em campo de texto.

9.6.23 A solução deverá permitir registrar bancos de dados existentes para emprego de proteção contínua capturando e mantendo snapshots e registros (logs) transacionais da base de dados de origem conforme definições contidas no agendamento.

9.6.24 A mesma tecnologia deverá permitir a clonagem de bases de dados.

9.6.25 Durante a clonagem, a solução deverá permitir a escolha para o administrador utilizar um servidor de banco de dados registrado ou criar um novo servidor.

9.6.26 Permitir que o administrador realize o clone de uma base de dados a partir de um snapshot.

9.6.27 Permitir que o administrador realize o clone de uma base de dados dentro de uma política de proteção contínua, ou seja, clonar uma base de dados em determinado dia, hora, minuto e segundo.

9.6.28 Permitir a definição de agendamento da periodicidade para realizar a atualização (refresh) dos dados da base clonada através do estado atual na base de dados de origem.

9.6.29 Permitir a definição de uma data para remoção ou exclusão do clone.

9.6.30 Permitir a execução de scripts ou comandos de pré e pós clonagem.

9.6.31 Deverá ser possível definir as políticas de retenção dos snapshots diários, semanais, mensais e trimestrais.

10. ITEM 04 – SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU

10.1 Software para Processamento Gráfico e Cálculo Aritmético:

10.1.1 Permitir a seleção, implantação e gestão de modelos de IA Generativa (LLMs) provenientes da Hugging Face e NVIDIA, bem como a importação de modelos personalizados ou treinados pelo contratante em clusters Kubernetes.

10.1.10 Permitir a criação de um endpoint de inferência e o compartilhamento dele com desenvolvedores para incorporar em seus aplicativos de IA. Permitir gerenciar e validar esses endpoints para garantir que eles estejam configurados corretamente.

10.1.11 Permitir o acesso a um endpoint de inferência por um aplicativo usando chaves de API. O gerenciamento de chaves de API deverá permitir o fornecimento e revogação do acesso à API para garantir controles de segurança de acesso adequados.

10.1.12 Permitir o controle de acesso baseado em função (RBAC), para fornecer permissões de acesso personalizadas aos usuários com base em suas funções atribuídas.

10.1.13 Possuir uma interface de usuário simples e dinâmica que simplifique o processo de implantação.

10.1.14 Possuir um painel dinâmico que permita monitorar a integridade da implantação com ferramentas de monitoramento em tempo real que identifiquem gargalos, rastreiem o desempenho e solucionem problemas.

10.1.15 Suportar a instalação e o funcionamento em estruturas sem qualquer conexão com a Internet (dark-site ou air-gapped).

11. ITEM 05 - LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE

11.1 A solução deverá incluir unidade de subscrição de software para armazenamento de objetos e arquivos, licenciada por terabyte (TB), com suporte técnico durante 60 (sessenta) meses, contemplando ambiente de produção em operação contínua (24x7).

11.2 Caso a solução proposta não ofereça suporte nativo a armazenamento de objetos e arquivos, será permitida a utilização de unidade externa dedicada, desde que esta disponha de todos os componentes, funcionalidades e suporte equivalentes à solução principal.

11.3 O sistema de armazenamento definido (SDS) deverá otimizar dados utilizando tecnologia de erasure coding na camada de capacidade, de modo a garantir eficiência e resiliência no armazenamento de arquivos e objetos.

11.4 A solução deverá permitir a recuperação granular de arquivos pelos usuários, sem necessidade de intervenção do administrador.

11.4.1 Para o protocolo SMB, a restauração deverá ocorrer por meio da funcionalidade “Versões Prévias” da pasta de destino.

11.4.2 Para o protocolo NFS, a recuperação deverá ser possível pela listagem do subdiretório oculto (snapshot).

11.5 O sistema deverá integrar-se a softwares antivírus de terceiros por meio do protocolo ICAP (Internet Content Adaptation Protocol), possibilitando varredura em tempo real de arquivos compartilhados via SMB sempre que forem abertos, modificados ou encerrados.

11.6 A interface de gerenciamento deverá exibir o estado dos arquivos após a varredura antivírus, incluindo status como limpo, em quarentena ou deletado, além do histórico de eventos correspondentes.

11.7 A interface de gerenciamento deverá também exibir relatórios detalhados contendo a lista de arquivos analisados, ameaças detectadas e arquivos colocados em quarentena.

11.8 A interface de gerenciamento deverá permitir ações diretas sobre os arquivos, incluindo:

11.8.1 Reexecução de varredura (Rescan);

11.8.2 Remoção de arquivos da quarentena;

11.8.3 Exclusão permanente de arquivos em quarentena.

11.9 A solução deverá possibilitar a configuração de ambiente de detecção avançada de intrusão (AIDE), capaz de identificar e corrigir automaticamente desvios na configuração de segurança do servidor de arquivos, sem necessidade de intervenção manual.

11.10 Deverá ser possível configurar políticas de senha forte (strong password) para o acesso à linha de comando (CLI) do servidor de arquivos.

11.11 O sistema deverá suportar configuração de qualidade de serviço (QoS), utilizando valores DSCP para diferenciação de códigos de serviço em rede.

11.12 Deverá suportar o protocolo NFS v4.2, otimizando as operações de entrada/saída (I/O) e reduzindo o consumo de rede.

11.13 A solução deverá contemplar as seguintes funcionalidades para compartilhamento de arquivos via protocolo SMB:

11.14 Autenticação integrada ao Active Directory.

11.15 Enumeração baseada em acesso (ABE), exibindo apenas pastas e arquivos aos quais o usuário possui permissão.

11.16 Assinatura digital de pacotes SMB (SMB Signing), garantindo autenticidade e integridade das transmissões.

11.17 Criptografia em nível de pasta (SMB Encryption), assegurando a confidencialidade dos dados.

11.18 Organização de compartilhamentos em um único espaço de nomes (Single Namespace), suportando ambientes locais ou geograficamente distribuídos, por meio do protocolo DFS-N (DFS Namespaces).

11.19 Suporte à autenticação via Active Directory e LDAP, além de acesso não gerenciado a compartilhamentos NFSv4 (autenticação LDAP) e NFSv3.

11.20 Suporte a acesso multiprotocolo (SMB e NFS) sobre o mesmo compartilhamento, preservando permissões via Windows ACLs e Unix mode bits.

11.21 Suporte a Home Shares por diretório, permitindo o provisionamento automático de pastas pessoais de usuário.

11.22 Suporte à aplicação de cotas de uso do sistema de arquivos, com notificações (soft limit) e bloqueio (hard limit), configuráveis por usuário, grupo ou diretório no momento da criação (Directory Level Quotas).

11.23 O módulo de armazenamento de objetos deverá possuir API REST compatível com AWS S3, apta a lidar com petabytes de dados não estruturados, atendendo casos de uso como backup, retenção de longo prazo e aplicações nativas de nuvem.

11.24 Deverá permitir que os usuários armazenem e gerenciem dados não estruturados em arquitetura de nuvem privada escalável.

11.25 A solução deverá permitir a gestão de objetos via interface gráfica de administração e via API REST compatível com S3, mediante autorização prévia do administrador.

11.26 Suportar integração com serviços de diretório (Microsoft Active Directory e OpenLDAP), possibilitando o controle de acesso a objetos.

11.27 Permitir o compartilhamento de buckets com usuários portadores de chaves de acesso, com delegação de permissões de leitura e escrita conforme o nível definido.

11.28 Exibir a listagem de buckets compartilhados, indicando os respectivos usuários com acesso.

11.29 Permitir o gerenciamento de buckets e objetos por meio de APIs REST compatíveis com a solução de gerenciamento central ou S3, mediante autorização administrativa.

11.30 Suportar o versionamento de múltiplas versões de um mesmo objeto dentro de um bucket.

11.31 Possibilitar a definição de regras de ciclo de vida, como exclusão automática de objetos ou versões após período determinado (dias, meses ou anos).

11.32 Implementar mecanismo de proteção contra exclusão ou alteração de objetos, com base em políticas de retenção WORM (Write-Once-Read-Many).

11.33 Disponibilizar painel de monitoramento de desempenho, apresentando requisições por segundo, taxa de banda (MB/s) e tempo médio de leitura (GET).

11.34 Suportar políticas de cotas de utilização, notificando usuários conforme o consumo de espaço ou número de buckets criados.

11.35 Suportar o envio de notificações em tempo real — como criação, deleção, leitura, gravação ou alteração de permissões — para fins de auditoria e retenção, compatível com servidores syslog ou sistemas equivalentes.

12. ITEM 06 - SOFTWARE DE BACKUP DE DADOS

12.1 Características Gerais do Licenciamento:

12.1.1 Aquisição de 200 (duzentas) licenças pelo período de 05 (cinco) anos ou 60 (sessenta) meses.

12.1.2 Não deverão existir limites quanto ao uso de agentes, conectores, repositórios de armazenamento, hosts físicos e outras tecnologias agregadas a arquitetura da solução especificada.

12.1.3 Ser a última versão disponível, não será aceita a utilização de versões anteriores para cobrir algum item desse descritivo técnico.

12.1.4 Mostrar na console de gerenciamento a quantidade de licenças adquiridas e utilizadas.

12.1.5 Caso a solução ofertada necessite de algum banco de dados, o mesmo deverá ser fornecido devidamente licenciado sem nenhum custo extra.

12.1.6 A solução deve ser compatível com o Item 07 Equipamento de Armazenamento de Dados de Backup on-premises.

12.2 Cópia e Restauração de Dados:

12.2.1 Permitir o controle da banda utilizada durante a operação de cópia de proteção dos backups.

12.2.2 Ser capaz de realizar cópia de arquivos abertos sem que a consistência deles seja comprometida.

12.2.3 Possuir a opção de priorização de tarefas de proteção com opção de resumo da cópia caso uma atividade de menor prioridade seja colocada em estado de espera por uma tarefa de maior prioridade.

12.2.4 Possuir a funcionalidade de paralelizar a gravação dos dados em dispositivos de armazenamento (funcionalidade conhecida como multiplexação).

12.2.5 Ser capaz de enviar alertas através de e-mail com o objetivo de reportar eventos ocorridos na operação e configuração da solução.

12.2.6 Ser capaz de enviar traps SNMP (Simple Network Management Protocol) com o objetivo de reportar eventos ocorridos na operação da solução.

12.2.7 Possuir a funcionalidade de agendamento automático de tarefas de cópia.

12.2.8 Para um mesmo dado armazenado deve haver a possibilidade de configuração de diferentes períodos de retenção.

12.3 Gerenciamento das Operações de Proteção e Restauração:

12.3.1 Possuir interface única, que seja capaz de gerenciar e executar operações de proteção e recuperação dos sistemas operacionais Windows, Unix e Linux; ambiente de virtualização Acropolis Operating System; aplicações, Microsoft Active Directory e banco de dados Microsoft SQL Server, PostgreSQL e Oracle.

12.3.2 O acesso administrativo ao console do servidor de gerenciamento da solução poderá ser feito através de ferramenta disponibilizada no próprio software (console gráfico) ou através de navegador Web.

12.3.3 Implementar distribuição automática de carga entre os movimentadores de dados, ou seja, os dados oriundos dos clientes de backup deverão ser distribuídos de forma automática entre os servidores de cópia, e em caso de falha de um dos servidores, o cliente automaticamente irá encaminhar seus dados para o outro servidor de cópia ativo. Esta funcionalidade deverá ser nativa do produto, e não pode ser construída com o uso de soluções baseadas em softwares de cluster de terceiros.

12.3.4 A base de dados para armazenamento do catálogo deverá possuir mecanismo de proteção (backup) das informações armazenadas no catálogo e funcionalidades de recuperação rápida do catálogo em caso de desastre.

12.4 Criptografia dos Dados Protegidos

12.4.1 Implementar criptografia de dados na origem (cliente de backup), de uma forma que seja garantido que o dado que trafegará na rede de modo criptografado.

12.4.2 Deverá implementar no mínimo chaves de criptografia de 128 bits ou 256 bits.

12.5 Desduplicação dos Dados Protegidos

12.5.1 Permitir uso da tecnologia de desduplicação de dados para toda a capacidade licenciada, eliminando blocos repetidos, para cópias e arquivamento em disco e movimentação de dados desduplicados, independentemente do quantitativo de dispositivos de armazenamento que compõem a infraestrutura da CONTRATANTE.

12.5.2 Implementar desduplicação de blocos na origem (client-side desduplication), de forma que o cliente envie apenas novos blocos de dados criados e/ou modificados a partir da última cópia total completa;

12.5.3 Implementar desduplicação de dados nos servidores de armazenamento (target desduplication), de forma que tais servidores tratem adequadamente blocos repetidos enviados pelos clientes, evitando assim o armazenamento de blocos redundantes;

12.5.4 Implementar desduplicação de dados em tarefas de cópia;

12.5.5 Implementar desduplicação e compressão em uma mesma tarefa;

12.5.6 Permitir a restauração granular de arquivos ou sistemas de arquivos a partir de cópias em disco ou fita. Em caso de backup armazenado em disco a recuperação granular poderá ser feito utilizando-se cópias que possam estar desduplicados;

12.6 Alertas e Relatórios da Proteção de Dados

12.6.1 Quantidade de rotinas de backup concluídos nas últimas 24 horas, nos últimos 30 dias e nos últimos 12 meses.

12.6.2 Quantidade de recuperações efetuadas nas últimas 24 horas, nos últimos 30 dias e nos últimos 12 meses.

12.6.3 Resumo de rotinas de backup concluídos com sucesso, com erro ou não concluídos.

12.6.4 Mostrar o total de licenças adquiridas e o total de licenças utilizadas e caso ocorra uma nova aquisição de licenças as novas licenças deverão constar nesse relatório.

12.6.5 Enviar os seguintes alertas via e-mail: rotina de backup finalizada com sucesso, rotina de backup finalizada com erro e rotina de backup com problema.

12.7 Fornecimento de licenciamento do Sistema Operacional

12.7.1 Fornecimento de licenciamento do sistema operacional Microsoft Windows Server Datacenter, baseado em núcleo (core-based licensing , para 48 cores físicos).

12.7.2 As licenças deverão ser entregues em formato eletrônico, acompanhadas de instruções para instalação e ativação, devendo incluir garantia mínima de 60 (sessenta) meses ou suporte técnico equivalente.

12.7.3 O licenciamento deverá ser compatível com servidores físicos e virtuais , observando o licenciamento mínimo exigido pela fabricante.

12.7.4 As licenças fornecidas deverão ser originais, legítimas e adquiridas por meio de canal autorizado da Microsoft, com comprovação documental no momento da entrega.

12.7.5 As licenças deverão ser entregues em formato eletrônico, acompanhadas de instruções para instalação e ativação, incluindo garantia mínima de 60 (sessenta) meses ou suporte técnico equivalente.

12.7.6 O item deverá ser plenamente compatível com a infraestrutura tecnológica do MPAM, em especial com ambientes físicos e virtuais já existentes.

12.7.7 Incluir Software Assurance (SA), garantindo direito a atualizações, suporte técnico estendido e benefícios de mobilidade de licenças durante todo o período contratual.

13. ITEM 07 - EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES

13.1 Características gerais:

13.1.1 Deverá corresponder a um sistema inteligente dedicado ao armazenamento de backups em disco, com funcionalidades integradas de criptografia, compressão, desduplicação e replicação dos dados já desduplicados;

13.12 O equipamento deve estar listado no site oficial do fabricante como um appliance ou sistema de armazenamento de backup em disco, em produção ativa;

13.1.3 O hardware e o software devem ser do mesmo fabricante. Não serão aceitas soluções customizadas especificamente para esta licitação, nem combinações OEM, equipamentos usados, recondicionados, de demonstração ou gateways;

13.1.4 O equipamento deve ser novo, sem uso anterior, pertencente à linha mais recente do fabricante, em produção contínua e sem previsão de fim de suporte (EOSL) nos próximos cinco anos a partir da data de abertura da licitação;

13.1.5 Soluções baseadas exclusivamente em software (appliances virtuais) não serão aceitas;

13.1.6 Deve ser compatível com montagem em racks padrão de 19”, acompanhado de trilhos, cabos, conectores, manuais e todos os itens necessários para instalação, configuração e operação completa;

13.1.7 Para soluções com arquitetura Scale-Out:

13.1.7.1 Deve permitir conexão com outros sistemas do mesmo fabricante para expansão de desempenho e capacidade;

13.1.7.2 Deve operar em modo ativo-ativo (alta disponibilidade com balanceamento de carga), redirecionando automaticamente os backups em caso de falha de um dos sistemas;

13.1.8 Para soluções com arquitetura Scale-Up:

13.1.8.1 Deve incluir duas controladoras, operando em modo ativo-ativo ou ativo-passivo, garantindo continuidade das operações de backup em caso de falha de uma das controladoras.

13.2 Requisitos de disponibilidade:

13.2.1 Deve possuir tolerância a falhas em componentes como discos, fontes de alimentação e ventiladores;

13.2.2 Deve contar com mecanismos que assegurem a integridade dos dados mesmo em casos de interrupção abrupta ou desligamento acidental;

13.2.3 Deve incluir proteção de cache de escrita para evitar perda de dados em caso de falha de energia;

13.2.4 Deve ser entregue com arranjos RAID-6, RAID-DP ou equivalente, com tolerância a falha de até dois discos e pelo menos um disco hot-spare por grupo RAID;

13.2.5 Os discos devem ser hot-pluggable e hot-swappable, permitindo substituição sem interrupção do sistema;

13.2.6 Deve oferecer monitoramento remoto pelo fabricante, com recursos como Call-Home para detecção proativa de falhas ou pré-falhas.

13.3 - Capacidade, desempenho e conectividade:

13.3.1 Deve oferecer no mínimo 100 (cem) TB de capacidade útil, sem considerar compressão, desduplicação ou espaço reservado ao sistema;

13.4 Para soluções Scale-Out:

13.4.1 Deve atingir taxa mínima de 5 TB/hora (cinco terabytes por hora) para operações de backups, sem considerar desduplicação;

13.4.2 Capacidade de ampliar a solução previamente fornecida, através da interconexão de módulos similares ou não, do mesmo fabricante. Para a expansão, volumes em nuvem, off-site, replicação ou similar para o atendimento a este requisito não serão aceitos, mantendo a característica de desduplicação global da solução.

13.4.3 A criptografia deve ser feita via hardware. Caso seja por software, a taxa de transferência deve ser 30% superior à mínima exigida, considerando apenas a desduplicação.

13.5 Para soluções Scale-Up:

13.5.1 Deve permitir expansão para pelo menos 500 TB (quinhentos terabytes) de capacidade útil, sem considerar compressão ou desduplicação, por meio de gavetas de discos, sem troca ou upgrade das controladoras originais, mantendo a desduplicação global;

13.5.2 Deve atingir taxa mínima de 15 TB/hora (quinze terabytes por hora) para operações de backup, considerando apenas a desduplicação;

13.5.3 A criptografia deve ser realizada por hardware. Se for por software, a taxa de transferência deve ser 30% superior à exigida, considerando apenas a desduplicação;

13.5.4 Deve incluir no mínimo duas interfaces de rede de 25 Gbps com conectores SFP28 para backup via LAN, fornecidos com o equipamento;

13.5.5 Deve incluir pelo menos duas interfaces de 1 GbE com conectores UTP CAT6 para gerenciamento, também fornecidos;

13.5.6 Deve possuir ao menos uma porta IPMI/iLO/iDRAC ou equivalente;

13.5.7 Interfaces adicionais devem ser fornecidas conforme as melhores práticas do fabricante para garantir o desempenho requerido;

13.5.8 Fornecer a quantidade necessária de discos para atingimento da performance mínima solicitada, ou seja, se a solução requerer mais discos além dos necessários para atender a capacidade solicitada no item 8.3.1, discos adicionais deverão ser fornecidos. Não é obrigatório o licenciamento de capacidade desses discos adicionais

13.5.9 Comprovar a taxa de transferência através da ferramenta de dimensionamento do fabricante da solução, desconsiderando o uso de ferramentas/protocolos de otimizações na origem no seu dimensionamento, caso a solução ofertada não seja fornecida com todos os discos possíveis para sua capacidade total.

14. ITEM 08 - SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES

14.1 Características gerais

14.1.1 Permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, de maneira perpétua, irrestrita e sem necessidade de licenciamentos ou ônus adicionais;

14.1.2 -Possuir licenças na modalidade de uso perpétuo para todo para o completo atendimento das especificações técnicas do equipamento, ou seja, o equipamento deverá continuar a operar normalmente mesmo após o período de manutenção e assistência técnica contratado;

14.1.3 Para soluções com arquitetura Scale-Out:

14.1.3.1 A desduplicação de dados deve ser mantida de forma global em todo o ambiente de armazenamento, independentemente da quantidade de dispositivos interligados;

14.1.4 Para soluções com arquitetura Scale-Up:

14.1.4.1 A desduplicação global deve ser preservada em todo o conjunto de armazenamento.

14.2 Requisitos de compatibilidade:

14.2.1 O software deve ser homologado e plenamente compatível com o software de backup fornecido no ITEM 06 - SOFTWARE DE BACKUP DE DADOS;

14.2.2 Deve permitir leitura e gravação simultâneas via protocolos CIFS, NFS e OST;

14.2.3 Deve oferecer suporte aos protocolos de monitoramento SNMP e Syslog;

14.2.4 Deve possibilitar que aplicações como Oracle (via RMAN) e Microsoft SQL realizem backups tipo Stream Based (Oracle Stream Backup) e “database dump” diretamente no equipamento, por meio de CIFS e NFS, sem uso de software de backup, evitando o consumo de licenças e sem necessidade de licenciamento por volume (TB) ou por servidor (CPU, Core, Tier). Caso essa funcionalidade exija licenciamento, todos os itens necessários devem ser incluídos na proposta.

14.3 - Funcionalidades operacionais:

14.3.1 Deve permitir a execução simultânea de processos de backup e restore;

14.3.2 Deve dispor de interface de gerenciamento baseada em navegador (WEB);

14.3.3 A desduplicação deve ser global, mesmo com volumes lógicos distintos, identificando dados redundantes entre diferentes fontes de backup e armazenando-os apenas uma vez;

14.3.4 A desduplicação deve ocorrer em conjunto com os processos de backup e restore, sem necessidade de janelas específicas;

14.3.5 Deve incluir mecanismos nativos para verificação da integridade dos dados desduplicados, com capacidade de correção automática em caso de inconsistência, sem uso de scripts externos;

14.3.6 Deve permitir replicação de dados via rede IP (LAN/WAN), de forma assíncrona, entre sistemas compatíveis do mesmo fabricante, utilizando desduplicação para otimizar o uso da banda;

14.3.7 Deve suportar topologias de replicação como 1:1, 1:N, N:1 e o cascateamento de equipamentos;

14.3.8 Deve integrar-se ao Microsoft Active Directory 2012 ou superior, para autenticação e controle de acesso;

14.3.9 Os dados armazenados devem ser criptografados com algoritmos de no mínimo AES128-SHA ou AES256-SHA;

14.3.10 Deve permitir autenticação em dois fatores (2FA), com integração a soluções OTP como Google Authenticator, Microsoft Authenticator ou equivalentes;

14.3.11 Caso a solução exija um sistema OTP específico com licenciamento ou hardware dedicado (ex: Common Access Card /Personal Information Verification cards, sistemas de OTP/tokenização licenciados, etc), todos os componentes necessários devem ser fornecidos para pelo menos 5 usuários;

14.3.12 Deve oferecer recurso de autorização dupla (Dual Auth) para alterações em configurações de proteção contra ransomware;

14.3.13 Deve incluir funcionalidades avançadas de segurança cibernética para proteção contra ransomware, assegurando a integridade dos dados de backup;

14.4 - Deve possuir mecanismo de imutabilidade dos dados:

14.4.1 A proteção deve estar sempre ativa, independente do software de backup, sem necessidade de janelas específicas ou scripts;

14.4.2 A proteção deve ser aplicada imediatamente após a desduplicação dos dados, sem depender de agendamento;

14.4.3 Deve adotar o conceito de air-gap, tornando os dados protegidos invisíveis à rede e inacessíveis por softwares de backup, independentemente do protocolo utilizado.

15. ITEM 09 – SWITCH CORE

15.1 Especificações Físicas

15.1.1 O equipamento deve contar com, no mínimo, 48 portas SFP28 compatíveis com velocidades de 1, 10 e 25 Gigabit Ethernet.

15.1.2 As interfaces devem ser auto-sensíveis, ajustando automaticamente a velocidade conforme o transceiver conectado, sem necessidade de configuração manual.

15.1.3 A altura máxima permitida é de 1 unidade de rack (1 RU).

15.1.4 Deve ser compatível com racks padrão de 19 polegadas, incluindo os kits de fixação apropriados.

15.1.5 As portas SFP28 devem aceitar transceivers dos tipos SFP+ 10GBase-SR, 10GBase-LR, 10GBase-ER, SFP 1000Base-SX, 1000Base-LX, 1000Base-ZX, 1000Base-T e cabos DAC.

15.1.6 Devem ser entregues ao menos 10 cabos DAC 25GbE SFP28 com comprimento mínimo de 3 metros, compatíveis com os appliances do item 1.

15.1.7 O switch deve possuir pelo menos 6 portas QSFP28 de 100GbE, com suporte a velocidades de 40GbE.

15.1.7.1 Deve ser compatível com transceivers 40GBase-SR4 e 40GBase-LR4.

15.1.7.2 Deve aceitar transceivers 100GBase-SR4 e 100GBase-LR4.

15.1.7.3 Deve suportar cabos DAC.

15.1.8 Deve acompanhar pelo menos 1 cabo DAC 100GbE com no mínimo 1 metro de comprimento, para conexão redundante entre switches.

15.1.9 A capacidade da matriz de comutação deve ser de no mínimo 4 Tbps.

15.1.10 O throughput mínimo exigido é de 1,5 Bpps.

15.1.11 O buffer deve ter capacidade mínima de 32 MB.

15.1.12 A latência máxima permitida é de 900 nanosegundos.

15.1.13 Deve suportar ao menos 160.000 endereços MAC.

15.1.14 A tabela ARP deve comportar até 64.000 entradas ou mais.

15.1.15 Deve aceitar jumbo frames com tamanho mínimo de 9000 bytes.

15.1.16 É obrigatória a presença de pelo menos uma porta RJ-45 para gerenciamento fora de banda.

15.1.17 O equipamento deve vir com CPU e memória (RAM e Flash) suficientes para suportar todas as funcionalidades descritas.

15.1.18 Fontes de alimentação internas devem ser redundantes e com ajuste automático para 110/220V.

15.1.19 O sistema de ventilação deve ser redundante, com fluxo de ar configurável (frontal-traseiro ou traseiro-frontal), sendo fornecido com ventiladores de fluxo frontal-traseiro.

15.1.20 Fontes e ventiladores devem ser hot-swappable e redundantes, permitindo substituição sem interrupção.

15.1.21 O equipamento deve ser projetado para ambientes de datacenter, com comutação de pacotes de alto desempenho.

15.2 - Funcionalidades Gerais

15.2.1 LEDs por porta devem indicar status e atividade do link.

15.2.2 A arquitetura da solução deve ser baseada em “spine-leaf”, com VxLAN como plano de dados e BGP EVPN como plano de controle.

15.2.3 Deve possuir porta de console para configuração via CLI, com conector RJ-45 ou RS-232, incluindo cabos e adaptadores necessários.

15.2.4 Gerenciamento via SSHv2 deve ser suportado.

15.2.5 O switch deve ter criptografia FIPS 140-2 validada pelo NIST.

15.2.6 Deve permitir espelhamento de uma ou mais portas para outra porta específica.

15.2.7 Também deve permitir espelhamento para porta remota via tunelamento, mesmo em domínios L2 distintos.

15.2.8 Deve implementar Netflow, sFlow ou tecnologia equivalente.

15.2.9 Gerenciamento via SNMPv3 deve ser possível.

15.2.10 Deve suportar o protocolo Syslog.

15.2.11 Deve implementar NTPv4 ou SNTP.

15.2.12 Autenticação via RADIUS deve ser suportada.

15.2.13 Autenticação via TACACS+ também deve ser suportada.

15.2.14 Controle de acesso por porta (IEEE 802.1x) deve estar presente.

15.2.15 Deve haver controle de broadcast, multicast e unicast por porta.

15.2.16 Deve implementar pelo menos uma fila de saída com prioridade estrita (SP Strict Priority) e divisão de banda ponderada (WRED, WRR ou similar).

15.2.17 Deve classificar, marcar e priorizar tráfego com base em IEEE 802.1p CoS.

15.2.18 Deve classificar, marcar e priorizar tráfego com base em DSCP (Differentiated Services CodePoint), conforme IETF.

15.2.19 Deve permitir classificação de tráfego por IP, portas TCP/UDP e endereços MAC.

15.3 - Virtualização de Switch

15.3.1 Deve permitir agregação de portas multi-chassi com redundância ativa/ativa sem Spanning Tree, usando MLAG,

MC-LAG, M-LAG, VLT (Virtual Link Trunking), Multi-Chassis EtherChannel ou equivalentes.

15.3.2 Todos os componentes necessários para alta disponibilidade devem ser fornecidos, incluindo cabos, transceivers e licenças.

15.3.3 Em modo virtualizado, os switches devem operar com processamento local, sem tempo de convergência em caso de falha.

15.4 - Funcionalidades de Camada 2

15.4.1 Suporte a até 4.000 VLANs conforme IEEE 802.1Q.

15.4.2 Implementação de VLAN Trunking conforme IEEE 802.1Q, com controle de VLANs permitidas por tronco.

15.4.3 Suporte a Link Aggregation (LAG) conforme IEEE 802.3ad.

15.4.4 Deve suportar no mínimo 80 grupos LAG com até 16 portas cada.

15.4.5 Implementação dos padrões IEEE 802.1d, 802.1s e 802.1w.

15.4.6 Deve possuir mecanismo de proteção da root bridge do Spanning Tree.

15.4.7 Deve permitir bloqueio de BPDUs em portas em modo fast forwarding, com desativação automática ao recebê-los.

15.4.8 Implementação de LLDP e LLDP-MED para descoberta de vizinhos.

15.4.9 Suporte a DCB com PFC (IEEE 802.1Qbb), ETS (IEEE 802.1Qaz) e DCBx.

15.5 - Funcionalidades de Roteamento

15.5.1 Deve realizar roteamento de camada 3 entre VLANs.

15.5.2 Suporte ao protocolo OSPFv3.

15.5.3 Suporte ao protocolo BGPv4.

15.5.4 Capacidade para no mínimo 106.000 rotas IPv4.

15.5.5 Capacidade para no mínimo 52.000 rotas IPv6.

15.5.6 Operação simultânea com IPv4 e IPv6.

15.5.7 Implementação de VRF ou VRF-Light.

15.5.8 Suporte a roteamento baseado em políticas (PBR).

15.5.9 Implementação do protocolo VRRPv3.

CLÁUSULA TERCEIRA – DA IMPLANTAÇÃO DA SOLUÇÃO E SERVIÇOS CORRELATOS:

A **CONTRATADA** será responsável por toda a instalação e configuração dos equipamentos, firmwares e softwares, incluindo o fornecimento de quaisquer itens adicionais necessários à sua execução.

1. A instalação poderá ser realizada integral ou parcialmente pelo fabricante, devendo a **CONTRATADA** prever esses serviços em sua proposta.

2. A **CONTRATADA** deverá disponibilizar técnicos certificados pelo fabricante, habilitados a instalar, operar e configurar os equipamentos fornecidos. Caso a instalação seja conduzida diretamente pelo fabricante, essa exigência estará dispensada.

3. A **CONTRATANTE** reserva-se o direito de solicitar a substituição parcial ou total da equipe da **CONTRATADA** durante a fase de implantação, caso seja constatada a ausência de qualificação técnica adequada.

4. Deverá ser apresentado cronograma de implantação e proposta de configuração da solução, ambos sujeitos à aprovação da equipe técnica da **CONTRATANTE**.

5. Ao final da instalação, deverão ser entregues, em meio digital, os manuais e procedimentos utilizados.

6. A instalação deverá incluir, no mínimo:

a) Fixação dos equipamentos em rack padrão 19”;

b) Conectorização elétrica e energização dos equipamentos;

c) Atualização de firmwares de todos os componentes (BIOS, Gerência Out of Band, controladoras HBA, interfaces de rede, discos, etc.);

d) Atualizações e releases disponíveis no site oficial;

e) Registro dos equipamentos e licenças no portal do fabricante.

f) Conectorização das interfaces de rede com os respectivos cabos/conectores;

g) Instalação, atualização e configuração dos componentes conforme boas práticas;

h) Integração dos equipamentos à rede da **CONTRATANTE**;

i) Outras atividades correlatas para garantir a operação da solução no ambiente da **CONTRATANTE**.

7. A aceitação dos itens do objeto contratado no ato da sua entrega ao Ministério Público do Estado do Amazonas será considerada como de caráter provisório. A aceitação definitiva dar-se-á após a instalação e configuração dos itens do objeto e a verificação do atendimento às especificações técnicas constantes deste instrumento.

8. Serão recusados os objetos imprestáveis ou defeituosos, que não atendam as especificações constantes neste termo de referência e/ou que não estejam adequados para uso.

9. Os itens deverão ser instalados, configurados e ativados pela **CONTRATADA** em local indicado pelo DTIC do MPAM.

10. O prazo para conclusão da instalação e configuração dos equipamentos e softwares será de até 30 (trinta) dias, contados a partir da data do recebimento provisório dos mesmos pela DTIC e emissão do termo provisório de recebimento.

11. Os equipamentos e serviços serão aceitos se, e somente se, houver comprovação de que todos os requisitos técnicos especificados neste contrato tenham sido atendidos e os itens se encontre em operação plena. Essa comprovação será feita mediante observação direta das características dos equipamentos, consulta à documentação técnica fornecida e verificação dos serviços de instalação e configurações.

12. Os serviços de instalação, configuração, migração e transferência de conhecimento técnico deverão ser realizados conforme especificado em cada item.

13. O serviço de instalação e configuração tem a finalidade de garantir que os itens fornecidos estejam operacionais no ambiente de Produção, e de Contingência caso exista.

14. Todos os serviços de instalação, configuração, migração e transferência de conhecimento técnico deverão ser executados de forma presencial, por especialista(s) técnico(s) certificado(s) nos componentes pelo fabricante dos mesmos com a devida apresentação de certificado(s) técnico(s) emitido(s) pelo fabricante do(s) produto(s).

15. Os serviços de instalação, configuração, migração e transferência de conhecimento técnico, deverão ser agendados previamente entre as partes, através de e-mail ou telefone, e deverão ser realizados em dias úteis e em horário de expediente do MPAM.

16. A transferência de conhecimento técnico será feita através de treinamento referente aos componentes do objeto deste instrumento, abrangendo todos os recursos de hardware e software do ambiente, para até 10 (dez) técnicos designados pela **CONTRATANTE**, cobrindo no mínimo os seguintes tópicos:

a) Instalação.

b) Configuração básica e avançada.

c) Operação básica e avançada.

d) Gerenciamento da solução/expansão.

e) Administração.

f) Solução de problemas (troubleshouting).

g) Laboratório prático baseado na solução/expansão adquirida.

17. O treinamento deverá ser realizado nas seguintes condições:

a) Deverá ser ministrado em língua portuguesa do Brasil, de forma presencial;

b) Local: Av. Coronel Teixeira, nº 7.995, Nova Esperança II, CEP. 69037-473, Manaus-AM;

c) Carga horária mínima de 30 (trinta) horas, divididas em, no máximo, 4 (quatro) horas diárias;

d) O conteúdo programático deverá ser aprovado pela DTIC antes da realização de cada treinamento.

18. O material didático e os certificados deverão ser disponibilizados pela **CONTRATADA** com finalidade específica para ministrar o treinamento à DTIC.

19. Ao final do treinamento, os participantes deverão estar aptos a operar e administrar as tecnologias referenciadas neste instrumento.

20. A transferência de conhecimento técnico deverá ocorrer no período correspondente ao recebimento definitivo da expansão, ou em caso de impedimento justificado, em nova data aceita pela fiscalização do contrato.

21. Caberá ainda a **CONTRATADA** a execução de todas as atividades, bem como o fornecimento de todos os materiais necessários e suficientes para a instalação e configuração dos equipamentos fornecidos.

22. O planejamento, instalação, configuração e migração dos equipamentos deverão ser executados por técnicos habilitados e credenciados pelo fabricante.

23. A **CONTRATADA** deverá designar um profissional Técnico Responsável para acompanhar a execução dos serviços desde o planejamento até a implantação da expansão.

24. Antes da implantação dos equipamentos, a equipe técnica da **CONTRATADA** deverá apresentar o cronograma da implantação contendo: o plano de instalação, plano de contingência e prazos máximos para a realização da mudança.

25. A **CONTRATADA** deverá realizar a migração completa do ambiente computacional atualmente em operação para a nova infraestrutura fornecida, incluindo, mas não se limitando a: máquinas virtuais, clusters Kubernetes, bancos de dados, configurações nativas, políticas de segurança, integrações existentes e demais componentes necessários para garantir a continuidade dos serviços. A migração deverá ser executada de forma planejada, segura e sem impacto significativo na disponibilidade dos sistemas, observando as melhores práticas recomendadas pelo fabricante e garantindo a integridade dos dados e das aplicações.

26. A **CONTRATADA** deverá prover PDU´s ou réguas smart adequadas para a devida conecção elétrica necessária dos equipamentos específicados neste contrato.

27. Após a conclusão das atividades de instalação, configuração, migração e pré-operação, deve ser iniciada a fase de operação assistida do objeto contratado.

28. A operação assistida terá duração total de 90 (noventa) dias corridos, sendo 15 (dias) dias corridos de forma presencial, e o restante do período podendo ser de forma remota, de modo a assegurar o auxílio e pronta ação corretiva da **CONTRATADA** necessária em questões relacionadas com a configuração, monitoramento e estabilização da nova solução com o objetivo de garantir o bom funcionamento dos equipamentos e serviços.

29. Durante a fase de operação assistida, a **CONTRATADA** deverá atuar de maneira a mitigar os riscos decorrentes da transição tecnológica da plataforma atualmente existente para a nova solução.

30. As atividades de operação assistida devem ser realizadas somente nas dependências da sede do MPAM em Manaus-AM, em horário de expediente da Procuradoria-Geral, e devem se iniciar logo após a migração tecnológica, testes e ativação dos serviços. Caso seja necessária a consecução de atividades que possam afetar a disponibilidade dos serviços, as atividades de operação assistida podem ser prolongadas após o horário de expediente da Procuradoria-Geral, sem qualquer ônus para o MPAM.

31. O período de operação assistida deve englobar, dentre outras, as seguintes atividades:

a) Monitoramento de funcionamento e da capacidade dos serviços;

b) Identificação e abertura de chamados técnicos para solução de falhas na solução;

c) Resolução de problemas (troubleshooting);

d) Análise da efetividade de regras e configurações;

e) Simulação de abertura de chamados;

f) Instalação de patches;

g) Execução/revisão de procedimentos de backup e restore de configurações;

h) Geração de relatórios técnicos, administrativos e gerenciais;

CLÁUSULA QUARTA – DA VIGÊNCIA:

O presente contrato tem vigência de **60 (sessenta) meses**, contados da data de publicação do extrato no Diário Oficial do MPAM, nos termos dos art. 105, caput, e 106, caput, da Lei n.º 14.133/2021.

1. A **CONTRATADA** terá o prazo de 5 (cinco) dias úteis para rubricar o contrato ou seus aditivos, contados a partir da data em que ela for notificada dessa providência pela Divisão de Contratos e Convênios (DCCON) da **CONTRATANTE**.

1.1 A assinatura contratual será efetuada por meio do Sistema Eletrônico de Informações (SEI) da **CONTRATANTE**.

1.2 Na hipótese de assinatura de termo aditivo de prorrogação, caso o prazo de expiração da avença for menor que o disposto no item 1 desta cláusula, a **CONTRATADA** deverá rubricar o instrumento até o último dia útil da vigência contratual.

1.3 Se a **CONTRATADA**, regularmente notificada pela DCCON, não assinar o contrato ou seu aditivo no prazo disposto neste item, ela ficará sujeita às penalidades descritas neste instrumento.

2. Consoante o art. 107, da Lei n.º 14.133/2021, o contrato poderá ser prorrogado sucessivas vezes, até o limite de 10 (dez) anos, desde que os preços permaneçam vantajosos para a **CONTRATANTE** e haja suficiência orçamentária.

3. A **CONTRATADA** não possui direito subjetivo à prorrogação contratual.

CLÁUSULA QUINTA – DA FUNDAMENTAÇÃO LEGAL DA CONTRATAÇÃO:

O presente contrato foi firmado mediante _____, fundamentando-se no art. _____, da Lei n.º 14.133/2021, e no Ato n.º 008/2024/PGJ, o qual define os procedimentos administrativos para contratação de bens e serviços no âmbito do Ministério Público do Estado do Amazonas, bem como nas demais legislações correlatas, conforme o _____.

CLÁUSULA SEXTA – DO REGIME DE EXECUÇÃO:

Conforme o Termo de Referência n.º 28.2025.DTIC.2002143.2025.007562 e o art. 6º, XXIX, da Lei n.º 14.133/2021, o regime de execução deste contrato é o da **empreitada por preço global**, modalidade em que a contratação do serviço se dá por preço certo e total.

CLÁUSULA SÉTIMA – DOS DOCUMENTOS INTEGRANTES:

Para melhor caracterizar o presente contrato, integram também este instrumento, como se nele estivessem transcritos, obedecidos os termos da legislação sobre contratos públicos, os seguintes documentos:

1. O Termo de Referência n.º 28.2025.DTIC.2002143.2025.007562;

2. O Edital de Licitação n.º _____;

3. A Proposta Comercial n.º _____ encaminhada pela **CONTRATADA**, no dia _____, contendo os valores unitário e total..

CLÁUSULA OITAVA – DO VALOR:

O valor global e estimado deste contrato é de _____

1. No preço contratado já estão incluídos todos os custos e despesas, tais como: custos diretos e indiretos, tributos incidentes, despesas administrativas, materiais, serviços, encargos sociais, trabalhistas, seguros, frete, embalagens, lucro, e outros necessários ao cumprimento integral do objeto deste instrumento.

CLÁUSULA NONA – DA GESTÃO, FISCALIZAÇÃO E ACOMPANHAMENTO:

O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133/21, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

1. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

2. As comunicações entre a **CONTRATANTE** e a **CONTRATADA** devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

3. A **CONTRATANTE** poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

4. Após a assinatura do contrato ou instrumento equivalente, a **CONTRATANTE** poderá convocar o representante da **CONTRATADA** para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da **CONTRATADA**, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

5. Preposto

5.1 A **CONTRATADA** deverá manter preposto junto à PGJ-AM, aceito pela respectiva **FISCALIZAÇÃO**, durante o período de vigência do contrato, para representá-la administrativamente, sempre que for necessário, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado, o qual deverá ser indicado mediante declaração de que deverá constar o nome completo, nº do CPF e do documento de identidade, além dos dados relacionados à sua qualificação profissional.

5.2 A empresa orientará o seu **PREPOSTO** quanto à necessidade de acatar as orientações da Administração, inclusive quanto ao cumprimento das Normas Internas e de Segurança e Medicina do Trabalho.

5.3. A **CONTRATANTE** poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a **CONTRATADA** designará outro para o exercício da atividade.

6. Fiscalização

6.1 A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos, conforme indicação em portaria específica publicada no Diario Oficial do MPAM.

6.2 Compete ao **Gestor da Ata/Contrato,** além de outras atribuições, nos termos da lei:

a) Acompanhar os prazos de execução e de vigência do contrato, conforme as rotinas e procedimentos estabelecidos pelo MPAM, e as cláusulas do contrato ou instrumento equivalente, comunicando à **CONTRATADA** e à unidade competente da Administração eventuais atrasos e encaminhando, em tempo hábil, expediente para a prorrogação do contrato;

b) Coordenar e acompanhar a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração;

c) Acompanhar a manutenção das condições de habilitação da **CONTRATADA**, para fins de empenho de despesa e pagamento, e anotar os problemas que obstam o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais;

d) Comunicar à Autoridade Competente as ocorrências relacionadas à execução do contrato que ultrapassarem a sua competência;

e) Emitir TERMO DE RECEBIMENTO DEFINITIVO, juntamente com a **FISCALIZAÇÃO**, comprovando a avaliação do cumprimento das obrigações assumidas pela **CONTRATADA**;

f) Receber e conferir as faturas/notas fiscais emitidas pela **CONTRATADA**, e encaminhar, devidamente certificadas/atestadas ao setor competente, observando, previamente, se a fatura apresentada pela **CONTRATADA** refere-se ao objeto que foi efetivamente pactuado;

g) Encaminhar o processo à unidade competente para proceder à liquidação da despesa, alertando para a data limite para pagamento das notas fiscais/fatura;

h) Requisitar a prorrogação de contrato, se possível, junto à Autoridade Competente, que deve ser providenciada antes de seu término, reunindo as justificativas necessárias;

i) Elaborar a comunicação à área competente para abertura de nova licitação, antes de findo a prestação de serviços e com antecedência razoável;

j) Cuidar das alterações de interesse da **CONTRATADA**, que deverão ser por ela formalizadas e devidamente fundamentadas, principalmente em se tratando de pedido de reequilíbrio econômico-financeiro ou repactuação, sendo que, no caso de pedido de prorrogação de prazo, deverá ser comprovado o fato impeditivo da execução, o qual, por sua vez, deverá corresponder àqueles previstos na Lei n. 14.133/21 e alterações, se possível;

k) Esclarecer dúvidas e transmitir instruções à **CONTRATADA**, comunicando alterações de prazos, cronogramas de execução e especificações do projeto, inclusive solicitando ao setor competente da Administração, quando necessário a emissão de parecer técnico;

l) Deflagrar e conduzir os procedimentos de fiscalização à **CONTRATADA**, com base nos termos contratuais, sempre que houver descumprimento de suas cláusulas por culpa da **CONTRATADA**, acionando as instâncias superiores e/ou os órgãos públicos competentes quando o fato exigir;

m) Verificar se a entrega de materiais ou a prestação do serviço está sendo executada em conformidade com o pactuado, no tocante a prazo, especificações, preço e quantidade;

n) Rejeitar equipamentos e serviços que estejam em desacordo com as especificações do objeto contratado;

o) Zelar pelo efetivo cumprimento das obrigações contratuais assumidas e pela qualidade dos produtos fornecidos e dos serviços prestados;

p) Notificar a **CONTRATADA** em qualquer ocorrência desconforme com as cláusulas contratuais, sempre por escrito, com prova de recebimento da notificação (procedimento formal, com prazo);

q) Verificar a regularidade fiscal, trabalhista e previdenciária da contratada para fins de pagamento; e

r) Orientar a **CONTRATADA**, por intermédio do preposto, sobre a correta execução do contrato e, pelo mesmo meio, levar ao seu conhecimento as situações temerárias, recomendando medidas e estabelecendo prazo de resolução.

6.3 Compete ao **Fiscal Técnico**, além de outras atribuições, nos termos da lei:

a) Acompanhar e fiscalizar a execução do contrato nos aspectos técnicos da solução, conforme o respectivo regramento técnico aplicável;

b) Zelar pelo efetivo cumprimento das obrigações contratuais assumidas e pela qualidade dos produtos fornecidos e dos serviços prestados, de modo a assegurar os melhores resultados para a Administração;

c) Ler atentamente o Termo de Contrato e anotar em registro próprio todas as ocorrências relacionadas à sua execução, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados;

d) Esclarecer dúvidas do preposto/representante da **CONTRATADA** que estiverem sob a sua alçada, encaminhando às áreas competentes os problemas que surgirem quando lhe faltar competência;

e) Notificar à **CONTRATADA**, para a correção da execução do contrato, de determinando prazo para a correção, qualquer inexatidão ou irregularidade;

f) Informar ao Gestor do Contrato, em tempo hábil, irregularidades que possam demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso;

g) Comunicar ao Gestor do Contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual;

h) Avaliar a qualidade dos serviços realizados ou dos itens entregues e justificativas, de acordo com os critérios de aceitação definidos em contrato; e

i) Orientar a **CONTRATADA**, por intermédio do preposto, sobre a correta execução do contrato e, pelo mesmo meio, levar ao seu conhecimento as situações temerárias, recomendando medidas e estabelecendo prazo de resolução.

CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DA CONTRATANTE:

São obrigações da **CONTRATANTE**:

1. Acompanhar e fiscalizar, como lhe aprouver e no seu exclusivo interesse, na forma prevista na Lei n.º 14.133/21, exigindo o cumprimento de todas as obrigações assumidas, de acordo com o contrato e seus anexos.

2. Nomear **GESTOR** e **FISCALIZAÇÃO** técnica e administrativa, para acompanhar e fiscalizar, a execução dos contratos.

3. As ações de fiscalização não excluem nem reduzem a responsabilidade da **CONTRATADA**, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios ou emprego de material inadequado ou de qualidade inferior.

4. Fornecer à **CONTRATADA** as informações necessárias à fiel execução do objeto deste instrumento.

5. Permitir o acesso, acompanhar e fiscalizar a execução do contrato, verificando a conformidade da prestação dos serviços e regular a entrega dos itens, de forma a assegurar o perfeito cumprimento do contrato.

6. Anotar em registro próprio e notificar a **CONTRATADA**, por escrito, a ocorrência de eventuais imperfeições, defeitos de fabricação, e avarias nos itens, fixando prazo para a sua reposição.

7. Rejeitar, no todo ou em parte, serviço ou fornecimento executado em desacordo com o contrato.

8. Efetuar regularmente o pagamento da **CONTRATADA**, dentro dos critérios estabelecidos neste contrato, quanto aos serviços devidamente realizados, por meio de Ordem Bancária, após o atesto das notas fiscais/faturas pelo comitê responsável.

9. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

9.1 A **CONTRATANTE** terá o prazo de 1 (um) mês, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

10. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pela **CONTRATADA** no prazo máximo de 1 (um) mês.

11. A **CONTRATANTE** não responderá por quaisquer compromissos assumidos pela **CONTRATADA** com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da **CONTRATADA**, de seus empregados, prepostos ou subordinados.

CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES DA CONTRATADA:

A **CONTRATADA** deverá cumprir todas as obrigações constantes neste termo de referência, minuta de contrato e seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando:

1. Apresentar, no prazo de até 10 (dez) dias corridos, contados a partir da assinatura do contrato ou do recebimento da Nota de Empenho e da Autorização de Fornecimento de Materiais/Serviços:

1.1 Indicação formal do preposto da **CONTRATADA** apto a representá-la junto à **CONTRATANTE**, que deverá responder pela fiel execução do contrato, designado para acompanhar sua execução e atuar como interlocutor principal junto à **CONTRATANTE**, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

a) A indicação do preposto deverá ser acompanhada de seus dados pessoais, (no mínimo o nome completo e CPF do funcionário da empresa) e dados de contrato, como e-mail, telefone, whatsapp e outros.

1.2 Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste instrumento.

2. Efetuar a entrega do objeto contratado, dentro do prazo e de acordo com as especificações constantes deste contrato, observando as prescrições e as recomendações do fabricante, a legislação estadual ou municipal, se houver, bem como outras normas correlatas, ainda que não estejam explicitamente citadas neste documento e seus anexos.

3. Apresentar, no prazo de até 10 (dez) dias úteis, contados a partir da entrega do objeto, o correspondente TERMO DE GARANTIA E ASSISTÊNCIA TÉCNICA, para os equipamentos/softwares/licenças fornecidos incluindo seus números de série, com o prazo de garantia solicitado nesta avença.

4. Não transferir a outrem, no todo ou em parte, o objeto deste termo, não sendo aceita a transferência de responsabilidade para outras entidades, sejam fabricantes, técnicos, subempreiteiros ou quaisquer outros.

4.1 É vedada a subcontratação total ou parcial do objeto, bem como a cessão ou transferência deste instrumento contratual, no todo ou em parte, incluindo a transferência da execução a terceiros, a qualquer título, sem prejuízo da possibilidade de a **CONTRATADA** contratar atividades-meio acessórias (ex.: frete, seguro, logística), desde que:

I – tais contratações não caracterizem subcontratação do objeto nem delegação de atividades técnicas essenciais; e

II – permaneça a **CONTRATADA** integralmente responsável pela execução, qualidade, prazos, garantias e assistência técnica previstas no Contrato e no Termo de Referência.

5. Comunicar imediatamente à **CONTRATANTE**, formalmente, toda e qualquer anormalidade que dificulte ou impossibilite a execução do objeto deste contrato e prestar os esclarecimentos julgados necessários.

6. Aceitar todas as decisões, métodos de inspeção, verificação e controle, obrigando-se a fornecer todos os dados, elementos e explicações que a **CONTRATANTE** julgar necessário.

6.1 A ação de fiscalização não exonera a **CONTRATADA** de suas responsabilidades contratuais.

7. Manter contato e realizar o planejamento dos serviços com a **CONTRATANTE** de forma a executar quaisquer tarefas ou ajustes inerentes ao objeto contratado.

8. Acatar as observações feitas pela **FISCALIZAÇÃO** da **CONTRATANTE** quanto à execução dos serviços.

9. Atender prontamente quaisquer orientações e exigências da equipe de **FISCALIZAÇÃO** do contrato ou autoridade superior (art. 137, II, da Lei n.º 14.133/21, e prestar todo esclarecimento ou informação por eles solicitados, inerentes à execução do objeto contratual;

9.1 A **CONTRATADA** deverá responder por escrito, no prazo máximo de até 2 (dois) dias consecutivos, a quaisquer comunicações e/ou esclarecimentos requisitados pela **CONTRATANTE**, pertinentes à execução do contrato e que venham a ser solicitados pelo MPAM.

10. A **CONTRATADA** deverá responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com Código de Defesa do Consumidor, Lei nº 8.078/90, e às demais normas pertinentes.

11. Apresentar justificativa por escrito, devidamente comprovada, nos casos de ocorrência de fato superveniente, excepcional ou imprevisível, estranho à vontade das partes, e de impedimento de execução por fato ou ato de terceiro reconhecido pela **CONTRATANTE** em documento contemporâneo a sua ocorrência, quando não puder cumprir os prazos estipulados para a execução, total ou parcial, do objeto deste contrato.

11.1 Nos casos de eventual atraso na entrega do objeto, comunicar à **CONTRATANTE**, antes de expirar tal prazo, quaisquer problemas que impossibilitem o cumprimento do prazo previsto, com a devida comprovação.

12. Substituir, reparar, corrigir, remover, refazer ou reconstituir, às suas expensas, no todo ou em parte, no prazo fixado pela **FISCALIZAÇÃO**, os itens que não atendam às especificações exigidas e foram rejeitados, os que se verifiquem imperfeições, vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.

13. Responsabilizar-se por falhas na execução dos serviços que venham a se tornar aparentes em data posterior à sua entrega, ainda que tenha havido aceitação deles.

14. Responsabilizar-se pela garantia e assistência técnica *on-site* dos itens, caso o fabricante e/ou assistência técnica autorizada por este não puder fazê-lo ou se recusar.

15. Manter, durante toda a execução do contrato, todas as condições de habilitação e qualificação exigidas na respectiva licitação, em compatibilidade com as obrigações assumidas.

16. Responder pela idoneidade moral e técnica dos seus empregados, sendo única, integral e exclusivamente responsável, em qualquer caso, por todos os danos e prejuízos, de qualquer natureza, causados, direta ou indiretamente, à **CONTRATANTE** ou a terceiros, provenientes da execução dos serviços objeto deste contrato, quaisquer que tenham sido as medidas preventivas adotadas, respondendo por si e seus procuradores.

17. Responsabilizar-se por obter todas as franquias, licenças, aprovações e demais exigências de órgãos competentes, inclusive responsabilizando-se por todos os ônus decorrentes.

18. A inobservância das especificações constantes deste instrumento implicará a não aceitação parcial ou total dos serviços, devendo a **CONTRATADA** refazer as partes recusadas sem direito a indenização

19. Cumprir as normas de proteção ao trabalho, inclusive aquelas relativas à segurança e à saúde no trabalho;

20. Não submeter os trabalhadores a condições degradantes de trabalho, jornadas exaustivas, servidão por dívida ou trabalhos forçados;

21. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos de idade, exceto na condição de aprendiz para os maiores de quatorze anos de idade, observada a legislação pertinente;

22. Não submeter o menor de dezoito anos de idade:

22.1 à realização de trabalho noturno;

22.2 à realização de trabalho em condições perigosas e insalubres; nem

22.3 à realização de atividades constantes na Lista de Piores Formas de Trabalho Infantil, aprovada pelo Decreto Federal n.º 6.481, de 12 de junho de 2008;

23. Receber e dar o tratamento adequado a denúncias de discriminação, violência e assédio no ambiente de trabalho;

24. Rubricar o contrato ou seus aditivos no prazo de 5 (cinco) dias úteis, contados a partir da notificação enviada pela DCCON.

CLÁUSULA DÉCIMA SEGUNDA – DA MATRIZ DE ALOCAÇÃO DE RISCOS:

1. Disposições gerais.

1.1. Para os fins desta Cláusula entende-se por risco todo evento futuro, incerto e alheio à vontade das partes, capaz de gerar impacto relevante no prazo, no custo ou na qualidade da execução contratual.

1.2. A alocação de riscos observa o art. 22 da Lei n.º 14.133/2021, de modo a atribuir-lhes, sempre que possível, à parte que detenha melhor capacidade de gerenciá-los ou mitigá-los, assegurando o equilíbrio econômico-financeiro do ajuste.

1.3. Sempre que caracterizado caso fortuito ou força maior, devidamente comprovado, aplicar-se-ão as regras desta Matriz, sem prejuízo das demais disposições legais pertinentes.

2. Riscos atribuídos exclusivamente à CONTRATANTE:

Evento	**Abrangência / Limite**	**Medida de mitigação ou compensação**
2.1 Alterações unilaterais do objeto ou das quantidades (art. 124, inciso I, da Lei n.º 14.133/2021).	Até os limites legais	Reequilíbrio mediante reajuste de preço, de prazo ou ambos, a pedido do CONTRATADO, nos termos da Cláusula Vigésima Primeira.
2.2 Caso fortuito ou força maior **externo** à cadeia de suprimentos do CONTRATADO (greves gerais, calamidade natural que impeça recebimento / instalação).	—	Suspensão de prazos e, se for o caso, recomposição de custos diretos comprovados.
2.3 Atraso de pagamento por fato imputável à Administração.	> 30 (dias) após vencimento	Incidência de atualização financeira (art. 92, inciso V, da Lei n.º 14.133/2021) e possibilidade de paralisação justificada (art. 137, § 3.º, inciso II, da Lei n.º 14.133/2021).
2.4 Falhas de infraestrutura, logística interna ou compatibilidade de sistemas sob gestão do MPAM.	—	Ajuste de cronograma sem ônus ao CONTRATADO; despesas adicionais cobertas pelo CONTRATANTE.
2.5 Contingenciamento ou indisponibilidade orçamentária superveniente.	—	Aplicação dos arts. 137, § 3.º, inciso II, e 138, § 2.º, da Lei n.º 14.133/2021, com suspensão ou rescisão e pagamento de indenizações cabíveis.

3. Riscos atribuídos exclusivamente à CONTRATADA:

Evento	**Abrangência / Limite**	**Medida de mitigação ou compensação**

Evento	Abrangência / Limite	Medida de mitigação ou compensação
3.1 Execução inadequada, atraso ou descumprimento de prazos sem causa justificada.	—	Aplicação de penalidades contratuais (arts. 155 e 156 da Lei n.º 14.133/2021) e obrigação de corrigir/repactuar às suas expensas.
3.2 Falha de fornecimento de materiais, insumos ou mão de obra.	—	Substituição ou suplementação imediata, sem ônus à CONTRATANTE.
3.3 Não conformidade dos equipamentos às especificações ou às amostras aprovadas.	—	Rejeição, substituição e aplicação de multas previstas.
3.4 Ausência ou insuficiência da garantia técnica **on-site** prevista.	—	Multa específica e extensão proporcional do período de garantia.
3.5 Danos causados por transporte ou armazenagem sob responsabilidade do fornecedor.	—	Reparação integral e sem custo para a CONTRATANTE.

4. Riscos COMPARTILHADOS:

4.1 São considerados riscos compartilhados aqueles que, pela própria natureza, escapam do controle exclusivo de uma das partes e cuja ocorrência possa comprometer a equação econômico-financeira do contrato.

Evento	Critério de compartilhamento	Forma de compensação
4.1.1 Alterações legais, normativas ou tributárias não previstas na data da proposta que onerem ou desonerem o objeto.	Cada parte arca com o impacto em até **5%** (cinco por cento) do valor atualizado do contrato; excedente será objeto de reequilíbrio conforme Cláusula Vigésima Primeira.	Ajuste de preços ou de escopo, conforme art. 124 da Lei n.º 14.133/2021.
4.1.2 Oscilação inflacionária ou cambial extraordinária, com variação acumulada superior a **10 %** do IPCA.	Impacto até **10 %** suportado pela parte contratada; excedente sujeito a reequilíbrio.	Reajuste ou repactuação após comprovação documental.
4.1.3 Situações de emergência pública ou calamidade que exijam alteração de cronograma.	Prorrogação automática dos prazos equivalente ao período de paralisação.	Eventuais custos diretos adicionais divididos meio a meio, mediante apresentação de planilha analítica.
4.1.4 Oscilações severas de mercado em componentes de manutenção (variação > 15 % do índice ICEI-TI).	Excedente dividido em partes iguais, mediante laudo de mercado independente.	Repactuação de preços de manutenção.

4.2 A superveniência de novos riscos não contemplados será tratada pelos mesmos critérios de alocação (capacidade de controle e gestão), mediante aditivo específico ou termo de apostilamento, observado o procedimento da Cláusula Vigésima Primeira.

5. Revisões e atualização da Matriz:

5.1 Ocorrendo fatos supervenientes relevantes, a presente Matriz poderá ser revista por aditivo específico, preservados os princípios da legalidade, da eficiência e do equilíbrio econômico-financeiro.

CLÁUSULA DÉCIMA TERCEIRA – DA GARANTIA TÉCNICA:

Todos os equipamentos e softwares utilizados no fornecimento do objeto deverão estar cobertos por suporte, garantia e assistência técnica do fabricante, durante toda a vigência do contrato.

1. A garantia dos hardwares deverá ser na modalidade on-site no Datacenter da **CONTRATADA**.

2. A **CONTRATADA** é a única responsável pelos equipamentos e softwares disponibilizados na prestação dos serviços fornecidos à **CONTRATANTE**, mesmo que tenham sido adquiridos de terceiros.

3. A **CONTRATADA** responderá pela reparação dos danos causados por defeitos relativos ao serviço prestado, conforme descrição e exigências deste instrumento. Por isso, deve prezar pela qualidade e eficiência, garantindo que o serviço e as soluções definitivas fornecidas não causem problemas adicionais àqueles apresentados pela **CONTRATANTE**, quando do recebimento de alertas ou da abertura dos chamados de suporte técnico.

4. Serviços de Suporte Técnico e Manutenção

4.1 Os equipamentos deverão possuir garantia de 60 (sessenta) meses, com suporte 24x7 e prazo de envio de peças até o próximo dia útil após abertura do chamado.

4.2 A **CONTRATANTE** poderá acionar diretamente o suporte do fabricante, sem necessidade de autorização prévia da **CONTRATADA**. Não haverá limitação quanto à quantidade de chamados, seja para dúvidas, configurações ou problemas relacionados a hardware e software.

4.3 Chamados poderão ser abertos via telefone 0800, portal web ou e-mail.

4.4 O atendimento telefônico inicial deverá ser realizado em português.

4.5 A contratada deverá garantir acesso completo ao portal do fabricante, incluindo base de conhecimento, atualizações de software e documentação.

4.6 Durante a vigência do suporte, todas as atualizações de firmware e software deverão ser fornecidas sem ônus à **CONTRATANTE**.

4.7 A contratada deverá apresentar os códigos de serviço (SKU, part number) referentes à garantia do fabricante, com os equipamentos devidamente registrados em nome da contratante.

4.8 É de responsabilidade da contratada garantir a compatibilidade técnica entre todos os componentes da solução durante toda a vigência contratual.

CLÁUSULA DÉCIMA QUARTA – DA GARANTIA CONTRATUAL:

Nos termos dos arts. 96 a 102 da Lei n.º 14.133/2021, a **CONTRATADA** deverá apresentar garantia contratual, podendo optar pela caução em dinheiro ou em títulos da dívida pública, seguro-garantia, fiança bancária ou título de capitalização, em valor correspondente a **5% (cinco por cento)** do valor integral da contratação, correspondendo à quantia de R$ _____.

1. A partir da data em que for notificada pela **CONTRATANTE**, a **CONTRATADA** deverá encaminhar a garantia contratual no prazo de 10 (dez) dias úteis, prorrogável por igual período, a critério daquela.

2. A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:

2.1 prejuízos advindos do não cumprimento do objeto do contrato;

2.2 prejuízos diretos causados à **CONTRATANTE** decorrentes de culpa ou dolo da **CONTRATADA**.

2.3 multas moratórias e compensatórias aplicadas pela **CONTRATANTE**; e

2.4 obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela **CONTRATADA**, quando couber.

3. No caso de acréscimo no valor contratual, a **CONTRATADA** obriga-se a depositar junto à **CONTRATANTE**, na mesma modalidade, o valor referente à diferença da garantia. Mesma providência deverá ser tomada no caso de prorrogação do prazo contratual para adequar o vencimento da garantia ao do termo aditivo.

4. As garantias prestadas serão liberadas ou restituídas após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da **CONTRATANTE** e, quando em dinheiro, atualizada monetariamente, segundo dispõe o art. 100 da Lei n.º 14.133/2021.

5. Na hipótese de prestação da garantia na modalidade seguro-garantia, este terá por objetivo garantir o fiel cumprimento das obrigações assumidas pela **CONTRATADA** perante a **CONTRATANTE**, inclusive as multas, os prejuízos e as indenizações decorrentes de inadimplemento, observadas as seguintes regras:

5.1 O seguro-garantia garantia deverá ter validade durante a execução do contrato e estender-se-á por mais **3 (três) meses após o término da vigência contratual,** devendo acompanhar as modificações referentes ao ínterim deste mediante a emissão do respectivo endosso pela seguradora;

5.2 O seguro-garantia continuará em vigor mesmo se o contratado não tiver pago o prêmio nas datas convencionadas.

6. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item 3 desta cláusula.

7. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação da multa moratória prevista neste contrato.

8. Caso o prazo a que se refere o item 8 da tabela da Cláusula Vigésima seja exaurido, tal circunstância autoriza a Administração a promover a retenção dos pagamentos devidos à **CONTRATADA** e/ou a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os arts. 137, I, e 139, IV, ambos da Lei n.º 14.133/2021.

8.1 O bloqueio efetuado com base neste item não gera direito a nenhum tipo de compensação financeira à **CONTRATADA**.

8.2 A **CONTRATADA**, a qualquer tempo, poderá substituir o bloqueio efetuado por quaisquer das modalidades de garantia, caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária.

11. A **CONTRATADA** se compromete a repor ou a completar a garantia na hipótese de utilização parcial ou total, para o pagamento da multa contratual ou encargos trabalhistas e previdenciários, e ainda, na alteração do valor contratado, para manter o percentual inicial, **no prazo de até 10 (dez) dias úteis**, contados da assinatura do termo aditivo ou a partir da data em que for notificada pela **CONTRATANTE**, a partir do qual se observará o disposto nesta cláusula.

12. A garantia somente será liberada ante a comprovação de que a empresa pagou todos os encargos trabalhistas e previdenciárias decorrentes da contratação, bem como apresentação de toda a documentação solicitada no edital pela **CONTRATANTE**.

13. Será considerada extinta a garantia:

13.1 Com a devolução da apólice, acompanhada de declaração da **CONTRATANTE**, mediante termo circunstanciado, de que a **CONTRATADA** cumpriu todas as cláusulas do contrato;

13.2 No prazo de três meses após o término da vigência, caso a **CONTRATANTE** não comunique a ocorrência de sinistros.

14. A garantia não será extinta em caso de ocorrência de sinistro ou irregularidade, devidamente comunicado à seguradora pela **FISCALIZAÇÃO.**

CLÁUSULA DÉCIMA QUINTA – DO ACORDO DE NÍVEL DE SERVIÇO (SLA):

Os chamados de suporte técnico serão classificados conforme o nível de severidade, com base no impacto causado no ambiente computacional da **CONTRATANTE**, conforme as tabelas a seguir:

1. Impacto:

Nível	**Descrição do Impacto**
1	Serviços totalmente indisponíveis
2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos
3	Acesso aos aplicativos

2. Níveis de Severidade:

		Níveis de Severidade
Modalidade	**Prazo**	

		1	2	3
Remoto	Início do Atendimento	1 hora	4 horas	8 horas
	Solução do Contorno	8 horas	12 horas	24 horas

3. Quando for necessário atendimento presencial, a **CONTRATADA** deverá disponibilizar técnicos para resolver os problemas no local. Preferencialmente, essas atividades devem ser previamente acordadas entre as partes, exceto em casos de severidade máxima ou evidente indisponibilidade da infraestrutura da **CONTRATANTE**.

4. O início do atendimento será considerado a partir da abertura do chamado técnico.

5. O atendimento será considerado encerrado quando a solução estiver disponível e funcionando perfeitamente no local de instalação.

6. Durante toda a vigência do contrato, a **CONTRATANTE** poderá abrir chamados ilimitados para suporte técnico.

7. A **CONTRATADA** será integralmente responsável por quaisquer danos ou prejuízos causados ao patrimônio da **CONTRATANTE** ou de terceiros, decorrentes de ações ou omissões de seus colaboradores durante a execução dos serviços solicitados.

8. Qualquer atividade relacionada a configurações, ajustes ou parametrizações após a implantação deverá ser precedida da abertura de um chamado técnico.

9. Caso a atividade seja realizada de forma proativa, a **CONTRATADA** deverá comunicar à **CONTRATANTE**, via e-mail, justificando a execução antecipada.

10. Se alguma atividade exigir a interrupção da solução, a **CONTRATANTE** deverá ser imediatamente notificada para autorizar ou reagendar a execução.

11. Atualizações que impliquem indisponibilidade do ambiente devem ser previamente agendadas com a equipe técnica da **CONTRATANTE**.

12. A **CONTRATADA** deverá manter uma Central de Atendimento em português (Brasil), operando 24 horas por dia, 7 dias por semana, durante todo o ano (24x7x365), para abertura de chamados e demais comunicações.

13. A **CONTRATANTE** poderá solicitar serviços específicos por meio dos seguintes canais de comunicação:

a) E-mail;

b) Telefone 0800;

c) Sistema de Chamados Web.

14. O serviço será considerado concluído somente após a confirmação da área técnica da **CONTRATANTE** quanto à sua execução satisfatória.

15. O encerramento de solicitações técnicas dependerá da anuência de ambas as partes: **CONTRATADA** e **CONTRATANTE**.

16. A **CONTRATADA** manterá um cadastro com os nomes das pessoas indicadas pela **CONTRATANTE** autorizadas a abrir e encerrar chamados.

17. O prazo para encerramento do atendimento não poderá ultrapassar os limites estabelecidos para cada nível de criticidade.

18. Considera-se suporte técnico as atividades que requerem acompanhamento por parte de um técnico da **CONTRATANTE**.

19. Quando for necessário atendimento local, o cronograma de execução deverá ser acordado entre as partes.

20. A **CONTRATADA** deverá iniciar o atendimento conforme os prazos definidos para cada nível de criticidade.

21. A manutenção corretiva inclui os serviços necessários para restaurar o funcionamento adequado dos equipamentos, com fornecimento de peças conforme especificações do fabricante, em caso de falhas ou defeitos de hardware.

22. A **CONTRATADA** deverá realizar os serviços de manutenção com ferramentas próprias e técnicos especializados, devidamente identificados.

23. O suporte técnico compreende ações para restabelecer o funcionamento correto das soluções contratadas, incluindo configuração, habilitação, implementação, manutenção e colocação em produção de funcionalidades.

24. Caso seja necessária a atualização de firmware, a **CONTRATADA** deverá fornecer o pacote de software e realizar a atualização.

25. Considerando que a resolução de problemas de software pode envolver o desenvolvimento de patches, admite-se a adoção de soluções de contorno (workaround) até a implementação da solução definitiva.

26. O período para solução de ocorrências de software será contado entre a formalização e o encerramento efetivo da ocorrência, seja com solução definitiva ou provisória.

27. Para ocorrências de hardware não resolvidas dentro do prazo, a **CONTRATADA** deverá substituir o equipamento ou módulo defeituoso em até 72 (setenta e duas) horas úteis. Após a substituição, deverá ser entregue um documento com as descrições e números de série dos equipamentos substituídos e novos.

28. A substituição definitiva de hardware deverá ser feita com equipamento novo, original, recomendado pelo fabricante, com configuração igual ou superior à do substituído.

29. Durante a substituição, a **CONTRATADA** deverá entregar documento contendo a descrição e número de série do equipamento defeituoso e do novo equipamento.

30. O prazo para solução de ocorrências de hardware será contado entre a formalização e o encerramento efetivo da ocorrência. Quando houver substituição, o encerramento será considerado apenas após o novo equipamento entrar em operação.

31. Para cálculo do tempo de atendimento, serão desconsiderados os períodos em que a **CONTRATANTE** estiver responsável por ações necessárias à análise e solução da ocorrência.

32. Não haverá limitação quanto ao número de técnicos da **CONTRATANTE** autorizados a abrir chamados, desde que previamente registrados como pontos de contato.

33. Durante o período de garantia, a **CONTRATADA** deverá fornecer todas as atualizações de software (versões, releases, patches), firmware ou microcódigos dos hardwares cobertos pela manutenção, sem custo adicional.

CLÁUSULA DÉCIMA SEXTA – DO RECEBIMENTO E DOS PRAZOS DE ENTREGA:

1. Da Entrega

1.1 Do prazo

1.1.1 A **CONTRATADA** deverá em, **no máximo, 60 (sessenta) dias corridos**, contados a partir da assinatura do contrato, finalizar a entrega de todos os itens do objeto especificado, com funcionamento e funcionalidades da solução de Datacenter completamente operacionais, totalmente ativadas e disponíveis na estrutura da **CONTRATADA**, conforme descritas neste contrato.

1.1.2 O prazo para entrega do objeto especificado poderá ser prorrogado mediante apresentação pela **CONTRATADA**, antes do fim do prazo especificado, de solicitação formal e fundamentada, condicionado à aceitação pela **CONTRATANTE**, que decidirá pela prorrogação do prazo ou aplicação das penalidades previstas em contrato.

1.2 Das condições de fornecimento

1.2.1 A **CONTRATADA** será responsável pelo transporte dos produtos, desde o local de sua fabricação/embalagem, conforme o caso, até o local de entrega, na sede da PROCURADORIA GERAL DE JUSTIÇA, a qual ocorrerá em dias úteis, no horário das 14h às 17h, no seguinte endereço:

Av. Coronel Teixeira, nº 7.995, Nova Esperança II

CEP. 69037-473, Manaus-AM

1.2.2 A entrega dos produtos deverá ser previamente agendada com o SETOR DE PATRIMÔNIO E MATERIAL – SPAT pelo telefone (92) 3655-0767.

1.2.3 Os produtos deverão ser entregues em perfeitas condições, conforme a quantidade e especificações pactuadas, observando o Edital, a Proposta da **CONTRATADA** e este contrato devendo, também, ser acondicionado adequadamente, em seu invólucro original, que deverão ser entregues devidamente acompanhados da respectiva nota fiscal, na qual constarão os valores discriminados dos itens que integram o conjunto, assim como as indicações referentes a: marca, modelo, procedência e prazo de garantia ou validade.

1.2.4 Os produtos devem estar em plena fabricação, não sendo aceitos aqueles com avisos de end-of-sale, end-of-support ou end-of-life emitidos pelo fabricante.

2. Do recebimento provisório e definitivo

2.1 O recebimento dos produtos será conduzido por uma COMISSÃO especialmente designada para essa finalidade. Essa comissão será composta por, no mínimo, três servidores ou empregados públicos, em conformidade com o disposto no Art. 117, §1º e Art. 140, inciso II da Lei n.º 14.133/21, conforme estabelecido neste subitem.

2.2 O RECEBIMENTO PROVISÓRIO será realizado pelo SETOR DE PATRIMÔNIO E MATERIAL - SPAT no ato da entrega da totalidade dos produtos empenhados, devidamente acompanhados da nota fiscal. Constitui-se de uma inspeção quantitativa, para posterior verificação de sua conformidade com as especificações do Termo de Referência e do Contrato.

a) O RECEBIMENTO PROVISÓRIO não constitui aceitação do objeto.

2.3 O RECEBIMENTO DEFINITIVO será realizado por FISCAL TÉCNICO ou COMISSÃO especialmente designada, no prazo máximo de 30 (trinta) dias, a contar do recebimento provisório, para verificação da conformidade dos equipamentos com as condições, especificações e obrigações contratuais.

a) É condição para RECEBIMENTO DEFINITIVO o fornecimento do TERMO DE GARANTIA E ASSISTÊNCIA TÉCNICA, informando que os referidos produtos estão cobertos por garantia de fábrica, de acordo com as exigências constantes neste instrumento;

b) O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais;

c) Uma vez constatado o cumprimento das obrigações de fornecimento, o TERMO DE RECEBIMENTO DEFINITIVO será emitido, que consistirá na declaração formal de que os itens fornecidos atendem aos requisitos estabelecidos no contrato, comprovando o atendimento das exigências contratuais.

2.4 Para avaliação da adequação às exigências contratuais e qualidade, o FISCAL TÉCNICO ou COMISSÃO submeterá os equipamentos recebidos a testes de aceitação, para aferição da boa execução do objeto contratado, após o qual, emitirá um relatório completo dos testes efetuados, devidamente assinado. Os testes serão constituídos das seguintes fases:

a) Abertura das embalagens;

b) Comprovação de que o equipamento/solução atende às especificações mínimas exigidas ou superiores oferecidas;

c) Testes funcionais de configuração e desempenho dos produtos.

2.5 Os itens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste instrumento, seus Anexos e na proposta, sem prejuízo da aplicação das penalidades, cabendo à **CONTRATADA** o dever de substituir os itens que não estejam de acordo com as especificações, observando-se o disposto no Art. 140, §1º da Lei n.º 14.133/21.

2.6 O RECEBIMENTO PROVISÓRIO ou DEFINITIVO do objeto não exclui a responsabilidade civil a ele relativa, nem a ético-profissional, pela perfeita execução do objeto deste termo.

2.7 As não conformidades e desvios de qualidade observados serão descritos em relatório, e não serão recebidos definitivamente, devendo a pendência ser completamente sanada pela **CONTRATADA**, em no máximo 15 (quinze) dias consecutivos, contados da notificação da **CONTRATANTE**.

2.8 Se, a qualquer tempo, vier a ser constatado que o material fornecido o foi em desacordo com as especificações e, em decorrência desse fato, observar-se qualquer tipo de dano ao equipamento onde está sendo utilizado, o reparo do equipamento ou, se for o caso, a sua substituição, será de inteira responsabilidade da **CONTRATADA**, nos termos da lei pertinente.

CLÁUSULA DÉCIMA SÉTIMA – DAS CONDIÇÕES DE PAGAMENTO:

O pagamento devido à **CONTRATADA** será creditado em conta-corrente, por meio de ordem bancária, efetuado mediante apresentação de nota fiscal/fatura, que será atestada pela **FISCALIZAÇÃO** deste contrato.

1. O pagamento será realizado à **CONTRATADA** de forma integral e condicionado ao marco da emissão do Termo de Recebimento Definitivo do objeto, assinado por ambas as partes.

2. Nos termos do art. 139, caput, e do art. 140, ambos do Ato n.º 008/2024/PGJ, os prazos para a **CONTRATANTE** liquidar e pagar são de:

2.1 até 10 (dez) dias úteis para a liquidação da despesa, a contar do recebimento da nota fiscal ou do instrumento de cobrança equivalente pela **CONTRATANTE**;

2.2 até 10 (dez) dias úteis para o pagamento, contados da liquidação da desepesa.

3. O requerimento de pagamento deverá ser encaminhado aos endereços eletrônicos protocolo@mpam.mp.br e dtic@mpam.mp.br, acompanhado da respectiva nota fiscal/fatura dos produtos, emitidas em conformidade com o Protocolo ICMS 42/2009 (NF-e), deverá estar devidamente discriminada, em nome da **PROCURADORIA-GERAL DE JUSTIÇA**, CNPJ n.º 04.153.748/0001-85, e acompanhada da seguinte documentação:

3.1 Certidão Negativa de Débitos para com a Fazenda Federal, Estadual e Municipal do domicílio ou sede da empresa, ou outra equivalente, na forma da lei.

3.2 Certidão Negativa de Débitos à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS.

3.3 Certidão Negativa de Débitos trabalhistas.

3.4 Requerimento solicitando o pagamento, em duas vias, constando o número da Nota de Empenho e deste contrato.

3.5 Recibo em duas vias.

4. Nenhum pagamento será efetuado à **CONTRATADA** enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência.

4.1 Na hipótese de a **CONTRATADA** não ter executado completamente o objeto, ou tê-lo realizado de maneira insatisfatória, conforme relatório da **FISCALIZAÇÃO**, o pagamento será feito de maneira proprocional e apenas pelos serviços efetivamente prestados.

4.2 Em qualquer dos casos deste item, a **CONTRATANTE** poderá reter os pagamentos devidos à **CONTRATADA** até que as pendências sejam resolvidas.

5. Se, quando da efetivação do pagamento, os documentos comprobatórios de situação regular, apresentados em atendimento às exigências de habilitação, estiverem com a validade expirada, o pagamento ficará retido até a apresentação de novos documentos dentro do prazo de validade.

6. Qualquer atraso ocorrido na apresentação da nota fiscal/fatura, ou dos documentos exigidos como condição de pagamento por parte da **CONTRATADA**, importará em prorrogação automática do prazo de vencimento da obrigação da **CONTRATANTE,** não sendo devido à **CONTRATADA** o pagamento de multa e juros moratórios.

7. Nenhum pagamento isentará a **CONTRATADA** das responsabilidades atinentes ao produto, tampouco implicará a aprovação definitiva da entrega, total ou parcialmente.

8.Nos casos de eventuais atrasos de pagamento, desde que a **CONTRATADA** não tenha concorrido de alguma forma para tanto, fica convencionado que os encargos moratórios devidos pela **CONTRATANTE**, entre a data de vencimento e a do dia do efetivo pagamento da nota fiscal/fatura, a serem incluídos na fatura do mês seguinte ao da ocorrência, serão calculados por meio da aplicação da seguinte fórmula:

EM = I x N x VP, onde:

EM = encargos moratórios

N = número de dias entre a data prevista para o pagamento e a do efetivo pagamento

VP = valor da parcela em atraso

I = índice de compensação financeira = 0,00016438, assim apurado:

I = i ÷ 365 = (6÷100) ÷ 365 = 0,00016438

Onde i = taxa percentual anual no valor de 6%.

CLÁUSULA DÉCIMA OITAVA – DA DOTAÇÃO ORÇAMENTÁRIA:

As despesas oriundas deste contrato correrão à conta da seguinte dotação orçamentária:

Unidade Gestora: 003101 – Procuradoria Geral de Justiça; **Unidade Orçamentária:** 03101 – Procuradoria Geral de Justiça; **Programa de Trabalho**: 03.122.0001.2001.0001 – Administração da Unidade; **Fonte**: – ; **Natureza da Despesa:** – , tendo sido emitida pela **CONTRATANTE**, em _____, a Nota de Empenho n.º_____, no valor global de **R$ _____**.

CLÁUSULA DÉCIMA NONA – DAS SANÇÕES ADMINISTRATIVAS:

Nos termos dos art. 155 da Lei n.º 14.133/2021, a **CONTRATADA** será responsabilizada administrativamente na forma desta cláusula.

1. São condutas passíveis de sanção administrativa:

1.1 Dar causa à inexecução parcial do contrato;

1.2 Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

1.3 Dar causa à inexecução total do contrato;

1.4 Deixar de entregar a documentação exigida para o certame;

1.5 Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

1.6 Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

1.7 Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

1.8 Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

1.9 Fraudar a licitação ou praticar ato fraudulento na execução do contrato;

1.10 Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

1.11 Praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

1.12 Praticar ato lesivo previsto no art. 5º da Lei n.º 12.846/2013.

2. Pela inexecução total ou parcial do compromisso assumido, a **CONTRATANTE** poderá aplicar à **CONTRATADA** as seguintes sanções:

2.1 Advertência, que será aplicada exclusivamente à conduta descrita no subitem 1.1 desta cláusula, quando não se justificar imposição de penalidade mais grave;

2.2 Multas, que serão aplicadas por qualquer das infrações descritas no item 1 desta cláusula, nos percentuais estabelecidos na Cláusula Vigésima deste contrato;

2.3 Impedimento de licitar e contratar com a Administração Pública Direta e Indireta do **ESTADO DO AMAZONAS**, em decorrência das infrações previstas nos subitens 1.2, 1.3, 1.4, 1.5, 1.6 e 1.7 desta cláusula, pelo prazo máximo de 3 (três) anos, havendo possibilidade de reabilitação da **CONTRATADA** após o decurso de 1 (um) ano;

2.4 Declaração de inidoneidade para licitar ou contratar com toda a Administração Pública brasileira, em virtude das condutas descritas nos subitens 1.8, 1.9, 1.10, 1.11 e 1.12 desta cláusula, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a **CONTRATADA** ressarcir a **CONTRATANTE** pelos prejuízos resultantes e após decorrido o prazo de 3 (três) anos;

3. As sanções serão aplicadas pela **CONTRATANTE** em procedimento apuratório que assegure à **CONTRATADA** as garantias do contraditório e da ampla defesa, com os recursos a eles inerentes.

3.1 Compete à Comissão Permanente de Licitação (CPL) da **CONTRATANTE** instruir os procedimentos apuratórios de que trata este item.

4. Cabe ao (à) **SUBPROCURADOR(A)-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS** a aplicação das sançoes descritas nos subitens 2.1, 2.2 e 2.3 desta cláusula.

4.1 Da decisão do (a) **SUBPROCURADOR(A)-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS** cabe recurso dirigido a este, no prazo de 15 (quinze) dias úteis, contado da data da intimação.

4.2 Se o (a) **SUBPROCURADOR(A)-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS** não reconsiderar a decisão em 5 (cinco) dias úteis, encaminhar-la-á ao (à) **PROCURADOR(A)-GERAL DE JUSTIÇA.**

5. Compete ao (à) **PROCURADOR(A)-GERAL DE JUSTIÇA** a aplicação da sanção disposta no subitem 2.4 desta cláusula.

5.1 Da decisão do (a) **PROCURADOR(A)-GERAL DE JUSTIÇA** caberá apenas pedido de reconsideração, que deverá ser apresentado no prazo de 15 (quinze) dias úteis.

6. As penalidades serão obrigatoriamente registradas no Sistema de Cadastro Único de Fornecedores - SICAF.

7. A sanção do subitem 2.2 desta cláusula pode ser aplicada isolada ou conjuntamente com as dos subitens 2.1, 2.3 e 2.4.

8. A aplicação das penalidades previstas nesta cláusula não exclui nem atenua a obrigação de a **CONTRATADA** reparar integralmente os danos causados à **CONTRATANTE**.

CLÁUSULA VIGÉSIMA – DAS MULTAS:

As multas a que se refere o subitem 2.2 da Cláusula Décima Nona serão impostas nas seguintes hipóteses:

Item	Penalidade	Sanção	Limite
1	Atraso injustificado na entrega do objeto contratado, ou pelo não cumprimento dos prazos estabelecidos no Edital	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor total da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
2	Atraso injustificado na regularização pertinente quando da recusa do objeto fornecido, na fase de **RECEBIMENTO**.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor total da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
3	Recusa em substituir o produto defeituoso, que vier a ser rejeitado, ou que na execução dos serviços de garantia e assistência técnica, apontem a necessidade de troca;	Multa de mora diária de **1% (um por cento)** sobre o valor da Nota de Empenho	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
4	Deixar de utilizar peças, componentes ou insumos originais ou certificados pelo fabricante, novos e de primeiro uso.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho. Por ocorrência	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.

Item	Penalidade	Sanção	Limite
5	Atraso injustificado para efetiva recolocação do produto em seu pleno estado de funcionamento, conforme condições de GARANTIA E ASSISTÊNCIA TÉCNICA deste Termo.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
6	Deixar de fornecer equipamento backup nos casos em que não for possível recuperar os produtos dentro dos prazos de atendimento previstos.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
7	Atraso injustificado para a substituição de determinado item (equipamento, serviço, software, licença), no atendimento de chamado de garantia e assistência técnica.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 20º (vigésimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 21.º (vigésimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da CONTRATADA às sanções correlatas.
8	Atraso injustificado para a análise e correção dos itens (equipamento, serviço, software, licença), no atendimento de chamado de garantia e assistência técnica.	Multa de mora diária de **0,5% (cinco décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 10º (décimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 11.º (décimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
9	Atraso injustificado para o fornecimento do TERMO DE GARANTIA E ASSISTÊNCIA TÉCNICA.	Multa de mora diária de **0,3% (três décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 10º (décimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 11.º (décimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
10	Atraso injustificado na resposta aos pedidos de esclarecimentos de ordem técnica.	Multa de mora diária de **0,2% (dois décimos por cento)** sobre o valor da Nota de Empenho, por dia de atraso, até o 10º (décimo) dia consecutivo, contado a partir do 1.º (primeiro) dia imediatamente posterior ao término do respectivo prazo.	A partir do 11.º (décimo primeiro) dia, a **CONTRATADA** ficará sujeita à inexecução parcial ou total do objeto, sendo possível a rescisão unilateral do contrato pela Administração e a sujeição da **CONTRATADA** às sanções correlatas.
11	Deixar de cumprir qualquer outra obrigação não prevista neste contrato	Multa de mora diária de **1% (um por cento)** sobre o valor da Nota de Empenho	Limitada a sua aplicação até **15% (quinze por cento)**.
12	Quando, sem justificativa aceita pela **CONTRATANTE**, o vencedor não providenciar o devido cadastramento junto ao Sistema de Administração Financeira e Contabilidade – Cadastramento de Credores da SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ-AM, na forma prevista no Edital.	Multa de **2,5% (dois inteiros e cinco décimos por cento)** sobre o valor total da proposta.	Não se aplica.
13	Inexecução parcial do objeto contratado.	Multa de até **0,5% (cinco décimos por cento)** até **30% (trinta por cento)** sobre o valor da Nota de Empenho, sem prejuízo das demais sanções previstas.	Não se aplica.
14	Inexecução total do objeto.	Multa de até **5% (cinco por cento)** até **30% (trinta por cento**) sobre o valor total do contrato, sem prejuízo das demais sanções previstas.	Não se aplica.

1. Serão descontados dos pagamentos porventura devidos à **CONTRATADA** as importâncias alusivas a multas, ou efetuar sua cobrança mediante inscrição na dívida ativa do Estado, ou por qualquer outra forma prevista em lei.

2. Caso a **CONTRATANTE** determine, a multa deverá ser recolhida no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

3. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a **CONTRATANTE** poderá cobrar o valor remanescente judicialmente.

CLÁUSULA VIGÉSIMA PRIMEIRA – DO REAJUSTAMENTO DE PREÇOS:

Nos termos do art. 92, §§ 3º e 4°, I, da Lei n.º 14.133/2021, os preços inicialmente contratados poderão ser reajustados, por requerimento da **CONTRATADA**, desde que observado o interregno mínimo de 12 (doze) meses, de acordo com a variação do Índice de Custo da Tecnologia da Informação (ICTI), computado pelo Instituto de Pesquisa Econômica Aplicada (Ipea), ou outro que venha substituí-lo, na forma e periodicidade regulamentadas.

1. Caberá à **CONTRATADA** efetuar os cálculos relativos ao reajustamento OU repactuação e demais documentos comprobatórios, submetendo-os à apreciação da **FISCALIZAÇÃO**.

2. O interregno mínimo de 12 (doze) meses para o primeiro reajustamento será contado a partir da data do orçamento estimado pela **CONTRATANTE**, que corresponderá à da assinatura do Quadro-Resumo de Compras, ocorrida em _____.

3. Nos reajustes subsequentes ao primeiro, o interregno de 12 (doze) meses será contado a partir da data de início dos efeitos financeiros do último reajustamento ocorrido.

4. O prazo para a **FISCALIZAÇÃO** responder ao pedido de reajustamento será de 1 (um) mês, contado do recebimento do pedido.

5. Conforme o art. 136, I, da Lei n.º 14.133/2021, o reajustamento poderá ser efetuado por simples apostila, salvo se coincidir com a porrogação contratual, hipótese em que deverá ser formalizado por termo aditivo.

6. Caso a **CONTRATADA** não requeira tempestivamente o reajustamento e prorrogue o contrato sem pleiteá-lo, ocorrerá a preclusão do direito.

7. A **CONTRATANTE** poderá restabelecer o equilíbrio econômico-financeiro do ajuste em seu favor, visando à adequação dos preços contratuais, quando se verificar que houve redução dos preços dos serviços no mercado, observando-se o disposto no art. 124 da Lei n.º 14.133/2021.

8. A **FISCALIZAÇÃO** poderá solicitar à **CONTRATADA**, durante a vigência deste contrato, a revisão dos preços e dos percentuais de desconto contratados quando o contrato mostrar-se desvantajoso para a Administração.

9. Nos termos do art. 124, II, "d", da Lei n.º 14.133/2021, ainda que não decorrido o interregno mínimo de 1 (um) ano a que se refere o item 2 desta cláusula, a **CONTRATADA** poderá pleitear à **FISCALIZAÇÃO** o reequilíbrio econômico-financeiro inicial do contrato em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução do contrato tal como pactuado, respeitada, em qualquer caso, a repartição objetiva de risco estabelecida no contrato.

CLÁUSULA VIGÉSIMA SEGUNDA – DA ALTERAÇÃO DO CONTRATO:

Nos termos dos arts. 124 e seguintes da Lei n.º 14.133/2021, o presente contrato pode ser alterado pelas partes, mediante termo aditivo.

1. A **CONTRATADA** é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

2. As supressões e acréscimos resultantes de acordo celebrado entre a **CONTRATADA** e a **CONTRATANTE** poderão exceder os limites estipulados no item anterior.

3. Nos termos do art. 136 da Lei n.º 14.133/2021, registros que não caracterizam alteração do contrato poderão ser formalizados por simples apostila.

CLÁUSULA VIGÉSIMA TERCEIRA – DA EXTINÇÃO DO CONTRATO:

O contrato se extingue quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

1. A extinção do contrato por vencimento do prazo não exonerará a **CONTRATADA** de suas responsabilidades contratuais nem das sanções que porventura lhe forem aplicadas.

1.1 A extinção a que alude este item não prejudicará o andamento de procedimento apuratório em face da **CONTRATADA**.

2. O contrato pode ser extinto antes do prazo nele fixado, sem ônus para a **CONTRATANTE**, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

2.1 A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação do contratado pelo contratante nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia.

2.2 Caso a notificação da não continuidade do contrato de que trata este item ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

3. O contrato pode ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no art. 137 da Lei n.º 14.133/21, bem como consensualmente, assegurados o contraditório e a ampla defesa.

3.1 Nessas hipóteses, aplicam-se os arts. 138 e 139 da mesma Lei.

3.2 A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a rescisão se não restringir sua capacidade de concluir o contrato.

3.3 Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

4. O termo de rescisão, sempre que possível, será precedido de:

4.1 Indenizações e multas.

4.2 Relação dos pagamentos já efetuados e ainda devidos;

4.3 Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos.

5. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório, nos termos do art. 131, caput, da Lei n.º 14.133/2021.

CLÁUSULA VIGÉSIMA QUARTA – DA RESERVA DE CARGOS:

Nos termos do art. 92, XVII, da Lei n.º 14.133/2021, a **CONTRATADA**, durante toda a vigência contratual, cumprirá a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz.

CLÁUSULA VIGÉSIMA QUINTA – DA PUBLICAÇÃO:

O presente contrato será publicado no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei n.º 14.133, de 2021, e sob a forma de extrato, no Diário Oficial Eletrônico do Ministério Público do Estado do Amazonas, após a sua assinatura, correndo as despesas por conta da **CONTRATANTE**, nos termos do art. 88, §2º, XV, do Ato n.º 008/2024/PGJ.

1. O contrato em sua íntegra será publicado no sítio oficial do Ministério Público do Estado do Amazonas, por meio do Portal da Transparência, nos termos do art. 91, caput, da Lei n.º 14.133/2021, e do art. 5º, II, da Resolução n.º 86/2012, do Conselho Nacional do Ministério Público - CNMP.

CLÁUSULA VIGÉSIMA SEXTA – DAS NORMAS APLICÁVEIS:

A **CONTRATADA** declara conhecer todas as normas abaixo e concorda em sujeitar-se às estipulações, sistemas de penalidades e demais regras delas constantes, mesmo que não expressamente transcritas no presente instrumento:

1. Lei n.º 14.133/2021 – Licitações e Contratos;
2. Lei n.º 10.406/2002 – Código Civil Brasileiro;
3. Lei n.º 8.078/1990 – Código de Defesa do Consumidor;
4. Decreto Federal n.º 6.481/2008 – Lista de Piores Formas de Trabalho Infantil;
5. Resolução n.º 37/2009, do Conselho Nacional do Ministério Público – CNMP;
6. Instrução Normativa n.º 5/2017, do Ministério do Planejamento, Desenvolvimento e Gestão, de forma subsidiária;
7. Ato n.º 008/2024/PGJ – Procedimentos Administrativos de Contratação de Bens e Serviços no Âmbito do Ministério Público do Estado do Amazonas; e
8. Demais legislações correlatas, de forma suplementar, à luz das normas específicas vigentes.

CLÁUSULA VIGÉSIMA SÉTIMA – DAS DISPOSIÇÕES FINAIS E DOS CASOS OMISSOS:

A **CONTRATADA**, em cumprimento à Resolução n.º 37/2009 do Conselho Nacional do Ministério Público e ao art. 48, parágrafo único, da Lei n.º 14.133/2021, declara que não possui cônjuge, companheira ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do Ministério Público do Estado do Amazonas.

1. A **CONTRATADA** e seus representantes legais apresentaram neste ato os documentos comprobatórios de suas condições jurídico-pessoais indispensáveis à lavratura do presente, inclusive a Certificação de Regularidade dos órgãos fiscais previdenciários públicos, a que estiver vinculada.
2. Os casos omissos neste contrato serão resolvidos pela Administração Superior da **CONTRATANTE**, baseados na legislação vigente.

CLÁUSULA VIGÉSIMA OITAVA – DO FORO CONTRATUAL:

As questões decorrentes da execução deste instrumento, que não possam ser dirimidas administrativamente, serão processadas e julgadas na justiça estadual, no foro de Manaus/AM, com expressa renúncia da **CONTRATADA** a qualquer outro que tenha ou venha a ter, por mais privilegiado que seja.

E, por estarem de acordo, foi o presente termo de contrato, depois de lido e anuído, assinado digitalmente pelas partes e por duas testemunhas.

Manaus, data da última assinatura eletrônica das partes.

(assinado eletronicamente)
ANDRÉ VIRGÍLIO BELOTA SEFFAIR
Subprocurador-Geral de Justiça para Assuntos Administrativos
Ministério Público do Estado do Amazonas

(assinado eletronicamente)
_____
Representante Legal da Contratada
Empresa _____

Documento assinado eletronicamente por **Adenilson Roberto de Oliveira Filho**, **Chefe da Divisão de Contratos e Convênios - DCCON**, em 17/12/2025, às 13:46, conforme art. 1°, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2033432** e o código CRC **257337B8**.

ANEXO III - DO EDITAL

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS

Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MODELO DE DECLARAÇÕES COMPLEMENTARES

Declaro, sob as penas da Lei, para os devidos fins junto à Comissão Permanente deLicitação que:

a) Cumpro plenamente os requisitos de habilitação, ciente de que respondo pela veracidade das informações prestadas, na forma da lei;

b) Em atenção item 5.6. e art. 14.º e seus incisos da Lei n.º 14.133/2021, não estou impedido de participar direta ou indiretamente desta licitação, e ainda, não possuo sócios, diretores ou gerentes, que sejam cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do Ministério Público do Estado do Amazonas e de sua CPL;

c) Recebi o edital e todos os documentos que o integram, dispondo de todos os elementos e informações necessários à elaboração da proposta de preços com total e completo conhecimento do objeto da licitação;

d) Os documentos e declarações apresentados são fiéis e verdadeiros;

e) Caso seja vencedor do certame e não cadastrado no SISTEMA DE ADMINISTRAÇÃO FINANCEIRA E CONTABILIDADE da SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ-AM, encaminharei à CONTRATANTE os documentos necessários para efetuar o referido cadastramento no prazo de 05 (cinco) dias úteis, a contar da adjudicação, sob pena de perder o direito de preferência à contratação em favor dos demais licitantes subsequentes, sem prejuízo da possibilidade de responder a procedimento administrativo de responsabilização por eventual retardamento da licitação;

f) O preço inclui além do lucro, todos os custos e despesas, com tributos incidentes e encargos devidos, materiais, serviços, transporte, a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas, bem como quaisquer outras despesas diretas e indiretas incidentes na prestação de serviços;

g) Apresentarei, quando da contratação, documento que indique o pessoal técnico operacional, das instalações e do aparelhamento adequado e disponíveis para a realização do objeto da licitação, bem como a qualificação de cada membro da equipe técnica que se responsabilizará pelos trabalhos;

h) Submeto-me e concordo integralmente com os termos do presente Edital, bem como com seus elementos e especificações, comprometendo-me a cumpri-los fielmente, inclusive no que se refere à fiscalização e ao controle técnico a serem exercidos por profissional expressamente designado para tal finalidade; e

i) A proposta apresentada para participar do presente Pregão foi elaborada de maneira independente por esta licitante e o seu conteúdo não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer outro participante potencial ou de fato, por qualquer meio ou por qualquer pessoa.

Local e data:

(assinatura)
(nome do representante legal pela empresa)
(CPF do representante legal)

ANEXO IV - DO EDITAL

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS

Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MODELO DE PROPOSTA DE PREÇOS

Proposta que faz a empresa _____, inscrita no CNPJ (MF) n.º _____, localizada _____, na cidade de _____, CEP _____, fone _____, e-mail _____, para o fornecimento dos bens abaixo relacionados, de acordo com todas as especificações e condições estabelecidas no **Pregão Eletrônico n.º 94.0XX/202X-CPL/MP/PGJ-SRP**, promovido pelo **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS / PROCURADORIA-GERAL DE JUSTIÇA**:

Item	Descrição	Marca / Modelo / Tipo / Referência	Qtd. (A)	Valor Unitário R$ (B)	Valor Total R$ (C=A*B)
01	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9	NUTANIX	4		
02	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU	NUTANIX	1		
03	SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX	NUTANIX	5		
04	SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU	NUTANIX	1		
05	LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE	NUTANIX	50		
...	...	...			
VALOR TOTAL DA PROPOSTA					**R$**

A _____(*nome da empresa)*_____ declara que concorda com todas as especificações do Edital.

a. **Prazo de validade da proposta: _____** (não será inferior a 90 (noventa) dias, a contar da data de sua apresentação).

b. **Prazo de entrega da solução: _____** (até 60 (sesenta) dias corridos, conforme dipõe o Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562;

c. **Modo de Transporte dos Produtos:**

( ) rodoviário/terrestre

( ) aéreo: ( ) normal ( ) expresso

( ) outros. Especificar:_____

d. **Prazo de garantia e assistência técnica**: _____ (mínimo 60 (sessenta) meses, conforme dipõe o Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562;

e. ***Site* e/ou e-mail do fabricante, se houver**: _____

f. **Dados Bancários**: (*indicar o nome e número do banco, nome e número completo da agência e número da conta corrente*);

g. **Contato para fins de faturamento:** *(indicar o nome, cargo, endereço, telefone, e-mail de contato do responsável pelo recebimento das futuras notas de empenho);*

h. **Contato para fins de faturamento:** *(indicar o nome, cargo, endereço, telefone, e-mail de contato do responsável pelo recebimento das futuras notas de empenho)*

Nome: _____

CNPJ ou CPF: _____

DECLARAÇÕES:

Declaro, sob as penas da Lei, para os devidos fins junto à Comissão Permanente de Licitação que:

a) Cumpro plenamente os requisitos de habilitação, ciente de que respondo pela veracidade das informações prestadas, na forma da lei;

b) Em atenção item 5.6. e art. 14.º e seus incisos da Lei n.º 14.133/2021, não estou impedido de participar direta ou indiretamente desta licitação, e ainda, não possuo sócios, diretores ou gerentes, que sejam cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do Ministério Público do Estado do Amazonas e de sua CPL;

c) Recebi o edital e todos os documentos que o integram, dispondo de todos os elementos e informações necessários à elaboração da proposta de preços com total e completo conhecimento do objeto da licitação;

d) Os documentos e declarações apresentados são fiéis e verdadeiros;

e) Caso seja vencedor do certame e não cadastrado no SISTEMA DE ADMINISTRAÇÃO FINANCEIRA E CONTABILIDADE da SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ-AM, encaminharei à CONTRATANTE os documentos necessários para efetuar o referido cadastramento no prazo de 05 (cinco) dias úteis, a contar da adjudicação, sob pena de perder o direito de preferência à contratação em favor dos demais licitantes subsequentes, sem prejuízo da possibilidade de responder a procedimento administrativo de responsabilização por eventual retardamento da licitação;

f) O preço inclui além do lucro, todos os custos e despesas, com tributos incidentes e encargos devidos, materiais, serviços, transporte, a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas, bem como quaisquer outras despesas diretas e indiretas incidentes na prestação de serviços;

g) Apresentarei, quando da contratação, documento que indique o pessoal técnico operacional, das instalações e do aparelhamento adequado e disponíveis para a realização do objeto da licitação, bem como a qualificação de cada membro da equipe técnica que se responsabilizará pelos trabalhos;

h) Submeto-me e concordo integralmente com os termos do presente Edital, bem como com seus elementos e especificações, comprometendo-me a cumpri-los fielmente, inclusive no que se refere à fiscalização e ao controle técnico a serem exercidos por profissional expressamente designado para tal finalidade; e

i) A proposta apresentada para participar do presente Pregão foi elaborada de maneira independente por esta licitante e o seu conteúdo não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer outro participante potencial ou de fato, por qualquer meio ou por qualquer pessoa.

Local e data:

(assinatura)
(nome do representante legal pela empresa)
(CPF do representante legal)

Observação: A apresentação da proposta implicará a plena aceitação, por parte do licitante, das condições estabelecidas neste edital e seus anexos, bem como, todas as especificações do objeto contidas na proposta vinculam a Contratada.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS

Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MODELO DE SOLICITAÇÃO DE CADASTRAMENTO – SEFAZ/AM

À DIRETORIA DE ORÇAMENTO E FINANÇAS

Procuradoria-Geral de Justiça do Estado do Amazonas
Avenida Coronel Teixeira, 7995, Nova Esperança
CEP: 69037-473 – Manaus / AM

A empresa (informar a razão social, CNPJ e endereço) solicita a esse Setor o seu cadastro no SISTEMA DE ADMINISTRAÇÃO FINANCEIRA E CONTABILIDADE, dessa S ECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ.

Assim sendo, acompanha esta carta de solicitação de cadastramento a documentação abaixo listada, exigida para a efetivação do registro:

a) Comprovante de inscrição e de situação cadastral emitido pela Receita Federal do Brasil;

b) Cópia legível do comprovante (por ex: extrato, cópia reprográfica de cartão bancário, etc.) dos seguintes dados bancários:

Banco: _____
Agência: _____
Conta: _____

Local e data:

(assinatura)
(nome do representante legal pela empresa)
(CPF do representante legal)

ANEXO VI - DO EDITAL

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS

Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MODELO - CREDENCIAMENTO PARA VISTORIA TÉCNICA

Pelo presente instrumento credenciamos o(a) Sr.(a) ....., portador do documento de Identidade n.º ....., o(a) qual está habilitado a proceder à vistoria técnica e assinar o Atestado de Vistoria em nome da empresa ..... CNPJ ..... prevista no ITEM 3.1 do Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562, referente ao procedimento licitatório PE 94.0XX/2026.

Local e data:

(assinatura)
(nome do representante legal pela empresa)
(CPF do representante legal)

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS

Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MODELO - ATESTADO DE VISTORIA TÉCNICA

Atestamos, para cumprimento do item 5.12 do Edital referente ao procedimento licitatório PE 94.0XX/2026, que a empresa ....., inscrita no CNPJ ....., representada neste ato por seu representante credenciado, o(a) Sr.(a) ....., portador(a) do documento de identidade profissional nº ....., compareceu ao local onde será executado o serviço/solução, conforme previsto no Item 3.1. do Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562 e, acompanhado por representante deste Ministério Público do Estado do Amazonas / Procuradoria-Geral de Justiça, tomou conhecimento *in loco* dos locais e instalações, tendo pleno conhecimento das especificações e condições locais para cumprimento das obrigações decorrentes do objeto da licitação em questão.

Manaus, AM, de de 202X.

Representante(a) designado(a) pela empresa licitante

De acordo

Representante da PGJ-AM

ANEXO VIII - DO EDITAL

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS

Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

MODELO DE DE DISPENSA DE VISTORIA TÉCNICA

Declaro(amos), para cumprimento do Item 5.12 do Edital referente ao procedimento licitatório ....., que a empresa ....., representada pelo, o(a) Sr.(a) ....., portador(a) do documento de identidade nº ....., optou por não vistoriar o local dos serviços conforme previsto no Subitem 3.1. do Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562.

Declaro, ainda, que quaisquer alegações de desconhecimento ou erro orçamentário por parte da futura contratada, para a execução dos serviços propostos não serão considerados nem usados como possível juízo de valor afim de compensações futuras.

Local e data:

(assinatura)
(nome do representante legal pela empresa)
(CPF do representante legal)

Documento assinado eletronicamente por **Sarah Madalena Barbosa Santos Cortes**, **Presidente da Comissão Permanente de Licitação - CPL**, em 30/12/2025, às 12:38, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2037917** e o código CRC **36215EC8**.

Licitação
Dispensa/Inexigibilidade
Pedido de Cotação Eletrônica

Ambiente: PRODUÇÃO

Disponibilizar Aviso de Licitação apenas para Divulgação

30/12/2025 15:58:55

Este Aviso de Licitação será Divulgado no Portal Nacional de Contratações Públicas - PNCP e no gov.br/compras (www.gov.br/compras) na data de 05/01/2026.

Resumo do Aviso de Licitação

Órgão: 85562 - PROCURADORIA GERAL DE JUSTIÇA DO ESTADO DO AM

UASG Responsável: 925849 - PROCURADORIA GERAL DE JUSTIÇA - AM

Modalidade de Licitação: Pregão

Nº da Licitação: 94001/2026

Característica: Tradicional

Forma de Realização: Eletrônico

Modo de Disputa: Aberto

Lei: Lei nº 14.133/2021

Critério de Julgamento: Menor Preço/Maior Desconto

Tipo de Objeto: Bens Comuns

Nº do Processo: 2025.007562

Quantidade de Itens: 9

Objeto:

Contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses.

Data da Divulgação: 05/01/2026

Data da Disponibilidade do Edital: A partir de 05/01/2026 às 08:00

Data/Hora da Abertura da Licitação: Em 19/01/2026 às 10:00

Disponibilizar apenas para Divulgação

Aviso de Licitação

Solução SERPRO

85562 - PROCURADORIA GERAL DE JUSTIÇA DO ESTADO DO AM
925849 - PROCURADORIA GERAL DE JUSTIÇA - AM

RELAÇÃO DE ITENS - PREGÃO ELETRÔNICO Nº 94001/2026-000

1 - Itens da Licitação

1 - Outros Serviços de Gerenciamento de Infraestrutura De Tecnologia da Informação e Comunicação (TIC)

Descrição Detalhada: EQUIPAMENTO HIPERCONVERGENTE –PLATAFORMA NUTANIX G9.

A descrição completa do Item 1 deve ser verificada no Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Tratamento Diferenciado: Não

Aplicabilidade Decreto 7174/2010: Não

Quantidade Total: 4

Critério de Julgamento: Menor Preço **Critério de Valor:** Valor Estimado

Unidade de Fornecimento: UNIDADE

Intervalo Mínimo entre Lances (R$): 10,00

Local de Entrega (Quantidade): Manaus/AM (4)

Grupo: G1

2 - Outros Serviços de Gerenciamento de Infraestrutura De Tecnologia da Informação e Comunicação (TIC)

Descrição Detalhada: EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU.

A descrição completa do Item 2 deve ser verificada no Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Tratamento Diferenciado: Não

Aplicabilidade Decreto 7174/2010: Não

Quantidade Total: 1

Critério de Julgamento: Menor Preço **Critério de Valor:** Valor Estimado

Unidade de Fornecimento: UNIDADE

Intervalo Mínimo entre Lances (R$): 10,00

Local de Entrega (Quantidade): Manaus/AM (1)

Grupo: G1

3 - Serviços de Gerenciamento de Sistemas Computacionais

Descrição Detalhada: SOFTWARE GESTÃO DAPLATAFORMA DE HIPERCONVERGENCIA NUTANIX.

A descrição completa do Item 3 deve ser verificada no Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Tratamento Diferenciado: Não

Aplicabilidade Decreto 7174/2010: Não

Quantidade Total: 5

Critério de Julgamento: Menor Preço **Critério de Valor:** Valor Estimado

Unidade de Fornecimento: UND SERVIÇO TÉCNICO

Intervalo Mínimo entre Lances (R$): 10,00

Local de Entrega (Quantidade): Manaus/AM (5)

Grupo: G1

Publicação Aviso PNCP e Relação de Itens (2038139) SEI 2025.007562 / pg. 354

4 - Serviços de Gerenciamento de Sistemas Computacionais

Descrição Detalhada: SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU.

A descrição completa do Item 4 deve ser verificada no Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Tratamento Diferenciado: Não

Aplicabilidade Decreto 7174/2010: Não

Quantidade Total: 1

Critério de Julgamento: Menor Preço **Critério de Valor:** Valor Estimado

Unidade de Fornecimento: UND SERVIÇO TÉCNICO

Intervalo Mínimo entre Lances (R$): 10,00

Local de Entrega (Quantidade): Manaus/AM (1)

Grupo: G1

5 - Serviços de Gerenciamento de Sistemas Computacionais

Descrição Detalhada: LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE.

A descrição completa do Item 5 deve ser verificada no Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Tratamento Diferenciado: Não

Aplicabilidade Decreto 7174/2010: Não

Quantidade Total: 50

Critério de Julgamento: Menor Preço **Critério de Valor:** Valor Estimado

Unidade de Fornecimento: UND SERVIÇO TÉCNICO

Intervalo Mínimo entre Lances (R$): 10,00

Local de Entrega (Quantidade): Manaus/AM (50)

Grupo: G1

6 - Serviços de Gerenciamento de Sistemas Computacionais

Descrição Detalhada: SOFTWARE DE BACKUP DE DADOS.

A descrição completa do Item 6 deve ser verificada no Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Tratamento Diferenciado: Não

Aplicabilidade Decreto 7174/2010: Não

Quantidade Total: 1

Critério de Julgamento: Menor Preço **Critério de Valor:** Valor Estimado

Unidade de Fornecimento: UND SERVIÇO TÉCNICO

Intervalo Mínimo entre Lances (R$): 10,00

Local de Entrega (Quantidade): Manaus/AM (1)

Grupo: G1

7 - Outros Serviços de Gerenciamento de Infraestrutura De Tecnologia da Informação e Comunicação (TIC)

Descrição Detalhada: EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES.

A descrição completa do Item 7 deve ser verificada no Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Tratamento Diferenciado: Não

Aplicabilidade Decreto 7174/2010: Não

Quantidade Total: 1

Critério de Julgamento: Menor Preço **Critério de Valor:** Valor Estimado

Unidade de Fornecimento: UNIDADE

Intervalo Mínimo entre Lances (R$): 10,00

Local de Entrega (Quantidade): Manaus/AM (1)

Grupo: G1

8 - Serviços de Gerenciamento de Sistemas Computacionais

Descrição Detalhada: SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES.

A descrição completa do Item 8 deve ser verificada no Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Tratamento Diferenciado: Não

Aplicabilidade Decreto 7174/2010: Não

Quantidade Total: 1

Critério de Julgamento: Menor Preço **Critério de Valor:** Valor Estimado

Unidade de Fornecimento: UND SERVIÇO TÉCNICO

Intervalo Mínimo entre Lances (R$): 10,00

Local de Entrega (Quantidade): Manaus/AM (1)

Grupo: G1

9 - Switch

Descrição Detalhada: Switch Quantidade Portas: 48UN, Tipo Portas: Sfp28, Velocidade Porta: 25 Gb, Alimentação: 110/220V, Características Adicionais: 50 Cm De Cabo De Empilhamento, Tipo: Padrão Rack 19"

Tratamento Diferenciado: Não

Aplicabilidade Decreto 7174/2010: Não

Quantidade Total: 2

Critério de Julgamento: Menor Preço **Critério de Valor:** Valor Estimado

Unidade de Fornecimento: Unidade

Intervalo Mínimo entre Lances (R$): 10,00

Local de Entrega (Quantidade): Manaus/AM (2)

Grupo: G1

2 - Composição dos Grupos

Grupo 1			
Nº do Item	Descrição	Quantidade Total	Unidade de Fornecimento
1	Outros Serviços de Gerenciamento de Infraestrutura De Tecnologia da Informação e Comunicação (TIC)	4	UNIDADE
2	Outros Serviços de Gerenciamento de Infraestrutura De Tecnologia da Informação e Comunicação (TIC)	1	UNIDADE
3	Serviços de Gerenciamento de Sistemas Computacionais	5	UND SERVIÇO TÉCNICO
4	Serviços de Gerenciamento de Sistemas Computacionais	1	UND SERVIÇO TÉCNICO
5	Serviços de Gerenciamento de Sistemas Computacionais	50	UND SERVIÇO TÉCNICO
6	Serviços de Gerenciamento de Sistemas Computacionais	1	UND SERVIÇO TÉCNICO
7	Outros Serviços de Gerenciamento de Infraestrutura De Tecnologia da Informação e Comunicação (TIC)	1	UNIDADE
8	Serviços de Gerenciamento de Sistemas Computacionais	1	UND SERVIÇO TÉCNICO
9	Switch	2	Unidade

Publicação Aviso PNCP e Relação de Itens (2038139) SEI 2025.007562 / pg. 356

26, caput, da Resolução n.º 006/2015-CSMP/AM, encontra-se esgotado;

CONSIDERANDO que a complexidade da apuração se elevou, demandando diligências mais aprofundadas para a localização da pessoa jurídica e a identificação de seus sócios-administradores, o que se amolda à natureza e ao prazo mais elástico do Inquérito Civil, nos termos do art. 37 da Resolução n.º 006/2015-CSMP/AM;

CONSIDERANDO, por fim, que o art. 26, § 2º, da Resolução n.º 006/2015-CSMP/AM determina que, vencido o prazo do Procedimento Preparatório, o membro do Ministério Público deverá arquivá-lo, ajuizar a ação cabível ou convertê-lo em Inquérito Civil;

RESOLVE:

I – CONVERTER o Procedimento Preparatório n.º 243.2024.000002 em INQUÉRITO CIVIL, com o objetivo de apurar suposta prática de violação a direitos das pessoas idosas por parte da empresa LACET NAVEGAÇÃO FLUVIAL LTDA., inscrita no CNPJ sob o n.º 00.754.870/0001-56, consistente no desrespeito à gratuidade e/ou ao desconto em passagens de transporte fluvial intermunicipal, e identificar os responsáveis pela conduta;

II - DETERMINAR as seguintes providências:

1 - Proceda-se à reautuação do feito como Inquérito Civil, com as devidas anotações e registros nos sistemas de controle, e publique-se a presente portaria no Diário Oficial Eletrônico do Ministério Público do Estado do Amazonas, conforme art. 31, V, da Resolução n.º 006/2015-CSMP/AM;

2. Nomeio a servidora Onilvania Ferreira Assunção para atuar como secretária administrativa no feito;

3. Reiterem-se as diligências já determinadas no despacho de fls. 25-27, notadamente a expedição de ofício à Junta Comercial do Estado do Amazonas – JUCEA para que, no prazo de 15 (quinze) dias, encaminhe a esta Promotoria de Justiça a ficha cadastral completa e atualizada da empresa investigada, contendo o endereço da sede, de eventuais filiais, e a qualificação completa (nome, CPF e endereço residencial) de seus sócios-administradores, admoestando-se acerca do teor do art. 10 da Lei da Ação Civil Pública, que pune a desídia dolosa em fornecer informação essencial ao andamento de investigação com o condão de repercutir na oferta de Ação Civil Pública;
4. Após a juntada das informações, expeça-se nova notificação à empresa e, se necessário, aos seus sócios-administradores, para que prestem os esclarecimentos devidos.

Cumpra-se.

Coari/AM, data da assinatura eletrônica.

Yury Dutra da Silva
Promotor de Justiça

COMISSÃO PERMANENTE DE LICITAÇÃO

AVISO DE LICITAÇÃO

PREGÃO ELETRÔNICO N.º 94.001/2026-CPL/MP/PGJ
PROCESSO SEI N.º 2025.007562

OBJETO: Contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses.

REGIME JURÍDICO: Lei Federal n.º 14.133 de 2021.

ABERTURA: 19/01/2026 às 10h. (horário de Brasília)

ENTREGA DAS PROPOSTAS: a partir de 05/01/2026

LOCAL: no site https://www.gov.br/compras/pt-br

UASG: 925849 – PROCURADORIA GERAL DE JUSTIÇA AM.

Informações adicionais, dúvidas e pedidos de esclarecimentos deverão ser dirigidos à COMISSÃO PERMANENTE DE LICITAÇÃO pelo telefone (92) 3655-0743 ou pelo e-mail licitacao@mpam.mp.br.

Manaus, 30 de dezembro de 2025.

Sarah Madalena Barbosa Côrtes de Melo
Presidente da Comissão Permanente de Licitação
Ato PGJ n.º 165/2025 - DOMPE, Ed. 3121, de 15.07.2025

ATOS DA DIVISÃO DE RECURSOS HUMANOS

PORTARIA Nº 522/2025/DRH/DRH ESTAGIO

O CHEFE DA DIVISÃO DE RECURSOS HUMANOS, no uso de suas atribuições, e

CONSIDERANDO o teor do Procedimento Administrativo SEI 2025.024274;

RESOLVE:

DESIGNAR o(a) estagiário(a) de Nível Médio MARIA ELOISA RUIZ BRASILINO, para exercer suas atribuições junto à(o) 01ª Promotoria de Justiça da Comarca de Manacapuru, a contar de 07/01/2026, no horário de 08:00 às 12:00 horas.

Publique-se, registre-se, cumpra-se.

Manaus (Am.), 23 de dezembro de 2025

JHERALMY HASTEM SANTOS ARAÚJO DA SILVA
Chefe da Divisão de Recursos Humanos

PORTARIA Nº 523/2025/DRH/DRH ESTAGIO

O CHEFE DA DIVISÃO DE RECURSOS HUMANOS, no uso de suas atribuições, e

CONSIDERANDO o teor do Procedimento Administrativo SEI 2025.024274;

RESOLVE:

DESIGNAR o(a) estagiário(a) de Nível Médio LARAH MACIEL DE OLIVEIRA, para exercer suas atribuições junto à(o) 02ª Promotoria de Justiça da Comarca de Manacapuru, a contar de 07/01/2026, no horário de 08:00 às 12:00 horas.

Publique-se, registre-se, cumpra-se.

Manaus (Am.), 23 de dezembro de 2025

PROCURADORIA-GERAL DE JUSTIÇA

Procuradora-Geral de Justiça:
Leda Mara Nascimento Albuquerque
Subprocuradora-Geral de Justiça para Assuntos Jurídicos e Institucionais:
Anabel Vitória Pereira Mendonça de Souza
Subprocurador-Geral de Justiça para Assuntos Administrativos:
André Virgílio Belota Seffair
Corregedora-Geral do Ministério Público:
Silvana Nobre de Lima Cabral
Secretária-Geral do Ministério Público:
Wandete de Oliveira Netto

PROCURADORES DE JUSTIÇA

Câmaras Cíveis
Elvys de Paula Freitas
Sandra Cal Oliveira
Jussara Maria Pordeus e Silva
Mara Nóbia Albuquerque da Cunha
Suzete Maria dos Santos
Nilda Silva de Sousa
Delisa Olívia Vieiralves Ferreira
Jorge Michel Ayres Martins
Anabel Vitória Pereira Mendonça de Souza
Marco Aurélio Lisciotto

Câmaras Criminais
Carlos Lélio Lauria Ferreira
Marlene Franco da Silva
Mauro Roberto Veras Bezerra
Sarah Pirangy de Souza
Aguinelo Balbi Júnior
Liani Mônica Guedes de Freitas Rodrigues
Adelton Albuquerque Matos

Câmaras Reunidas
Karla Fregapani Leite
Públio Caio Bessa Cyrino
Sílvia Abdala Tuma
José Bernardo Ferreira Júnior
Neyde Regina Demósthenes Trindade
Silvana Nobre de Lima Cabral

CONSELHO SUPERIOR

Leda Mara Nascimento Albuquerque (Presidente)
Silvana Nobre de Lima Cabral
Mara Nóbia Albuquerque da Cunha
Adelton Albuquerque Matos
Elvys de Paula Freitas
Jorge Michel Ayres Martins
Nilda Silva de Sousa

OUVIDORIA
Sílvia Abdala Tuma

Ministério Público do Estado do Amazonas
Procuradoria-Geral de Justiça

AVISO DE LICITAÇÃO

PREGÃO ELETRÔNICO N.º 94.001/2026-CPL/MP/PGJ

PROCESSO SEI N.º 2025.007562

OBJETO: Contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma **solução de datacenter**, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, **com garantia de 60 (sessenta) meses.**

REGIME JURÍDICO: Lei Federal n.º 14.133 de 2021.

ABERTURA: 19/01/2026 às 10h. (horário de Brasília)

ENTREGA DAS PROPOSTAS: a partir de **05/01/2026**

LOCAL: no site https://www.gov.br/compras/pt-br

UASG: 925849 – PROCURADORIA GERAL DE JUSTIÇA AM.

Informações adicionais, dúvidas e pedidos de esclarecimentos deverão ser dirigidos à COMISSÃO PERMANENTE DE LICITAÇÃO pelo telefone **(92) 3655-0743 ou pelo e-mail licitacao@mpam.mp.br.**

Manaus, 30 de dezembro de 2025.

Sarah Madalena Barbosa Côrtes de Melo
Presidente da Comissão Permanente de Licitação
Ato PGJ n.º 165/2025 - DOMPE, Ed. 3121, de 15.07.2025

Jornal do Commercio

JORNALISMO QUE INFORMA E TRANSFORMA.

WWW.JCAM.COM.BR

JORNAL DO COMMERCIO

JCOMMERCIO

Av. Leonardo Malcher, 598 - Centro
Manaus/AM
Central de Relacionamento
(92) 2126-0600
uniodontomanaus.com.br

uniodonto Manaus

UNIODONTO MANAUS – COOPERATIVA ODONTOLÓGICA LTDA.
CNPJ 23.031.479/0001-29 – NIRE 13400000700 – ANS 31139-1

ERRATA DE EDITAL DE CONVOCAÇÃO DE ASSEMBLÉIA GERAL EXTRAORDINÁRIA

No Edital de Convocação de Assembleia Geral Extraordinária publicado no dia 02 de janeiro de 2026, no Jornal do Comércio, Edição 44.458, Publicações Legais, por um erro de digitação no ano de realização da referida Assembleia, onde se lê: "que será realizada no dia **15 de janeiro 2025**, (5ª feira)", lê-se "que será realizada no dia **15 de janeiro 2026**, (5ª feira)". Os demais itens permanecem inalterados.

Manaus, 03 de janeiro de 2026

Dra. Maria Eliana Cruz de Almeida Pereira
Presidente do Conselho de Administração

MULTIPLATAFORMA

DISPONÍVEL EM TODAS AS PLATAFORMAS DIGITAIS

Jornal do Commercio
JCAM
JCAM.COM.BR

Este documento foi assinado digitalmente por Jornal do Comercio LTDA.
Para verificar as assinaturas vá ao site http://assinaturas.certisign.com.br e utilize o código 2A99-EC3B-61FD-6094.

PROTOCOLO DE ASSINATURA(S)

O documento acima foi proposto para assinatura digital na plataforma Certisign Assinaturas. Para verificar as assinaturas clique no link: http://assinaturas.certisign.com.br/Verificar/2A99-EC3B-61FD-6094 ou vá até o site http://assinaturas.certisign.com.br e utilize o código abaixo para verificar se este documento é válido.

Código para verificação: 2A99-EC3B-61FD-6094

Hash do Documento

28BE29B741F809F42FB383C793D604ACB9D506B266AB45A13A9793BF923880C8

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 02/01/2026 é(são) :

☑ Maria Suely Vasconcelos Do Nascimento - 04.561.791/000*-** em 02/01/2026 19:39 UTC-03:00
Tipo: Certificado Digital - EMPRESA JORNAL DO COMERCIO LTDA - 04.561.791/0001-80

Evidências

Geolocation: Latitude: -3.107141 Longitude: -60.0057246 Accuracy: 2703.229078375638
IP: 172.16.4.14
AC: AC DIGITAL MULTIPLA G1

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

OFÍCIO Nº 2.2026.CPL.2038659.2025.007562

Manaus, *na data da assinatura eletrônica.*

A Sua Excelência o Senhor

ANDRÉ VIRGÍLIO BELOTA SEFFAIR

Subprocurador-Geral de Justiça para Assuntos Administrativos

Assunto: Designação de Pregoeiro(a), suplente e equipe de apoio - PE 94.001/2026-CPL/MP/PGJ.

Senhor Subprocurador-Geral de Justiça,

Honra-me cumprimentá-lo com o presente e, à oportunidade, solicitar a designação dos servidores abaixo mencionados como **Pregoeiro(a)** e **suplente** de Pregoeiro(a), bem como dos demais **membros** (titulares e/ou suplentes) desta Comissão Permanente de Licitação que integrarão a equipe de apoio do respectivo certame, conforme relação a seguir:

- **PREGÃO ELETRÔNICO N.º 94.001/2026-CPL/MP/PGJ - PROCESSO SEI N.º 2025.007562**

Objeto: *Contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma* ***solução de datacenter,*** *contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com* ***garantia de 60 (sessenta) meses****.*

Data: 19/01/2026

Horário: 10h (horário de Brasília)

Pregoeiro(a):

— **SARAH MADALENA BARBOSA CÔRTES DE MELO**

Equipe de Apoio:

— KÁTIA RENATA DA SILVA SILVESTRE (Suplente);

— ANNE JAKELINE CARVALHO DAS NEVES; e

— MAURICIO ARAÚJO MEDEIROS.

Respeitosamente,

Sarah Madalena B. Côrtes de Melo

Presidente da Comissão Permanente de Licitação
Ato PGJ n.º 165/2025 - DOMPE, Ed. 3121, de 15.07.2025

Documento assinado eletronicamente por **Sarah Madalena Barbosa Santos Cortes**, **Presidente da Comissão Permanente de Licitação - CPL**, em 12/01/2026, às 14:10, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2038659** e o código CRC **E58672A3**.

PORTARIA 66/2026/SUBADM

A PROCURADORA-GERAL DE JUSTIÇA, por substituição legal, no uso de suas atribuições legais, e

CONSIDERANDO o teor do Procedimento Interno n.º 2025.007562 – SEI,

CONSIDERANDO o teor do ATO PGJ N.º 389/2007, datado de 26.11.2007, que regulamenta a utilização da modalidade Pregão no âmbito do Ministério Público do Estado do Amazonas,

RESOLVE:

I – DESIGNAR a servidora **SARAH MADALENA BARBOSA CÔRTES DE MELO**, Agente de Apoio – Administrativo, como Pregoeira do **Pregão Eletrônico n.º 94.001/2026-CPL/MP/PGJ - *Contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma* ***solução de datacenter,*** *contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com* ***garantia de 60 (sessenta) meses****;* e, para auxiliá-la, bem como substituí-la em seus impedimentos ou afastamentos, a servidora **KÁTIA RENATA DA SILVA SILVESTRE** , Agente de Apoio – Administrativo;

II – DESIGNAR os servidores **ANNE JAKELINE CARVALHO DAS NEVES** e **MAURÍCIO ARAÚJO MEDEIROS**, ambos Agentes de Apoio – Administrativo, membros da Comissão Permanente de Licitação desta Instituição, para compor a Equipe de Apoio do referido Pregão.

Publique-se, registre-se, cumpra-se.

SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, em Manaus/AM, *na data da assinatura eletrônica*.

ANABEL VITÓRIA PEREIRA MENDONÇA DE SOUZA
Procuradora-Geral de Justiça, em substituição legal

Documento assinado eletronicamente por **Anabel Vitória Pereira Mendonça de Souza**, **Subprocurador(a)-Geral de Justiça para Assuntos Jurídicos e Institucionais**, em 19/01/2026, às 15:36, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2048588** e o código CRC **271DB8B2**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

CERTIDÃO Nº 83.2026.SUBADM.2049676.2025.007562

Certifica-se, para os devidos fins, que a Portaria nº 66/2026/SUBADM foi encaminhada ao DOMPE para publicação, em 19/01/2026.

Documento assinado eletronicamente por **Mayra Magalhaes Coelho Bezerra**, **Agente Técnico - Jurídico**, em 19/01/2026, às 15:50, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2049676** e o código CRC **9EBF213C**.

25/03/2026 a 03/04/2026.
Anabel Vitória Pereira Mendonça de Souza
SUBPROCURADORA-GERAL DE JUSTIÇA PARA ASSUNTOS JURÍDICOS E INSTITUCIONAIS

REQUERIMENTO Nº 415671/2026

Interessado: José Augusto Palheta Taveira Júnior
A SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS JURÍDICOS E INSTITUCIONAIS, no uso de suas atribuições legais, autoriza o gozo de 10 dia(s) de férias ao(à) Exmo. Sr. Promotor de Justiça de Entrância Final em epígrafe, relativas ao período aquisitivo 1º/2025, para fruição no período no período de 01/07/2026 a 10/07/2026.
Anabel Vitória Pereira Mendonça de Souza
SUBPROCURADORA-GERAL DE JUSTIÇA PARA ASSUNTOS JURÍDICOS E INSTITUCIONAIS

REQUERIMENTO Nº 415810/2026

Interessado: Flávio Mota Morais Silveira
A SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS JURÍDICOS E INSTITUCIONAIS, no uso de suas atribuições legais, autoriza o gozo de 10 dia(s) de férias ao(à) Exmo. Sr. Promotor de Justiça de Entrância Final em epígrafe, relativos ao período aquisitivo 2º/2025, originalmente previstas no período de 02/03/2026 a 11/03/2026, para fruição no no período de 23/02/2026 a 04/03/2026.
Anabel Vitória Pereira Mendonça de Souza
SUBPROCURADORA-GERAL DE JUSTIÇA PARA ASSUNTOS JURÍDICOS E INSTITUCIONAIS

REQUERIMENTO Nº 415814/2026

Interessado: Flávio Mota Morais Silveira
A SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS JURÍDICOS E INSTITUCIONAIS, no uso de suas atribuições legais, autoriza o gozo de 10 dia(s) de férias ao(à) Exmo. Sr. Promotor de Justiça de Entrância Final em epígrafe, relativas ao período aquisitivo 1º/2026, para fruição no período no período de 27/04/2026 a 06/05/2026.
Anabel Vitória Pereira Mendonça de Souza
SUBPROCURADORA-GERAL DE JUSTIÇA PARA ASSUNTOS JURÍDICOS E INSTITUCIONAIS

REQUERIMENTO Nº 415815/2026

Interessado: Flávio Mota Morais Silveira
A SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS JURÍDICOS E INSTITUCIONAIS, no uso de suas atribuições legais, autoriza o gozo de 10 dia(s) de férias ao(à) Exmo. Sr. Promotor de Justiça de Entrância Final em epígrafe, relativas ao período aquisitivo 1º/2026, para fruição no período no período de 08/06/2026 a 17/06/2026.
Anabel Vitória Pereira Mendonça de Souza
SUBPROCURADORA-GERAL DE JUSTIÇA PARA ASSUNTOS JURÍDICOS E INSTITUCIONAIS

REQUERIMENTO Nº 415816/2026

Interessado: Flávio Mota Morais Silveira
A SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS JURÍDICOS E INSTITUCIONAIS, no uso de suas atribuições legais, autoriza o gozo de 10 dia(s) de férias ao(à) Exmo. Sr. Promotor de Justiça de Entrância Final em epígrafe, relativas ao período aquisitivo 2º/2026, para fruição no período no período de 13/07/2026 a 22/07/2026.
Anabel Vitória Pereira Mendonça de Souza
SUBPROCURADORA-GERAL DE JUSTIÇA PARA ASSUNTOS JURÍDICOS E INSTITUCIONAIS

REQUERIMENTO Nº 415817/2026

Interessado: Flávio Mota Morais Silveira
A SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS JURÍDICOS E INSTITUCIONAIS, no uso de suas atribuições legais, autoriza o gozo de 10 dia(s) de férias ao(à) Exmo. Sr. Promotor de Justiça de Entrância Final em epígrafe, relativas ao período aquisitivo 2º/2026, para fruição no período no período de 21/09/2026 a 30/09/2026.
Anabel Vitória Pereira Mendonça de Souza
SUBPROCURADORA-GERAL DE JUSTIÇA PARA ASSUNTOS JURÍDICOS E INSTITUCIONAIS

ATOS DA SUBPROCURADORIA-GERAL PARA ASSUNTOS ADMINISTRATIVOS

PORTARIA Nº 65/2026/SUBADM

O SUBPROCURADOR–GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, no uso de suas atribuições legais, e

CONSIDERANDO o teor do Procedimento Administrativo n.º 2025.027347 – SEI,

RESOLVE:

LOTAR a servidora ANA PAULA FRAGATA LIMA, Assessora Jurídica de Promotoria de Justiça de Entrância Inicial, para exercer suas funções junto à Promotoria de Justiça de Nova Olinda do Norte/AM, a contar de 12/01/2026.

Publique-se, registre-se, cumpra-se.

SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, em Manaus/AM, 14 de janeiro de 2026.

ANDRÉ VIRGÍLIO BELOTA SEFFAIR
Subprocurador-Geral de Justiça para Assuntos Administrativos

PORTARIA Nº 66/2026/SUBADM

A PROCURADORA–GERAL DE JUSTIÇA, por substituição legal, no uso de suas atribuições legais, e

CONSIDERANDO o teor do Procedimento Interno n.º 2025.007562 – SEI,

CONSIDERANDO o teor do ATO PGJ N.º 389/2007, datado de 26.11.2007, que regulamenta a utilização da modalidade Pregão no âmbito do Ministério Público do Estado do Amazonas,

RESOLVE:

I – DESIGNAR a servidora SARAH MADALENA BARBOSA CÔRTES DE MELO, Agente de Apoio – Administrativo, como Pregoeira do Pregão Eletrônico n.º 94.001/2026-CPL/MP/PGJ - Contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado

PROCURADORIA-GERAL DE JUSTIÇA

Procuradora-Geral de Justiça:
Leda Mara Nascimento Albuquerque
Subprocuradora-Geral de Justiça para Assuntos Jurídicos e Institucionais:
Anabel Vitória Pereira Mendonça de Souza
Subprocurador-Geral de Justiça para Assuntos Administrativos:
André Virgílio Belota Seffair
Corregedora-Geral do Ministério Público:
Silvana Nobre de Lima Cabral
Secretária-Geral do Ministério Público:
Wandete de Oliveira Netto

PROCURADORES DE JUSTIÇA

Câmaras Cíveis
Elvys de Paula Freitas
Sandra Cal Oliveira
Jussara Maria Pordeus e Silva
Mara Nóbia Albuquerque da Cunha
Suzete Maria dos Santos
Nilda Silva de Sousa
Delisa Olívia Vieiralves Ferreira
Jorge Michel Ayres Martins
Anabel Vitória Pereira Mendonça de Souza
Marco Aurélio Lisciotto

Câmaras Criminais
Carlos Lélio Lauria Ferreira
Marlene Franco da Silva
Mauro Roberto Veras Bezerra
Sarah Pirangy de Souza
Aguinelo Balbi Júnior
Liani Mônica Guedes de Freitas Rodrigues
Adelton Albuquerque Matos

Câmaras Reunidas
Karla Fregapani Leite
Públio Caio Bessa Cyrino
Sílvia Abdala Tuma
José Bernardo Ferreira Júnior
Neyde Regina Demósthenes Trindade
Silvana Nobre de Lima Cabral

CONSELHO SUPERIOR

Leda Mara Nascimento Albuquerque (Presidente)
Silvana Nobre de Lima Cabral
Mara Nóbia Albuquerque da Cunha
Adelton Albuquerque Matos
Elvys de Paula Freitas
Jorge Michel Ayres Martins
Nilda Silva de Sousa

OUVIDORIA
Sílvia Abdala Tuma

Publicação DOMPE 3241_19/01/2026_Portaria 66 (2050210) SEI 2025.007562 / pg. 365

para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses; e, para auxiliá-la, bem como substituí-la em seus impedimentos ou afastamentos, a servidora KÁTIA RENATA DA SILVA SILVESTRE, Agente de Apoio – Administrativo;

II – DESIGNAR os servidores ANNE JAKELINE CARVALHO DAS NEVES e MAURÍCIO ARAÚJO MEDEIROS, ambos Agentes de Apoio – Administrativo, membros da Comissão Permanente de Licitação desta Instituição, para compor a Equipe de Apoio do referido Pregão.

Publique-se, registre-se, cumpra-se.

SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, em Manaus/AM, na data da assinatura eletrônica.

ANABEL VITÓRIA PEREIRA MENDONÇA DE SOUZA
Procuradora-Geral de Justiça, em substituição legal

PORTARIA Nº 67/2026/SUBADM

A PROCURADORA–GERAL DE JUSTIÇA, por substituição legal, no uso das atribuições legais, e

CONSIDERANDO o teor do Procedimento Interno n.º 2026.000309 - SEI;

RESOLVE:

I – CONSTITUIR Grupo de Trabalho composto pelos servidores FÁBIO DA SILVA REBOUÇAS, Assessor Jurídico de Subprocurador-Geral de Justiça, e PAULO HENRIQUE GURJÃO DA SILVA, Assessor Jurídico de Procurador de Justiça, para atuarem no acervo processual da 18ª Procuradoria de Justiça, conforme indicação da Coordenação do Centro de Apoio Operacional – CAO-PROC;

II - FIXAR o prazo para realização dos trabalhos em 30 (trinta) dias, no período de 19/01/2026 a 19/02/2026, com meta individual de 90 (noventa) processos por integrante, englobando despachos de instrução, instauração e/ou conversão de procedimentos, promoções, pareceres, petições judiciais iniciais, intermediárias, recursais e outras similares, excluindo-se aquelas em que a manifestação consista em mera ciência ou expediente do Ministério Público;

III - DETERMINAR a apresentação de relatório individualizado, com cópia, em único documento PDF, das peças produzidas pelos servidores integrantes deste Grupo de Trabalho, devidamente atestado pelo Exmo. Sr. Dr. ADELTON ALBUQUERQUE MATOS, Procurador de Justiça e Coordenador do CAO-PROC.

IV - AUTORIZAR o pagamento de gratificação estabelecida pelo § 1.º do art. 6.º, do ATO PGJ N.º 233/2011, aos servidores integrantes do presente grupo de trabalho, após apresentação de relatório individual de atividades.

Publique-se, registre-se, cumpra-se.

SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, em Manaus/AM, 19 de janeiro de 2026.

ANABEL VITÓRIA PEREIRA MENDONÇA DE SOUZA
Procuradora-Geral de Justiça, em substituição legal

PORTARIA Nº 68/2026/SUBADM

A PROCURADORA–GERAL DE JUSTIÇA, por substituição legal, no uso das atribuições legais, e

CONSIDERANDO o teor do Procedimento Interno n.º 2026.000169 - SEI;

RESOLVE:

I – CONSTITUIR Grupo de Trabalho composto pelas servidoras HELOYSA NOGUEIRA DA ROCHA e KELEM CRISTINA LOPES DE CASTRO, Assessoras Jurídicas de Promotoria de Justiça de Entrância Inicial, para atuarem no acervo processual da 03.ª Promotoria de Justiça de Manacapuru;

II - FIXAR o prazo para realização dos trabalhos em 30 (trinta) dias, no período de 19/01/2026 a 18/02/2026, com meta individual de 90 (noventa) processos por integrante, englobando despachos de instrução, instauração e/ou conversão de procedimentos, promoções, pareceres, petições judiciais iniciais, intermediárias, recursais e outras similares, excluindo-se aquelas em que a manifestação consista em mera ciência ou expediente;

III - DETERMINAR a apresentação de relatório individualizado, com cópia, em único documento PDF, das peças produzidas pelas servidoras integrantes deste Grupo de Trabalho, devidamente atestado pelo Exmo. Sr. Dr. VINÍCIUS RIBEIRO DE SOUZA, Promotor de Justiça de Entrância Inicial.

IV - AUTORIZAR o pagamento de gratificação estabelecida pelo § 1.º do art. 6.º, do ATO PGJ N.º 233/2011, aos servidores integrantes do presente grupo de trabalho, após apresentação de relatório individual de atividades.

Publique-se, registre-se, cumpra-se.

SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, em Manaus/AM, 19 de janeiro de 2026.

ANABEL VITÓRIA PEREIRA MENDONÇA DE SOUZA
Procuradora-Geral de Justiça, em substituição legal

PORTARIA Nº 70/2026/SUBADM

O SUBPROCURADOR-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, no uso de suas atribuições legais, e

CONSIDERANDO o teor do Despacho Nº 60.2026.07AJ-SUBADM.2046183.2025.027615;

RESOLVE:

EXCLUIR os servidores BRUNO MARQUES DA SILVA e KAREN BRANDÃO PONTES, ambos Agentes Técnico-Jurídicos, do Grupo de Trabalho constituído pela PORTARIA Nº 1402/2025/SUBADM, datada de 27 de dezembro de 2025, que tem por objetivo atuar na demanda reprimida de processos em trâmite nas Promotorias de Justiça vinculadas ao CAO-PDC, a contar de 07/01/2026.

Publique-se, registre-se, cumpra-se.

SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, em Manaus/AM, na data da assinatura de eletrônica.

ANABEL VITÓRIA PEREIRA MENDONÇA DE SOUZA

PROCURADORIA-GERAL DE JUSTIÇA

Procuradora-Geral de Justiça:
Leda Mara Nascimento Albuquerque
Subprocuradora-Geral de Justiça para Assuntos Jurídicos e Institucionais:
Anabel Vitória Pereira Mendonça de Souza
Subprocurador-Geral de Justiça para Assuntos Administrativos:
André Virgílio Belota Seffair
Corregedora-Geral do Ministério Público:
Silvana Nobre de Lima Cabral
Secretária-Geral do Ministério Público:
Wandete de Oliveira Netto

PROCURADORES DE JUSTIÇA

Câmaras Cíveis
Elvys de Paula Freitas
Sandra Cal Oliveira
Jussara Maria Pordeus e Silva
Mara Nóbia Albuquerque da Cunha
Suzete Maria dos Santos
Nilda Silva de Sousa
Delisa Olívia Vieiralves Ferreira
Jorge Michel Ayres Martins
Anabel Vitória Pereira Mendonça de Souza
Marco Aurélio Lisciotto

Câmaras Criminais
Carlos Lélio Lauria Ferreira
Marlene Franco da Silva
Mauro Roberto Veras Bezerra
Sarah Pirangy de Souza
Aguinelo Balbi Júnior
Liani Mônica Guedes de Freitas Rodrigues
Adelton Albuquerque Matos

Câmaras Reunidas
Karla Fregapani Leite
Públio Caio Bessa Cyrino
Sílvia Abdala Tuma
José Bernardo Ferreira Júnior
Neyde Regina Demósthenes Trindade
Silvana Nobre de Lima Cabral

CONSELHO SUPERIOR

Leda Mara Nascimento Albuquerque (Presidente)
Silvana Nobre de Lima Cabral
Mara Nóbia Albuquerque da Cunha
Adelton Albuquerque Matos
Elvys de Paula Freitas
Jorge Michel Ayres Martins
Nilda Silva de Sousa

OUVIDORIA
Sílvia Abdala Tuma

Publicação DOMPE 3241_19/01/2026_Portaria 66 (2050210) SEI 2025.007562 / pg. 366

Ao
MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS

Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

ANEXO IV - PROPOSTA DE PREÇOS

Proposta que faz a empresa **CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA**, inscrita no CNPJ (MF) n.º **02.092.332/0003-30**, localizada na **R. Samuel Meira Brasil– 394 – Sala 29 – Bairro: Taquara II – Serra – ES – CEP: 29.167-650**, fone **(11) 9. 6649-5676**, e-mail: **public.sector@clm.tech**, para o fornecimento dos bens abaixo relacionados, de acordo com todas as especificações e condições estabelecidas no **Pregão Eletrônico n.º 94.001/2026-CPL/MP/PGJ - SRP**, promovido pelo **MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS / PROCURADORIA-GERAL DE JUSTIÇA:**

Item	Descrição	Marca/Modelo/ Tipo/Referência	Qtd. (A)	Valor Unitário (B)	Valor Total (C= A*B)
01	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9	NUTANIX **Modelo:** NX8155G9	4	R$ 588.062,00	R$ 2.352.248,00
02	EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU	NUTANIX **Modelo:** NX-3155-G9	1	R$ 832.942,00	R$ 832.942,00
03	SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX	NUTANIX **Modelo:** NAI GPT IN A BOX PRO	5	R$ 790.000,00	R$ 3.950.000,00
04	SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU	NUTANIX **Modelo:** SW-NAI-PRO-GB-PR	1	R$ 164.252,00	R$ 164.252,00
05	LICENÇA PARAARMAZENAMENTO DE DADOS NÃO	NUTANIX **Modelo:** SW-NAI-GPT-PRO-C-PR	50	R$ 9.250,98	R$ 462.549,00

	ESTRUTURADOS - NUTANIX UNIFIED STORAGE				
06	SOFTWARE DE BACKUP DE DADOS	VEEAM **Modelo:** Veeam Data Platform Advanced	1	R$ 900.000,00	R$ 900.000,00
07	EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	Exagrid **Modelo:** EX54-SEC	1	R$ 230.000,00	R$ 230.000,00
08	SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	EXAGRID **Modelo:** Backup Storage Software	1	R$ 1.200.000,00	R$ 1.200.000,00
09	SWITCH CORE	JUNIPER **Modelo:** QFX5120	2	R$ 262.143,50	R$ 524.287,00
VALOR TOTAL DA PROPOSTA				**R$ 10.616.278,00**	

VALOR TOTAL DA PROPOSTA **R$ 10.616.278,00** - **Dez milhões, seiscentos e dezesseis mil, duzentos e setenta e oito reais.**

A **CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA**, declara que concorda com todas as especificações do Edital.

a. Prazo de validade da proposta: 90 (noventa) dias, a contar da data de sua apresentação.
b. Prazo de entrega da solução: 60 (sessenta) dias corridos, conforme depõe o Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562;
c. Modo de Transporte dos Produtos:
   (x) aéreo
d. Prazo de garantia e assistência técnica: 60 (sessenta) meses, conforme depõe o Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562;
e. Site e/ou e-mail do fabricante, se houver:
   https://www.nutanix.com
   https://www.veeam.com
   https://www.exagrid.com

https://www.juniper.net
https://www.microsoft.com/pt-br

f. Dados Bancários:
Banco do Brasil – 001
Agência: 1744-2
Conta Corrente: 24503-8

g. Contato para fins de recebimento de notas de empenho:
Nome: Tatiana Montroze
public.sector@clm.tech
Cel: 11 9.6649-5676

h. Contato para fins de faturamento:
Nome: Alexandre Nicácio / Larissa Maciel
E-mail: alexandre.nicacio@clm.tech/ recebimentofiscal@clm.tech/
Larissa.maciel@clm.tech
CNPJ: 02.092.332/0003-30

DECLARAÇÕES:

Declaro, sob as penas da Lei, para os devidos fins junto à Comissão Permanente de Licitação que:

a. Cumpro plenamente os requisitos de habilitação, ciente de que respondo pela veracidade das informações prestadas, na forma da lei;

b. Em atenção item 5.6. e art. 14.º e seus incisos da Lei n.º 14.133/2021, não estou impedido de participar direta ou indiretamente desta licitação, e ainda, não possuo sócios, diretores ou gerentes, que sejam cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do Ministério Público do Estado do Amazonas e de sua CPL;

c. Recebi o edital e todos os documentos que o integram, dispondo de todos os elementos e informações necessários à elaboração da proposta de preços com total e completo conhecimento do objeto da licitação;

d. Os documentos e declarações apresentados são fiéis e verdadeiros;

e. Caso seja vencedor do certame e não cadastrado no SISTEMA DE ADMINISTRAÇÃO FINANCEIRA E CONTABILIDADE da SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ-AM, encaminharei à CONTRATANTE os documentos necessários para efetuar o

referido cadastramento no prazo de 05 (cinco) dias úteis, a contar da adjudicação, sob pena de perder o direito de preferência à contratação em favor dos demais licitantes subsequentes, sem prejuízo da possibilidade de responder a procedimento administrativo de responsabilização por eventual retardamento da licitação;

f. O preço inclui além do lucro, todos os custos e despesas, com tributos incidentes e encargos devidos, materiais, serviços, transporte, a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas, bem como quaisquer outras despesas diretas e indiretas incidentes na prestação de serviços;

g. Apresentarei, quando da contratação, documento que indique o pessoal técnico operacional, das instalações e do aparelhamento adequado e disponíveis para a realização do objeto da licitação, bem como a qualificação de cada membro da equipe técnica que se responsabilizará pelos trabalhos;

h. Submeto-me e concordo integralmente com os termos do presente Edital, bem como com seus elementos e especificações, comprometendo-me a cumpri-los fielmente, inclusive no que se refere à fiscalização e ao controle técnico a serem exercidos por profissional expressamente designado para tal finalidade; e

i. A proposta apresentada para participar do presente Pregão foi elaborada de maneira independente por esta licitante e o seu conteúdo não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer outro participante potencial ou de fato, por qualquer meio ou por qualquer pessoa

Serra (ES), 19 de janeiro de 2026.

gov.br Documento assinado digitalmente
TATIANA MONTEIRO MONTROZE
Data: 19/01/2026 15:03:59-0300
Verifique em https://validar.iti.gov.br

CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA
Tatiana Monteiro Montroze
RG: 40.183.211-9
CPF: 354.042.638-81

ITENS	DOCUMENTAÇÃO	COMPROVAÇÃO
7. ITEM 01 - EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9		
7.1 Características Gerais		
7.1.1 A infraestrutura deverá ser composta por appliances Nutanix com integração completa entre hardware e software, armazenamento e rede, entregando uma solução hiperconvergente pronta para operação.	https://www.nutanix.com/products/hardware-platforms/specsheet?platformProvider=Nutanix	
7.1.2 Serão aceitos apenas appliances homologados pela Nutanix para uso com o Nutanix AOS (Acropolis Operating System) e Nutanix AHV (Acropolis Hypervisor) ou outro hipervisor suportado pela plataforma.	https://www.nutanix.com/products/hardware-platforms/specsheet?platformProvider=Nutanix	
7.1.3 Caso necessário, será permitida a entrega de equipamentos ou recursos adicionais para atender aos requisitos mínimos, desde que todos os componentes estejam integrados e certificados pela Nutanix.	Ciente e de acordo / Conforme Proposta Tecnica	
7.1.4 É permitida a entrega de múltiplos nós em um único chassi, desde que compatível com a arquitetura Nutanix.	Ciente e de acordo / Conforme Proposta Tecnica	
7.1.5 A solução deve incluir a ferramenta Nutanix Prism, em sua ultima versão ou equivalente, que oferece gerenciamento centralizado e interface gráfica para monitoramento, atualizações e operação da infraestrutura, incluindo:	Ciente e de acordo / Conforme Proposta Tecnica	
7.1.5.1 Atualização de BIOS, firmware, hipervisor e SDS;	RA-2147-Nutanix-for-Enterprise-Edge.pdf	
7.1.5.2 Visualização do hardware físico;	RA-2147-Nutanix-for-Enterprise-Edge.pdf	
7.1.5.3 Diagnóstico, inventário e expansão de nós.	RA-2147-Nutanix-for-Enterprise-Edge.pdf	
7.1.6 Caso alguma funcionalidade não esteja disponível via Prism ou equivalente para monitoramento ou atualização, a CONTRATADA deverá realizar este serviço de forma remota/on-line ou presencial.	Ciente e de acordo / Conforme Proposta Tecnica	
7.1.7 Todas as atualizações devem ser homologadas pela Nutanix e aplicadas conforme as melhores práticas da fabricante. Esta ferramenta deve ser gráfica, com suporte a apresentação de visões do hardware físico dos nós, suporte a troca de drives, com controle do inventário, com ferramenta de diagnóstico e com módulo para a adição de novos nós.	Ciente e de acordo / Conforme Proposta Tecnica	
7.1.8 A arquitetura deve garantir alta disponibilidade (HA) e resiliência a falhas, com suporte a recuperação de desastres (DR).	https://www.nutanixbible.com/4c-book-of-aos-storage.html	
7.1.9 Os appliances devem permitir expansão modular e não disruptiva dos serviços de rede e aplicações, com detecção automática de novos nós.	TN-2042-Prism.PDF	
7.1.10 Deve centralizar o armazenamento de dados em discos compartilhados, redundantes.	https://www.nutanixbible.com/4c-book-of-aos-storage.html	
7.1.11 Cada nó deverá conter armazenamento dedicado para o sistema operacional da plataforma.	System-Specs-NX8155G9.PDF	
7.1.12 A solução deve estar preparada para ambientes de virtualização em alta disponibilidade, conforme as práticas recomendadas pela Nutanix.	Ciente e de acordo / Conforme Proposta Tecnica	
7.1.13 Deve suportar software de virtualização para consolidação de servidores e recuperação automática em caso de falhas físicas, minimizando o downtime.	https://www.nutanixbible.com/4c-book-of-aos-storage.html	
7.1.14 A entrega deve ser feita com todos os componentes física e logicamente integrados, sem ponto único de falha, com acesso imediato ao ambiente via sistema de gestão da plataforma após energização e conexão.	Ciente e de acordo / Conforme Proposta Tecnica	
7.1.15 A instalação deve ser compatível com racks padrão de 19 polegadas, incluindo todos os acessórios necessários para montagem no ambiente da CONTRATANTE.	Ciente e de acordo / Conforme Proposta Tecnica System-Specs-NX8155G9.PDF	
7.1.16 O equipamento deve integrar a linha de produtos Nutanix da família “NX”, assegurando total compatibilidade com atual ambiente e possibilidade de expansão das zonas de disponibilidade já estabelecidas, conforme informações disponibilizadas no endereço eletrônico oficial da fabricante: https://www.nutanix.com/products/hardwareplatforms/specsheet?platformProvider=Nutanix.	Ciente e de acordo / Conforme Proposta Tecnica	
7.2 Configuração do Nó ou Chassi		
7.2.1 Serão admitidas ofertas de chassis que comportam múltiplos servidores (nós/nodes), para o atendimento da especificação técnica.	System-Specs-NX8155G9.PDF	
7.2.2 Cada nó, ou chassi, deverá possuir ventiladores e fontes redundantes para a operação adequada dos equipamentos.	Ciente e de acordo / Conforme Proposta Tecnica	

7.2.3 Todas as fontes de alimentação deverão ser acompanhadas de seus respectivos cabos de energia compatíveis.	Ciente e de acordo / Conforme Proposta Tecnica
7.3 Características de Processamento por Nó	
7.3.1 Cada servidor deverá possuir, no mínimo, 02 (dois) processadores com arquitetura x86, voltados ao uso em servidores, contendo as seguintes características mínimas:	om.br/content/www/br/pt/products/sku/236637/intel-xeon-silver-4510-processor-30m-cache-2-40-ghz/specifications.html
7.3.1.1 12 (doze) núcleos físicos e 24 (vinte e quatro) threads por processador;	om.br/content/www/br/pt/products/sku/236637/intel-xeon-silver-4510-processor-30m-cache-2-40-ghz/specifications.html
7.3.1.2 Frequência de clock nominal de, no mínimo, 2,4 GHz;	om.br/content/www/br/pt/products/sku/236637/intel-xeon-silver-4510-processor-30m-cache-2-40-ghz/specifications.html
7.3.1.3 Controladora de memória integrada com suporte à tecnologia DDR5 ou superior.	om.br/content/www/br/pt/products/sku/236637/intel-xeon-silver-4510-processor-30m-cache-2-40-ghz/specifications.html
7.3.2 Será admitida a entrega de processadores de geração superior ao modelo originalmente especificado, desde que mantenham no mínimo a mesma quantidade de núcleos e threads, independentemente de demais especificações.	Ciente e de acordo / Conforme Proposta Tecnica
7.4 Especificações de Memória por Nó	
7.4.1 Cada servidor deverá ser fornecido com, no mínimo, 1.536 GB (um mil quinhentos e trinta e seis gigabytes) de memória RAM, distribuída uniformemente entre os processadores, utilizando módulos DDR5 ou superior.	Ciente e de acordo / Conforme Proposta Tecnica
7.5 Especificações de Rede por Nó	
7.5.1 Cada servidor deverá ser entregue com as seguintes interfaces de rede:	Ciente e de acordo / Conforme Proposta Tecnica
7.5.1.1 Mínimo de 2 (duas) interfaces de 25/10 GbE SFP28, integradas em uma placa de rede;	System-Specs-NX8155G9.pdf
7.5.1.2 Mínimo de 1 (uma) interface exclusiva de gerenciamento Ethernet 1000Base-T.	System-Specs-NX8155G9.pdf
7.5.2 A interface de gerenciamento deverá vir acompanhada de cabos UTP categoria 6 (ou superior), com comprimento mínimo de 5 (cinco) metros e conectores RJ-45	Ciente e de acordo / Conforme Proposta Tecnica
7.6 Especificações de Armazenamento por Nó	
7.6.1 Cada servidor deverá ser entregue com a seguinte configuração mínima de discos:	
7.6.1.1 04 (quatro) unidades de SSD NVMe, ou SSD SAS/SATA, com capacidade mínima de 3,84 TB por unidade (volumetria bruta);	Ciente e de acordo / Conforme Proposta Tecnica
7.6.1.2 08 (oito) unidades de disco rígido (HDD), com capacidade mínima de 12 TB por unidade (volumetria bruta).	Ciente e de acordo / Conforme Proposta Tecnica
8. ITEM 02 - EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU	
8.1 Características Gerais	
8.1.1 A solução deverá ser composta exclusivamente por appliances de nuvem privada, com integração total entre recursos de computação, armazenamento e rede, entregues como infraestrutura unificada.	https://www.nutanix.com/products/hardware-platforms/specsheet?platformProvider=Nutanix
8.1.2 Serão aceitos apenas appliances homologados para uso com a solução de armazenamento definido por software (Software Defined Storage – SDS) ofertada	https://www.nutanix.com/products/hardware-platforms/specsheet?platformProvider=Nutanix
8.1.3 A entrega de equipamentos ou recursos adicionais será aceita, desde que necessária para o atendimento aos requisitos mínimos e que todos os componentes estejam devidamente integrados.	Ciente e de acordo / Conforme Proposta Tecnica
8.1.4 É permitida a entrega de múltiplos nós consolidados em um único chassi modular.	Ciente e de acordo / Conforme Proposta Tecnica
8.1.5 A solução deverá incluir ferramenta unificada de gerenciamento e atualização, com capacidade de monitorar e atualizar BIOS, firmwares, hypervisor e componentes do SDS. Caso não realize todos os procedimentos listados, a CONTRATADA deverá garantir a execução dessas tarefas presencial ou remotamente.	https://www.nutanixbible.com/3-book-of-prism.html e RA-2147-Nutanix-for-Enterprise-Edge / RA-2147-Nutanix-for-Enterprise-Edge.pdf
8.1.6 A ferramenta de gestão deverá ser gráfica, com visualização física dos nós, suporte à substituição de drives, inventário automatizado, diagnóstico integrado e capacidade de adicionar novos nós ao cluster.	TN-2042-Prism.pdf
8.1.7 A arquitetura deverá contemplar alta disponibilidade nativa e recursos para recuperação de desastres (DR), de forma a garantir continuidade dos serviços mesmo em caso de falhas parciais.	https://www.nutanixbible.com/4c-book-of-aos-storage.html
8.1.8 Os equipamentos devem possuir arquitetura modular, permitindo expansão de capacidade com inclusão de novos appliances sem interrupção dos serviços.	TN-2042-Prism.PDF
8.1.9 O armazenamento deverá ser centralizado, com discos compartilhados e redundância nativa.	https://www.nutanixbible.com/4c-book-of-aos-storage.html
8.1.10 Cada servidor deverá conter unidade de armazenamento dedicada ao sistema operacional da plataforma e aos softwares de virtualização e processamento gráfico.	System-Specs-NX3155G9.pdf

8.1.11 A infraestrutura deverá estar preparada para suportar ambientes virtualizados de alta disponibilidade, de acordo com as boas práticas do fabricante da solução.	Ciente e de acordo / Conforme Proposta Tecnica
8.1.12 A solução deverá oferecer suporte a consolidação de servidores e recuperação automática em caso de falhas físicas.	TN-2027-Data-Protection-and-Disaster
8.1.13 A entrega deverá ocorrer com a solução fisicamente e logicamente pré-integrada, sem ponto único de falha, com acesso imediato à plataforma após energização e conexão física.	Ciente e de acordo / Conforme Proposta Tecnica
8.1.14 A instalação deverá ser compatível com racks padrão de 19", com todos os acessórios de fixação inclusos.	Ciente e de acordo / Conforme Proposta Tecnica/System-Specs-NX3155G9.pdf
8.1.15 O equipamento deve integrar a linha de produtos Nutanix da família “NX”, assegurando total compatibilidade com atual ambiente e possibilidade de expansão das zonas de disponibilidade já estabelecidas, conforme informações disponibilizadas no endereço eletrônico oficial da fabricante: https://www.nutanix.com/products/hardwareplatforms/specsheet?platformProvider=Nutanix.	Ciente e de acordo / Conforme Proposta Tecnica
8.2 Configuração do Nó ou Chassi	
8.2.1 Serão admitidas ofertas de chassis que comportam múltiplos servidores (nós/nodes), para o atendimento da especificação técnica.	System-Specs-NX3155G9.pdf
8.2.2 Cada nó ou chassi deverá possuir ventiladores e fontes de alimentação redundantes.	Ciente e de acordo / Conforme Proposta Tecnica
8.2.3 Cada fonte deverá ser entregue com seu respectivo cabo de energia.	Ciente e de acordo / Conforme Proposta Tecnica
8.3 Características de Processamento por Nó	
8.3.1 Cada servidor deverá possuir, no mínimo, dois processadores com arquitetura x86, dedicados a ambientes de datacenter, com as seguintes características	Ciente e de acordo / Conforme Proposta Tecnica
8.3.2 12 (doze) núcleos físicos e 24 (vinte e quatro) threads por processador;	om.br/content/www/br/pt/products/sku/236637/intel-xeon-silver-4510-processor-30m-cache-2-40-ghz/specifications.html
8.3.3 Frequência mínima de 2,4 GHz;	om.br/content/www/br/pt/products/sku/236637/intel-xeon-silver-4510-processor-30m-cache-2-40-ghz/specifications.html
8.3.4 Controladora de memória integrada DDR5 ou superior.	om.br/content/www/br/pt/products/sku/236637/intel-xeon-silver-4510-processor-30m-cache-2-40-ghz/specifications.html
8.3.5 A substituição por processadores mais recentes será aceita, desde que observadas as quantidades mínimas de núcleos e threads.	Ciente e de acordo / Conforme Proposta Tecnica
8.4 Especificações de Memória por Nó	
8.4.1 - Cada servidor deverá ser entregue com no mínimo 1.024 GB (um mil e vinte e quatro gigabytes) de memória RAM, utilizando módulos DDR5 ou superior, distribuídos de forma equilibrada entre os processadores.	Ciente e de acordo / Conforme Proposta Tecnica
8.5 Especificações de Rede por Nó	Ciente e de acordo / Conforme Proposta Tecnica
8.5.1 Cada servidor deverá conter no mínimo:	
8.5.1.1 2 (duas) interfaces de rede 25/10 GbE SFP28;	System-Specs-NX3155G9.pdf
8.5.1.2 1 (uma) interface de gerenciamento 1000Base-T;	System-Specs-NX3155G9.pdf
8.5.1.3 A interface de gerenciamento deverá ser acompanhada de cabos UTP Cat-6 ou superior, com 5 metros de comprimento e conectores RJ-45.	System-Specs-NX3155G9.pdf
8.6 Especificações de Armazenamento por Nó	
8.6.1 Cada servidor deverá ser entregue com:	
8.6.1.1 2 discos SSD NVMe, SAS ou SATA, com capacidade mínima de 3,84 TB cada (volumetria bruta);	Ciente e de acordo / Conforme Proposta Tecnica
8.6.1.2 4 discos HDD com capacidade mínima de 12 TB cada (volumetria bruta).	Ciente e de acordo / Conforme Proposta Tecnica
8.7 Especificações de Processamento Gráfico e Cálculo Aritmético	
8.7.1 Cada servidor deverá conter uma placa gráfica com as seguintes características:	Ciente e de acordo / Conforme Proposta Tecnica
8.7.1.1 48 GB de memória GDDR6 de GPU;	l40s-datasheet-2841316.PDF
8.7.1.2 Interconexão PCIe Gen4 com largura de banda de 64 GB/s;	l40s-datasheet-2841316.PDF
8.7.1.3 Suporte a DirectX 12.075, Shader Model 5.175, OpenGL 4.686 e Vulkan 1.186;	l40s-datasheet-2841316.PDF
8.7.1.4 Compatibilidade com NVIDIA vPC/vApps, NVIDIA RTX Virtual Workstation e NVIDIA Virtual Compute Server;	https://www.nutanix.com/en_au/nvidia / https://docs.nvidia.com/vgpu/latest/index.html
8.7.1.5 Consumo máximo de 350W.	l40s-datasheet-2841316.PDF
9. ITEM 03 – SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX	
9.1 Camada de Armazenamento da Solução:	

9.1.1 A solução deverá contar com camada de armazenamento compartilhada entre todos os servidores e appliances descritos neste Termo, utilizando tecnologia de armazenamento definido por software (Software Defined Storage – SDS).	https://www.nutanixbible.com/2d-book-of-basics-distributed-system.html
9.1.2 A arquitetura de armazenamento deverá ser otimizada para ambientes virtuais, com escalabilidade contínua e elástica, permitindo expansão de capacidade pela adição de novos nós/appliances sem necessidade de licenciamento adicional de virtualização.	https://www.nutanixbible.com/2d-book-of-basics-distributed-system.html
9.1.3 Não serão aceitas soluções baseadas em tecnologia RAID para redundância de dados.	https://www.nutanixbible.com/4c-book-of-aos-storage.html
9.1.4 A solução deverá suportar as tecnologias de compressão e desduplicação de dados inline, near-line ou pós-processada, com o objetivo de otimização do armazenamento.	https://www.nutanixbible.com/4c-book-of-aos-storage.html
9.1.5 A solução deverá prover recursos de QoS (Quality of Service), para controle do volume de I/Os de VMs.	BP-2050-Physical-Networking.pdf
9.1.6 Deverá permitir uso de técnicas de Erasure Coding para otimização de aplicações com baixa sensibilidade à latência de escrita.	https://www.nutanixbible.com/4c-book-of-aos-storage.html
9.1.7 A solução deverá permitir a expansão do cluster através da adição de nós/servidores que incrementem tão somente a capacidade de armazenamento, sem a necessidade de emprego de licenças de virtualização nesses nós/servidores;	Web-Console-Guide-Prism-v7_0.pdf
9.1.8 A substituição de discos defeituosos deverá ocorrer sem impacto nas operações de leitura e escrita das aplicações.	Drive-Replacement-G9.pdf
9.1.9 A falha de um nó da solução não poderá comprometer a disponibilidade da camada de armazenamento das VMs.	https://www.nutanixbible.com/4c-book-of-aos-storage.html
9.1.10 A criptografia deverá ser aplicada em nível de cluster ou volume, via hardware ou software, com KMS nativo. Caso não possua, será aceita entrega de servidor redundante externo com essa funcionalidade.	https://www.nutanixbible.com/4b-book-of-aos-security.html
9.1.11 A distribuição dos dados deverá ocorrer de forma automática e uniforme dentro do cluster.	https://www.nutanixbible.com/4c-book-of-aos-storage.html
9.1.12 A solução deverá permitir criação de cópias no tempo (snapshots) sem movimentação dos dados originais e com redirecionamento de escritas subsequentes.	https://www.nutanixbible.com/4c-book-of-aos-storage.html
9.1.13 Deverá suportar clonagem de instâncias virtuais a partir de snapshots, sem movimentação dos dados.	https://www.nutanixbible.com/4c-book-of-aos-storage.html
9.1.14 Acesso ao armazenamento deverá ser possível via iSCSI por instâncias físicas ou virtuais externas ao cluster, garantindo suporte a aplicações de alta disponibilidade.	https://www.nutanixbible.com/11a-book-of-storage-services-volumes.html
9.2 Tecnologia de Replicação e Proteção de Dados:	
9.2.1 Deverá ser fornecida funcionalidade de replicação local realizando clones e snapshots com proteção contínua dos dados da máquina virtual.	https://www.nutanixbible.com/4e-book-of-aos-backup-dr.html
9.2.2 A solução deve prover as funcionalidades de Thin Provisioning e Serviços de Cópias de dados.	TN-2032-Data-Efficiency.pdf
9.2.3 Deverá permitir a configuração de um grupo ou domínio de proteção de instâncias virtuais, que poderão ser protegidas por cópias point-intime, bem como replicadas para um cluster remoto.	https://www.nutanixbible.com/4e-book-of-aos-backup-dr.html
9.2.4 Deverá permitir a união de máquinas virtuais em um único grupo de proteção.	https://www.nutanixbible.com/4e-book-of-aos-backup-dr.html
9.2.5 Deverá proteger, por cópias point-in-time, simultaneamente todas as máquinas virtuais pertencentes ao grupo.	https://www.nutanixbible.com/4e-book-of-aos-backup-dr.html
9.2.6 Deverá contemplar, também, a proteção nativa de máquinas virtuais consistentes com aplicações, onde há proteção dos dados em memória a partir da movimentação das operações de escrita para disco, de sistemas operacionais Linux e Windows. Caso a plataforma de nuvem privada não permita executar esta funcionalidade nativamente, a CONTRATADA deverá atender este requisito compondo com outra solução.	https://www.nutanixbible.com/4e-book-of-aos-backup-dr.html
9.2.7 Deverá permitir a configuração de uma entidade capaz de centralizar todo o fluxo do tráfego replicado entre clusters distintos, convergindo assim os recursos para um único ponto focal. Esse recurso centralizado deverá posteriormente redirecionar o tráfego corretamente para os equipamentos específicos do cluster de contingência.	https://www.nutanixbible.com/13a-book-of-dr-services-leap.html RA-2147-Nutanix-for-Enterprise-Edge.pdf
9.2.8 Deverá permitir ajustar o consumo de banda em replicações.	BP-2005-Data-Protection.pdf
9.2.9 Deverá permitir a existência de frequências distintas de replicação para instâncias virtuais em grupos diferentes.	

9.3 Gerenciamento Integrado:	
9.3.1 A solução deve oferecer solução de gerenciamento integrado, licenciado para gerenciar inclusive múltiplos clusters.	https://www.nutanixbible.com/3a-book-of-prism-architecture.html
9.3.2 Monitoração automática e periódica da solução, com o envio de notificações preventivamente em caso de falhas, notificando o suporte do fornecedor a tomar medidas preventivas e acordadas com a CONTRATANTE a fim de evitar tempo de inatividade e impactos na produção.	TN-2133-Nutanix-Pulse-Remote-Diagnos.pdf
9.3.3 Deve oferecer portal de acesso do próprio fornecedor para download de atualizações e de softwares agregados.	Ciente e de acordo / Conforme Proposta Tecnica
9.3.4 A ferramenta de gerenciamento, local, deve fornecer um dashboard reportando a utilização dos recursos do cluster como CPU, Memória, Armazenamento, IOPS do cluster, largura de banda do cluster, latência do cluster e informações sobre o virtualizador empregado e os alertas de saúde.	Prism-Central-Guide-vpc_2024_3.PDF
9.3.5 A solução deve fornecer atualização de todos os componentes (Firmware, e softwares de virtualização que fazem parte da solução) em forma de pacote com instalação assistida.	RA-2147-Nutanix-for-Enterprise-E.pdf
9.3.6 Contemplar as funcionalidades como:	
9.3.6.1 Emissão de relatório avançados do ambiente;	nix.com/page/documents/details?targetId=Intelligent-Operations-Guide-vpc_7_5:ssp-report-management-ssp-pc-c.html
9.3.6.2 Personalização da console principal;	portal.nutanix.com/page/documents/details?targetId=Web-Console-Guide-Prism-v7_5:wc-overview-wc-r.html
9.3.6.3 Planejamento e previsão de capacidade;	utanix.com/page/documents/details?targetId=Intelligent-Operations-Guide-vpc_7_5:mul-capacity-planning-pc-c.html
9.3.6.4 Detecção de ineficiência de cargas de trabalho e dimensionamento ideal;	utanix.com/page/documents/details?targetId=Intelligent-Operations-Guide-vpc_7_5:mul-behavioral-learning-pc-c.html
9.3.6.5 Planejamento de capacidade ou cargas de trabalho ao longo do tempo;	utanix.com/page/documents/details?targetId=Intelligent-Operations-Guide-vpc_7_5:mul-capacity-planning-pc-c.html
9.3.6.6 Permitir automação de operações de gerência do ambiente.	nix.com/page/documents/details?targetId=Intelligent-Operations-Guide-vpc_7_5:mul-automation-management-pc-c.html
9.4 Provisionamento de Containers:	
9.4.1 Deverá ser entregue uma plataforma de provisionamento de containers, integrada, a plataforma de virtualização.	https://www.nutanixbible.com/18a-book-of-cloud-native-services-nutanix-kubernetes-platform.html
9.4.2 A plataforma deverá permitir a criação de múltiplo clusters.	Nutanix-Kubernetes-Engine-v2_10.PDF
9.4.3 A fabricante da solução deverá, comprovadamente, pertencer a categoria de membro da CNCF (Cloud Native Computing Foundation).	https://www.nutanixbible.com/18-book-of-cloud-native-services.html
9.4.4 Seleção de sistemas operacionais, bem como suas distintas versões de microcódigo para implementação automática, sendo compatível com sistemas Linux.	Nutanix-Kubernetes-Engine-v2_10.PDF
9.4.5 Seleção das configurações de rede do cluster de containers ou microserviços.	Nutanix-Kubernetes-Engine-v2_10.PDF
9.4.6 Seleção do tipo de armazenamento persistente a ser empregado em containers.	Nutanix-Kubernetes-Engine-v2_10.PDF
9.4.7 Seleção da quantidade de nós dos tipos “Control Plane” e “Workers” que serão implementados simultaneamente.	Nutanix-Kubernetes-Engine-v2_10.PDF
9.4.8 A plataforma de containers deverá permitir a criação de alertas, facilitando a gestão do cluster.	Nutanix-Kubernetes-Engine-v2_10.PDF
9.4.9 Deverá ter suporte a implementação de clusters de plataformas de containers, similares a Kubernetes, NCI, baremetal, public cloud.	https://www.nutanix.com/products/cloud-platform/software-options#nkp
9.4.10 A plataforma de containers deverá possuir integração para o acesso através de RBAC, permitindo seu uso completo através de acesso administrativo e permitindo seu uso parcial através de acesso controlado aos demais usuários.	Nutanix-Kubernetes-Engine-v2_10.PDF
9.4.11 Suporte implementação de clusters de plataformas de containers, similares a Kubernetes com suporte a Bring-Your-Own-OS: Rocky Linux, Ubuntu, RHEL e similares.	https://www.nutanix.com/products/cloud-platform/software-options#nkp
9.4.12 Permitir a configuração de clusters com alta-disponibilidade para os “Control Plane” nodes, com ou sem balanceador de carga;	Nutanix-Kubernetes-Engine-v2_10.PDF
9.4.13 Prover armazenamento persistente através de integração com Container Storage Interface (CSI), para armazenamento de blocos e arquivos. Também deverá ser possível configurar armazenamento de arquivos compatível com protocolo Simple Storage Service;	Nutanix-Kubernetes-Engine-v2_10.PDF
9.4.14 Deverá fornecer um mecanismo de monitoramento que aciona alertas no cluster Kubernetes;	Nutanix-Kubernetes-Engine-v2_10.PDF
9.4.15 Oferecer as seguintes funcionalidades em ambiente Kubernetes:	Nutanix-Kubernetes-Engine-v2_10.PDF
9.4.15.1 Gerenciamento de Dados;	Nutanix-Kubernetes-Engine-v2_10.PDF
9.4.15.2 Proteção e Restauração de Dados;	Nutanix-Kubernetes-Engine-v2_10.PDF
9.4.15.3 Aceleração da Entrega de Aplicativos;	Nutanix-Kubernetes-Engine-v2_10.PDF

9.4.15.4 Gerenciamento de Autoatendimento de Aplicativos;	Nutanix-Kubernetes-Engine-v2_10.PDF
9.4.15.5 Automação e Monitoramento de Infraestrutura;	Nutanix-Kubernetes-Engine-v2_10.PDF
9.4.15.6 Padronização de Políticas de Governança e Conformidade;	Nutanix-Kubernetes-Engine-v2_10.PDF
9.4.16 Para a estratégia de criação de cópias dos dados para ambiente de containers Kubernetes, a solução deverá permitir:	Nutanix-Kubernetes-Engine-v2_10.PDF
9.4.16.1 Fornecimento de software para “worker nodes” Kubernetes, garantindo o suporte unificado e conjunto da solução como um todo;	Nutanix-Kubernetes-Engine-v2_10.PDF
9.4.16.2 Plataformas de container baseadas em Kubernetes.	Nutanix-Kubernetes-Engine-v2_10.PDF
9.4.16.3 Permitira realização de copias e armazenamento em repositório externo.	Nutanix-Kubernetes-Engine-v2_10.PDF
9.4.16.4 Movimentação das imagens de backup para compartilhamentos NFS por meio de solução de armazenamento compatível com protocolo S3, permitindo que o repositório NFS seja utilizado como backend de Object Storage.	Nutanix-Kubernetes-Engine-v2_10.PDF
9.4.16.5 Capacidade de restaurar o Namespace para seu local original e para um novo Namespace.	Nutanix-Kubernetes-Engine-v2_10.PDF
9.5 Segurança de Rede:	
9.5.1 Suportar microssegmentação para prover controle granular e governança de todo o tráfego de entrada e saída de uma máquina virtual (VM), grupos de máquinas virtuais (VMs) e containers	https://www.nutanixbible.com/12a-book-of-network-services-flow-network-security.html
9.5.2 Permitir a associação de políticas de rede a VMs e conteiners em vez de segmentos de rede específicos (por exemplo VLANs) ou identificadores (endereços IP ou MAC).	https://www.nutanixbible.com/12a-book-of-network-services-flow-network-security.html
9.5.3 Prover visualização de tráfego e relacionamentos com a descoberta automática dos fluxos entre as máquinas virtuais e containers.	https://www.nutanixbible.com/12a-book-of-network-services-flow-network-security.html
9.5.4 Permitir políticas de segurança centradas na carga de trabalho em vez de uma abordagem centrada na rede, permitindo examinar o tráfego de, e para as VMs, independentemente de como as configurações de rede mudam e onde residem no data center	Nutanix-Flow-Guide-v6_5.pdf
9.5.5 Políticas aplicadas por categorias de VMs e containers.	Nutanix-Flow-Guide-v6_5.pdf
9.5.6 Permitir isolamento de conteiners e VMs comprometidas, colocando-a em quarentena.	Nutanix-Flow-Guide-v6_5.pdf
9.5.7 - Permitir restrição de tráfego entre camadas de aplicação.	Nutanix-Flow-Guide-v6_5.pdf
9.5.8 Atualização automática de políticas.	Nutanix-Flow-Guide-v6_5.pdf
9.5.9 Integração com ferramentas de terceiros como IDS/IPS e load balancer.	ds-nutanix-flow.pdf
9.6 Licenciamento do Software de Virtualização:	
9.6.1 Entrega do licenciamento completo da plataforma de virtualização, versão mais avançada.	Ciente e de acordo / Conforme Proposta Tecnica
9.6.2 Suporte à criação de VMs com múltiplas interfaces de rede e múltiplas arquiteturas (32/64 bits).	AHV-Admin-Guide-v10_0.pdf; https://portal.nutanix.com/page/documents/compatibility-interoperability-matrix/guestos
9.6.3 Permitir provisionamento aos principais sistemas operacionais (Windows Server 2022, CentOS 8, Ubuntu 20, RHEL 9) ou superiores.	https://portal.nutanix.com/page/documents/compatibility-interoperability-matrix/guestos
9.6.4 Alocação dinâmica de recursos (CPU/RAM).	AHV-Admin-Guide-v10_0.PDF
9.6.5 Hypervisor deverá estar instalado em unidade flash dedicada.	System-Specs-NX8155G9.PDF
9.6.6 Suporte a GPU virtual ou passthrough nativo.	AHV-Admin-Guide-v10_0.pdf
9.6.7 Suporte a BIOS/UEFI, snapshots, exportação OVA.	AHV-Admin-Guide-v10_0.pdf
9.6.8 Deverá permitir o provisionamento de máquinas virtuais, e grupos de máquinas virtuais, em equipamentos específicos com o propósito de respeitar licenciamentos de aplicações. Em caso de falha do equipamento, a máquina virtual não deverá ser migrada para outro equipamento remanescente;	AHV-Admin-Guide-v10_0.pdf
9.6.9 Alta resiliência a falhas de nós/discos.	https://www.nutanixbible.com/4c-book-of-aos-storage.html
9.6.10 Armazenamento distribuído e gerenciado via console web.	https://www.nutanixbible.com/3b-book-of-prism-navigation.html Prism-Central-Guide-vpc_2024_3
9.6.11 Deverá permitir a inicialização, a reinicialização, o reset, o desligamento da VM e o desligamento do sistema operacional dela;	Prism-Central-Guide-vpc_2024_3
9.6.12 Suportar a tecnologia de snapshot nativos do Hypervisor;	Prism-Central-Guide-vpc_2024_3
9.6.13 Permitir a adição de novos servidores no cluster;	Prism-Central-Guide-vpc_2024_3

9.6.14 Permitir criar uma área de armazenamento compartilhada, distribuída e otimizada para ambientes virtuais;	Prism-Central-Guide-vpc_2024_3
9.6.15 Permitir o agrupamento dos volumes lógicos de todos os servidores no cluster provendo uma área de armazenamento comum para o ambiente virtual;	https://www.nutanixbible.com/4c-book-of-aos-storage.html
9.6.16 Possuir mecanismo de redundância e proteção de dados nativo que armazena cópias dos dados em diversos discos e hosts do cluster de forma transparente;	https://www.nutanixbible.com/4c-book-of-aos-storage.html
9.6.17 Deverá ser fornecido licenciamento do software de virtualização na versão mais completa para todos os servidores do ambiente de armazenamento distribuído.	Ciente e de acordo / Conforme Proposta Tecnica
9.6.18 Deverá contemplar pelo menos 20 (vinte) núcleos de processamento virtuais (vCPU) ou físicos (pCPU) de solução para gestão de base de dados como serviço (DBaaS).	Ciente e de acordo / Conforme Proposta Tecnica
9.6.19 Deverá ser totalmente compatível com a solução ofertada para atendimento aos requisitos deste termo de referência.	Ciente e de acordo / Conforme Proposta Tecnica
9.6.20 Permitir automatizar as tarefas para provisionamento, emprego de correções de software (patching), gerenciamento do ciclo de vida, clonagem, atualização dos dados em bases clonadas (refresh), proteção contínua e recuperação de bases de dados.	https://www.nutanix.com/products/database-service
9.6.21 Deverá ser compatível pelo menos com Oracle, Microsoft SQL, PostgreSQL, MariaDB, MongoDB e MySQL.	https://www.nutanix.com/products/database-service
9.6.22 Permitir o uso de uma chave SSH pública para acesso ao servidor de banco de dados com opção através do upload de um arquivo e através da inserção direta da chave em campo de texto.	NVD-2155-Nutanix-Databases.pdf
9.6.23 A solução deverá permitir registrar bancos de dados existentes para emprego de proteção contínua capturando e mantendo snapshots e registros (logs) transacionais da base de dados de origem conforme definições contidas no agendamento.	https://www.nutanix.dev/2022/09/29/nutanix-benefit-8-integrated-self-service-database-management/
9.6.24 A mesma tecnologia deverá permitir a clonagem de bases de dados.	NVD-2155-Nutanix-Databases.pdf
9.6.25 Durante a clonagem, a solução deverá permitir a escolha para o administrador utilizar um servidor de banco de dados registrado ou criar um novo servidor.	NVD-2155-Nutanix-Databases.pdf
9.6.26 Permitir que o administrador realize o clone de uma base de dados a partir de um snapshot.	https://www.nutanix.dev/2022/09/29/nutanix-benefit-8-integrated-self-service-database-management/
9.6.27 Permitir que o administrador realize o clone de uma base de dados dentro de uma política de proteção contínua, ou seja, clonar uma base de dados em determinado dia, hora, minuto e segundo.	NVD-2155-Nutanix-Databases.pdf
9.6.28 Permitir a definição de agendamento da periodicidade para realizar a atualização (refresh) dos dados da base clonada através do estado atual na base de dados de origem	https://www.nutanix.dev/2022/09/29/nutanix-benefit-8-integrated-self-service-database-management/
9.6.29 Permitir a definição de uma data para remoção ou exclusão do clone.	NVD-2155-Nutanix-Databases.pdf
9.6.30 Permitir a execução de scripts ou comandos de pré e pós clonagem.	NVD-2155-Nutanix-Databases.pdf
9.6.31 Deverá ser possível definir as políticas de retenção dos snapshots diários, semanais, mensais e trimestrais.	https://www.nutanix.dev/2022/09/29/nutanix-benefit-8-integrated-self-service-database-management/
10. ITEM 04 – SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU	
10.1 Software para Processamento Gráfico e Cálculo Aritmético:	
10.1.1 Permitir a seleção, implantação e gestão de modelos de IA Generativa (LLMs) provenientes da Hugging Face e NVIDIA, bem como a importação de modelos personalizados ou treinados pelo contratante em clusters Kubernetes.	https://www.nutanixbible.com/20a-nutanix-enterprise-ai.html
10.1.10 Permitir a criação de um endpoint de inferência e o compartilhamento dele com desenvolvedores para incorporar em seus aplicativos de IA. Permitir gerenciar e validar esses endpoints para garantir que eles estejam configurados corretamente.	https://www.nutanixbible.com/20a-nutanix-enterprise-ai.html
10.1.11 Permitir o acesso a um endpoint de inferência por um aplicativo usando chaves de API. O gerenciamento de chaves de API deverá permitir o fornecimento e revogação do acesso à API para garantir controles de segurança de acesso adequados.	https://www.nutanixbible.com/20a-nutanix-enterprise-ai.html
10.1.12 Permitir o controle de acesso baseado em função (RBAC), para fornecer permissões de acesso personalizadas aos usuários com base em suas funções atribuídas.	https://www.nutanixbible.com/20a-nutanix-enterprise-ai.html
10.1.13 Possuir uma interface de usuário simples e dinâmica que simplifique o processo de implantação.	https://www.nutanixbible.com/20a-nutanix-enterprise-ai.html

10.1.14 Possuir um painel dinâmico que permita monitorar a integridade da implantação com ferramentas de monitoramento em tempo real que identifiquem gargalos, rastreiem o desempenho e solucionem problemas.	https://www.nutanixbible.com/20a-nutanix-enterprise-ai.html
10.1.15 Suportar a instalação e o funcionamento em estruturas sem qualquer conexão com a Internet (dark-site ou air-gapped).	https://www.nutanixbible.com/18a-book-of-cloud-native-services-nutanix-kubernetes-platform.html
11. ITEM 05 - LICENÇA PARAARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE	
11.1 A solução deverá incluir unidade de subscrição de software para armazenamento de objetos e arquivos, licenciada por terabyte (TB), com suporte técnico durante 60 (sessenta) meses, contemplando ambiente de produção em operação contínua (24x7).	Ciente e de acordo / Conforme Proposta Tecnica
11.2 Caso a solução proposta não ofereça suporte nativo a armazenamento de objetos e arquivos, será permitida a utilização de unidade externa dedicada, desde que esta disponha de todos os componentes, funcionalidades e suporte equivalentes à solução principal.	Não se Aplica
11.3 O sistema de armazenamento definido (SDS) deverá otimizar dados utilizando tecnologia de erasure coding na camada de capacidade, de modo a garantir eficiência e resiliência no armazenamento de arquivos e objetos.	https://www.nutanixbible.com/4c-book-of-aos-storage.html
11.4 A solução deverá permitir a recuperação granular de arquivos pelos usuários, sem necessidade de intervenção do administrador.	7A.pdf
11.4.1 Para o protocolo SMB, a restauração deverá ocorrer por meio da funcionalidade “Versões Prévias” da pasta de destino.	7A.pdf
11.4.2 Para o protocolo NFS, a recuperação deverá ser possível pela listagem do subdiretório oculto (snapshot).	7A.pdf
11.5 O sistema deverá integrar-se a softwares antivírus de terceiros por meio do protocolo ICAP (Internet Content Adaptation Protocol), possibilitando varredura em tempo real de arquivos compartilhados via SMB sempre que forem abertos, modificados ou encerrados.	7A.pdf / 7C.pdf
11.6 A interface de gerenciamento deverá exibir o estado dos arquivos após a varredura antivírus, incluindo status como limpo, em quarentena ou deletado, além do histórico de eventos correspondentes.	7A.pdf
11.7 A interface de gerenciamento deverá também exibir relatórios detalhados contendo a lista de arquivos analisados, ameaças detectadas e arquivos colocados em quarentena.	7A.pdf
11.8 A interface de gerenciamento deverá permitir ações diretas sobre os arquivos, incluindo:	
11.8.1 Reexecução de varredura (Rescan);	7A.pdf
11.8.2 Remoção de arquivos da quarentena;	7A.pdf
11.8.3 Exclusão permanente de arquivos em quarentena.	7A.pdf
11.9 A solução deverá possibilitar a configuração de ambiente de detecção avançada de intrusão (AIDE), capaz de identificar e corrigir automaticamente desvios na configuração de segurança do servidor de arquivos, sem necessidade de intervenção manual.	7A.pdf
11.10 Deverá ser possível configurar políticas de senha forte (strong password) para o acesso à linha de comando (CLI) do servidor de arquivos.	7A.pdf
11.11 O sistema deverá suportar configuração de qualidade de serviço (QoS), utilizando valores DSCP para diferenciação de códigos de serviço em rede.	7A.pdf
11.12 Deverá suportar o protocolo NFS v4.2, otimizando as operações de entrada/saída (I/O) e reduzindo o consumo de rede.	7A.pdf / 7C.pdf
11.13 A solução deverá contemplar as seguintes funcionalidades para compartilhamento de arquivos via protocolo SMB:	
11.14 Autenticação integrada ao Active Directory.	7C.pdf
11.15 Enumeração baseada em acesso (ABE), exibindo apenas pastas e arquivos aos quais o usuário possui permissão.	7A.pdf
11.16 Assinatura digital de pacotes SMB (SMB Signing), garantindo autenticidade e integridade das transmissões.	7A.pdf
11.17 Criptografia em nível de pasta (SMB Encryption), assegurando a confidencialidade dos dados.	7C.pdf

11.18 Organização de compartilhamentos em um único espaço de nomes (Single Namespace), suportando ambientes locais ou geograficamente distribuídos, por meio do protocolo DFS-N (DFS Namespaces).	7C.pdf
11.19 Suporte à autenticação via Active Directory e LDAP, além de acesso não gerenciado a compartilhamentos NFSv4 (autenticação LDAP) e NFSv3.	7C.pdf
11.20 Suporte a acesso multiprotocolo (SMB e NFS) sobre o mesmo compartilhamento, preservando permissões via Windows ACLs e Unix mode bits.	7C.pdf
11.21 Suporte a Home Shares por diretório, permitindo o provisionamento automático de pastas pessoais de usuário.	7A.pdf
11.22 Suporte à aplicação de cotas de uso do sistema de arquivos, com notificações (soft limit) e bloqueio (hard limit), configuráveis por usuário, grupo ou diretório no momento da criação (Directory Level Quotas).	7A.pdf
11.23 O módulo de armazenamento de objetos deverá possuir API REST compatível com AWS S3, apta a lidar com petabytes de dados não estruturados, atendendo casos de uso como backup, retenção de longo prazo e aplicações nativas de nuvem.	7E.pdf
11.24 Deverá permitir que os usuários armazenem e gerenciem dados não estruturados em arquitetura de nuvem privada escalável.	7E.pdf
11.25 A solução deverá permitir a gestão de objetos via interface gráfica de administração e via API REST compatível com S3, mediante autorização prévia do administrador	7E.pdf
11.26 Suportar integração com serviços de diretório (Microsoft Active Directory e OpenLDAP), possibilitando o controle de acesso a objetos.	7E.pdf
11.27 Permitir o compartilhamento de buckets com usuários portadores de chaves de acesso, com delegação de permissões de leitura e escrita conforme o nível definido.	7E.pdf
11.28 Exibir a listagem de buckets compartilhados, indicando os respectivos usuários com acesso.	7E.pdf
11.29 Permitir o gerenciamento de buckets e objetos por meio de APIs REST compatíveis com a solução de gerenciamento central ou S3, mediante autorização administrativa.	7E.pdf
11.30 Suportar o versionamento de múltiplas versões de um mesmo objeto dentro de um bucket.	7E.pdf
11.31 Possibilitar a definição de regras de ciclo de vida, como exclusão automática de objetos ou versões após período determinado (dias, meses ou anos)	7E.pdf
11.32 Implementar mecanismo de proteção contra exclusão ou alteração de objetos, com base em políticas de retenção WORM (Write-Once-ReadMany).	7E.pdf
11.33 Disponibilizar painel de monitoramento de desempenho, apresentando requisições por segundo, taxa de banda (MB/s) e tempo médio de leitura (GET).	7E.pdf
11.34 Suportar políticas de cotas de utilização, notificando usuários conforme o consumo de espaço ou número de buckets criados.	7E.pdf
11.35 Suportar o envio de notificações em tempo real — como criação, deleção, leitura, gravação ou alteração de permissões — para fins de auditoria e retenção, compatível com servidores syslog ou sistemas equivalentes.	7E.pdf
12. ITEM 06 - SOFTWARE DE BACKUP DE DADOS	
12.1 Características Gerais do Licenciamento:	
12.1.1 Aquisição de 200 (duzentas) licenças pelo período de 05 (cinco) anos ou 60 (sessenta) meses.	Ciente e de acordo / Conforme Proposta Tecnica
12.1.2 Não deverão existir limites quanto ao uso de agentes, conectores, repositórios de armazenamento, hosts físicos e outras tecnologias agregadas a arquitetura da solução especificada.	
12.1.3 Ser a última versão disponível, não será aceita a utilização de versões anteriores para cobrir algum item desse descritivo técnico.	Ciente e de acordo / Conforme Proposta Tecnica
12.1.4 Mostrar na console de gerenciamento a quantidade de licenças adquiridas e utilizadas.	https://helpcenter.veeam.com/docs/vbr/userguide/view_license_console.html?ver=13
12.1.5 Caso a solução ofertada necessite de algum banco de dados, o mesmo deverá ser fornecido devidamente licenciado sem nenhum custo extra.	Ciente e de acordo / Conforme Proposta Tecnica
12.1.6 A solução deve ser compatível com o Item 07 Equipamento de Armazenamento de Dados de Backup on-premises.	https://www.exagrid.com/pt/exagrid-products/supported-data-backup-applications/veeam-backup/

12.2 Cópia e Restauração de Dados:	
12.2.1 Permitir o controle da banda utilizada durante a operação de cópia de proteção dos backups.	tps://helpcenter.veeam.com/docs/agentforwindows/userguide/settings_network_bandwidth.html?ver=13
12.2.2 Ser capaz de realizar cópia de arquivos abertos sem que a consistência deles seja comprometida.	https://helpcenter.veeam.com/docs/vbr/userguide/application_aware_processing.html?ver=13
12.2.3 Possuir a opção de priorização de tarefas de proteção com opção de resumo da cópia caso uma atividade de menor prioridade seja colocada em estado de espera por uma tarefa de maior prioridade.	https://helpcenter.veeam.com/docs/vbr/userguide/job_priorities.html?ver=13
12.2.4 Possuir a funcionalidade de paralelizar a gravação dos dados em dispositivos de armazenamento (funcionalidade conhecida como multiplexação).	https://helpcenter.veeam.com/docs/vbr/userguide/enabling_multithreaded_transfer.html?ver=13
12.2.5 Ser capaz de enviar alertas através de e-mail com o objetivo de reportar eventos ocorridos na operação e configuração da solução.	https://helpcenter.veeam.com/docs/vbr/userguide/general_email_notifications.html?ver=13
12.2.6 Ser capaz de enviar traps SNMP (Simple Network Management Protocol) com o objetivo de reportar eventos ocorridos na operação da solução.	https://helpcenter.veeam.com/docs/vbr/userguide/snmp_settings.html?ver=13
12.2.7 Possuir a funcionalidade de agendamento automático de tarefas de cópia.	
12.2.8 Para um mesmo dado armazenado deve haver a possibilidade de configuração de diferentes períodos de retenção.	https://helpcenter.veeam.com/docs/vbr/userguide/backup_copy_retention.html?ver=13
12.3 Gerenciamento das Operações de Proteção e Restauração:	
12.3.1 Possuir interface única, que seja capaz de gerenciar e executar operações de proteção e recuperação dos sistemas operacionais Windows, Unix e Linux; ambiente de virtualização Acropolis Operating System; aplicações, Microsoft Active Directory e banco de dados Microsoft SQL Server, PostgreSQL e Oracle.	http://helpcenter.veeam.com/docs/vbr/userguide/vbr_ui.html?ver=13
12.3.2 O acesso administrativo ao console do servidor de gerenciamento da solução poderá ser feito através de ferramenta disponibilizada no próprio software (console gráfico) ou através de navegador Web.	https://helpcenter.veeam.com/docs/vbr/userguide/ui.html?ver=13
12.3.3 Implementar distribuição automática de carga entre os movimentadores de dados, ou seja, os dados oriundos dos clientes de backup deverão ser distribuídos de forma automática entre os servidores de cópia, e em caso de falha de um dos servidores, o cliente automaticamente irá encaminhar seus dados para o outro servidor de cópia ativo. Esta funcionalidade deverá ser nativa do produto, e não pode ser construída com o uso de soluções baseadas em softwares de cluster de terceiros.	https://helpcenter.veeam.com/docs/vbr/userguide/backup_proxy.html?ver=13
12.3.4 A base de dados para armazenamento do catálogo deverá possuir mecanismo de proteção (backup) das informações armazenadas no catálogo e funcionalidades de recuperação rápida do catálogo em caso de desastre.	https://helpcenter.veeam.com/docs/vbr/userguide/vbr_config.html?ver=13
12.4 Criptografia dos Dados Protegidos	
12.4.1 Implementar criptografia de dados na origem (cliente de backup), de uma forma que seja garantido que o dado que trafegará na rede de modo criptografado.	https://helpcenter.veeam.com/docs/vbr/userguide/encryption_hiw.html?ver=13
12.4.2 Deverá implementar no mínimo chaves de criptografia de 128 bits ou 256 bits.	https://helpcenter.veeam.com/docs/vbr/userguide/encryption_hiw.html?ver=13
12.5 Desduplicação dos Dados Protegidos	
12.5.1 Permitir uso da tecnologia de desduplicação de dados para toda a capacidade licenciada, eliminando blocos repetidos, para cópias e arquivamento em disco e movimentação de dados desduplicados, independentemente do quantitativo de dispositivos de armazenamento que compõem a infraestrutura da CONTRATANTE.	https://helpcenter.veeam.com/docs/vbr/userguide/compression_deduplication.html?ver=13
12.5.2 Implementar desduplicação de blocos na origem (client-side desduplication), de forma que o cliente envie apenas novos blocos de dados criados e/ou modificados a partir da última cópia total completa;	https://helpcenter.veeam.com/docs/vbr/userguide/compression_deduplication.html?ver=13
12.5.3 Implementar desduplicação de dados nos servidores de armazenamento (target desduplication), de forma que tais servidores tratem adequadamente blocos repetidos enviados pelos clientes, evitando assim o armazenamento de blocos redundantes;	https://helpcenter.veeam.com/docs/vbr/userguide/compression_deduplication.html?ver=13
12.5.4 Implementar desduplicação de dados em tarefas de cópia;	erguide/backup_copy_settings_storage.html?ver=13 / https://helpcenter.veeam.com/docs/vbr/userguide/compression_deduplication.html?ver=13
12.5.5 Implementar desduplicação e compressão em uma mesma tarefa;	https://helpcenter.veeam.com/docs/vbr/userguide/compression_deduplication.html?ver=13
12.5.6 Permitir a restauração granular de arquivos ou sistemas de arquivos a partir de cópias em disco ou fita. Em caso de backup armazenado em disco a recuperação granular poderá ser feito utilizando-se cópias que possam estar desduplicados;	https://helpcenter.veeam.com/docs/vbr/userguide/integration_flr.html?ver=13
12.6 Alertas e Relatórios da Proteção de Dados	

12.6.1 Quantidade de rotinas de backup concluídos nas últimas 24 horas, nos últimos 30 dias e nos últimos 12 meses.	https://helpcenter.veeam.com/docs/one/userguide/data_retention.html?ver=13
12.6.2 Quantidade de recuperações efetuadas nas últimas 24 horas, nos últimos 30 dias e nos últimos 12 meses.	https://helpcenter.veeam.com/docs/one/userguide/data_retention.html?ver=13
12.6.3 Resumo de rotinas de backup concluídos com sucesso, com erro ou não concluídos.	https://helpcenter.veeam.com/docs/vbr/userguide/session_results_web.html?ver=13
12.6.4 Mostrar o total de licenças adquiridas e o total de licenças utilizadas e caso ocorra uma nova aquisição de licenças as novas licenças deverão constar nesse relatório.	https://helpcenter.veeam.com/docs/vbr/userguide/view_license_console.html?ver=13
12.6.5 Enviar os seguintes alertas via e-mail: rotina de backup finalizada com sucesso, rotina de backup finalizada com erro e rotina de backup com problema.	https://helpcenter.veeam.com/docs/vbr/userguide/general_email_notifications.html?ver=13
12.7 Fornecimento de licenciamento do Sistema Operacional	
12.7.1 Fornecimento de licenciamento do sistema operacional Microsoft Windows Server Datacenter, baseado em núcleo (core-based licensing , para 48 cores físicos)	Ciente e de acordo / Conforme Proposta Tecnica
12.7.2 As licenças deverão ser entregues em formato eletrônico, acompanhadas de instruções para instalação e ativação, devendo incluir garantia mínima de 60 (sessenta) meses ou suporte técnico equivalente.	Ciente e de acordo / Conforme Proposta Tecnica
12.7.3 O licenciamento deverá ser compatível com servidores físicos e virtuais , observando o licenciamento mínimo exigido pela fabricante.	Ciente e de acordo / Conforme Proposta Tecnica
12.7.4 As licenças fornecidas deverão ser originais, legítimas e adquiridas por meio de canal autorizado da Microsoft, com comprovação documental no momento da entrega.	Ciente e de acordo / Conforme Proposta Tecnica
12.7.5 As licenças deverão ser entregues em formato eletrônico, acompanhadas de instruções para instalação e ativação, incluindo garantia mínima de 60 (sessenta) meses ou suporte técnico equivalente.	Ciente e de acordo / Conforme Proposta Tecnica
12.7.6 O item deverá ser plenamente compatível com a infraestrutura tecnológica do MPAM, em especial com ambientes físicos e virtuais já existentes.	Ciente e de acordo / Conforme Proposta Tecnica
12.7.7 Incluir Software Assurance (SA), garantindo direito a atualizações, suporte técnico estendido e benefícios de mobilidade de licenças durante todo o período contratual.	Ciente e de acordo / Conforme Proposta Tecnica
13. ITEM 07 - EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	
13.1 Características gerais:	
13.1.1 Deverá corresponder a um sistema inteligente dedicado ao armazenamento de backups em disco, com funcionalidades integradas de criptografia, compressão, desduplicação e replicação dos dados já desduplicados;	Descrição Detalhada do Produto ExaGrid
13.12 O equipamento deve estar listado no site oficial do fabricante como um appliance ou sistema de armazenamento de backup em disco, em produção ativa;	Especificações Técnicas do ExaGrid
13.1.3 O hardware e o software devem ser do mesmo fabricante. Não serão aceitas soluções customizadas especificamente para esta licitação, nem combinações OEM, equipamentos usados, recondicionados, de demonstração ou gateways;	Descrição Detalhada do Produto ExaGrid
13.1.4 O equipamento deve ser novo, sem uso anterior, pertencente à linha mais recente do fabricante, em produção contínua e sem previsão de fim de suporte (EOSL) nos próximos cinco anos a partir da data de abertura da licitação;	ExaGrid Product Line
13.1.5 Soluções baseadas exclusivamente em software (appliances virtuais) não serão aceitas;	Não se Aplica
13.1.6 Deve ser compatível com montagem em racks padrão de 19”, acompanhado de trilhos, cabos, conectores, manuais e todos os itens necessários para instalação, configuração e operação completa;	Especificações Técnicas do ExaGrid
13.1.7 Para soluções com arquitetura Scale-Out:	Descrição Detalhada do Produto ExaGrid
13.1.7.1 Deve permitir conexão com outros sistemas do mesmo fabricante para expansão de desempenho e capacidade;	https://www.exagrid.com/wp-content/uploads/ExaGrid-Detailed-Product-Description_DS.pdf
13.1.7.2 Deve operar em modo ativo-ativo (alta disponibilidade com balanceamento de carga), redirecionando automaticamente os backups em caso de falha de um dos sistemas;	Descrição Detalhada do Produto ExaGrid
13.1.8 Para soluções com arquitetura Scale-Up:	Não se Aplica
13.1.8.1 Deve incluir duas controladoras, operando em modo ativo-ativo ou ativo-passivo, garantindo continuidade das operações de backup em caso de falha de uma das controladoras.	-
13.2 Requisitos de disponibilidade:	-

13.2.1 Deve possuir tolerância a falhas em componentes como discos, fontes de alimentação e ventiladores;	Especificações Técnicas do ExaGrid
13.2.2 Deve contar com mecanismos que assegurem a integridade dos dados mesmo em casos de interrupção abrupta ou desligamento acidental;	Descrição Detalhada do Produto ExaGrid
13.2.3 Deve incluir proteção de cache de escrita para evitar perda de dados em caso de falha de energia;	Especificações Técnicas do ExaGrid
13.2.4 Deve ser entregue com arranjos RAID-6, RAID-DP ou equivalente, com tolerância a falha de até dois discos e pelo menos um disco hotspare por grupo RAID;	Descrição Detalhada do Produto ExaGrid
13.2.5 Os discos devem ser hot-pluggable e hot-swappable, permitindo substituição sem interrupção do sistema;	Descrição Detalhada do Produto ExaGrid
13.2.6 Deve oferecer monitoramento remoto pelo fabricante, com recursos como Call-Home para detecção proativa de falhas ou pré-falhas.	ExaGrid Standard Customer Support & Maintenance
13.3 - Capacidade, desempenho e conectividade:	
13.3.1 Deve oferecer no mínimo 100 (cem) TB de capacidade útil, sem considerar compressão, desduplicação ou espaço reservado ao sistema;	ExaGrid Product Line
13.4 Para soluções Scale-Out:	ExaGrid Detailed Product Description
13.4.1 Deve atingir taxa mínima de 5 TB/hora (cinco terabytes por hora) para operações de backups, sem considerar desduplicação;	ExaGrid Product Line
13.4.2 Capacidade de ampliar a solução previamente fornecida, através da interconexão de módulos similares ou não, do mesmo fabricante. Para a expansão, volumes em nuvem, off-site, replicação ou similar para o atendimento a este requisito não serão aceitos, mantendo a característica de desduplicação global da solução	ExaGrid Product Line
13.4.3 A criptografia deve ser feita via hardware. Caso seja por software, a taxa de transferência deve ser 30% superior à mínima exigida, considerando apenas a desduplicação.	https://www.exagrid.com/exagrid-products/comprehensive-security/
13.5 Para soluções Scale-Up:	Não se Aplica
13.5.1 Deve permitir expansão para pelo menos 500 TB (quinhentos terabytes) de capacidade útil, sem considerar compressão ou desduplicação, por meio de gavetas de discos, sem troca ou upgrade das controladoras originais, mantendo a desduplicação global;	-
13.5.2 Deve atingir taxa mínima de 15 TB/hora (quinze terabytes por hora) para operações de backup, considerando apenas a desduplicação;	-
13.5.3 A criptografia deve ser realizada por hardware. Se for por software, a taxa de transferência deve ser 30% superior à exigida, considerando apenas a desduplicação;	-
13.5.4 Deve incluir no mínimo duas interfaces de rede de 25 Gbps com conectores SFP28 para backup via LAN, fornecidos com o equipamento;	-
13.5.5 Deve incluir pelo menos duas interfaces de 1 GbE com conectores UTP CAT6 para gerenciamento, também fornecidos;	-
13.5.6 Deve possuir ao menos uma porta IPMI/iLO/iDRAC ou equivalente;	-
13.5.7 Interfaces adicionais devem ser fornecidas conforme as melhores práticas do fabricante para garantir o desempenho requerido;	-
13.5.8 Fornecer a quantidade necessária de discos para atingimento da performance mínima solicitada, ou seja, se a solução requerer mais discos além dos necessários para atender a capacidade solicitada no item 8.3.1, discos adicionais deverão ser fornecidos. Não é obrigatório o licenciamento de capacidade desses discos adicionais	-
13.5.9 Comprovar a taxa de transferência através da ferramenta de dimensionamento do fabricante da solução, desconsiderando o uso de ferramentas/protocolos de otimizações na origem no seu dimensionamento, caso a solução ofertada não seja fornecida com todos os discos possíveis para sua capacidade total.	-
14. ITEM 08 - SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	
14.1 Características gerais	
14.1.1 Permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, de maneira perpétua, irrestrita e sem necessidade de licenciamentos ou ônus adicionais;	Ciente e de acordo / Conforme Proposta Tecnica

14.1.2 -Possuir licenças na modalidade de uso perpétuo para todo para o completo atendimento das especificações técnicas do equipamento, ou seja, o equipamento deverá continuar a operar normalmente mesmo após o período de manutenção e assistência técnica contratado;	Ciente e de acordo / Conforme Proposta Tecnica
14.1.3 Para soluções com arquitetura Scale-Out:	
14.1.3.1 A desduplicação de dados deve ser mantida de forma global em todo o ambiente de armazenamento, independentemente da quantidade de dispositivos interligados;	ExaGrid Global Deduplication
14.1.4 Para soluções com arquitetura Scale-Up:	Não se Aplica
14.1.4.1 A desduplicação global deve ser preservada em todo o conjunto de armazenamento.	-
14.2 Requisitos de compatibilidade:	-
14.2.1 O software deve ser homologado e plenamente compatível com o software de backup fornecido no ITEM 06 - SOFTWARE DE BACKUP DE DADOS;	https://www.exagrid.com/wp-content/uploads/ExaGrid-Detailed-Product-Description_DS.pdf
14.2.2 Deve permitir leitura e gravação simultâneas via protocolos CIFS, NFS e OST;	https://www.exagrid.com/wp-content/uploads/ExaGrid-Detailed-Product-Description_DS.pdf
14.2.3 Deve oferecer suporte aos protocolos de monitoramento SNMP e Syslog;	https://www.exagrid.com/wp-content/uploads/ExaGrid-Detailed-Product-Description_DS.pdf
14.2.4 Deve possibilitar que aplicações como Oracle (via RMAN) e Microsoft SQL realizem backups tipo Stream Based (Oracle Stream Backup) e “database dump” diretamente no equipamento, por meio de CIFS e NFS, sem uso de software de backup, evitando o consumo de licenças e sem necessidade de licenciamento por volume (TB) ou por servidor (CPU, Core, Tier). Caso essa funcionalidade exija licenciamento, todos os itens necessários devem ser incluídos na proposta.	https://www.exagrid.com/wp-content/uploads/ExaGrid-Detailed-Product-Description_DS.pdf
14.3 - Funcionalidades operacionais:	
14.3.1 Deve permitir a execução simultânea de processos de backup e restore;	ExaGrid Performance
14.3.2 Deve dispor de interface de gerenciamento baseada em navegador (WEB);	ExaGrid Management
14.3.3 A desduplicação deve ser global, mesmo com volumes lógicos distintos, identificando dados redundantes entre diferentes fontes de backup e armazenando-os apenas uma vez;	ExaGrid Deduplication ExaGrid Inline Deduplication
14.3.4 A desduplicação deve ocorrer em conjunto com os processos de backup e restore, sem necessidade de janelas específicas;	https://www.exagrid.com/wp-content/uploads/ExaGrid-Detailed-Product-Description_DS-4.pdf ExaGrid Data Integrity
14.3.5 Deve incluir mecanismos nativos para verificação da integridade dos dados desduplicados, com capacidade de correção automática em caso de inconsistência, sem uso de scripts externos;	https://www.exagrid.com/wp-content/uploads/ExaGrid-Detailed-Product-Description_DS-4.pdf
14.3.6 Deve permitir replicação de dados via rede IP (LAN/WAN), de forma assíncrona, entre sistemas compatíveis do mesmo fabricante, utilizando desduplicação para otimizar o uso da banda;	Ciente e de acordo / Conforme Proposta Tecnica
14.3.7 Deve suportar topologias de replicação como 1:1, 1:N, N:1 e o cascateamento de equipamentos;	ExaGrid Replication Topologies
14.3.8 Deve integrar-se ao Microsoft Active Directory 2012 ou superior, para autenticação e controle de acesso;	ExaGrid Active Directory
14.3.9 Os dados armazenados devem ser criptografados com algoritmos de no mínimo AES128-SHA ou AES256-SHA;	ExaGrid Security
14.3.10 Deve permitir autenticação em dois fatores (2FA), com integração a soluções OTP como Google Authenticator, Microsoft Authenticator ou equivalentes;	ExaGrid Two-Factor Authentication (pagina 3)
14.3.11 Caso a solução exija um sistema OTP específico com licenciamento ou hardware dedicado (ex: Common Access Card /Personal Information Verification cards, sistemas de OTP/tokenização licenciados, etc), todos os componentes necessários devem ser fornecidos para pelo menos 5 usuários;	
14.3.12 Deve oferecer recurso de autorização dupla (Dual Auth) para alterações em configurações de proteção contra ransomware;	ExaGrid Ransomware Protection

14.3.13 Deve incluir funcionalidades avançadas de segurança cibernética para proteção contra ransomware, assegurando a integridade dos dados de backup;	ExaGrid Ransomware Protection
14.4 - Deve possuir mecanismo de imutabilidade dos dados:	ExaGrid Immutable Data
14.4.1 A proteção deve estar sempre ativa, independente do software de backup, sem necessidade de janelas específicas ou scripts;	ExaGrid Security
14.4.2 A proteção deve ser aplicada imediatamente após a desduplicação dos dados, sem depender de agendamento;	ExaGrid Immutable Data
14.4.3 Deve adotar o conceito de air-gap, tornando os dados protegidos invisíveis à rede e inacessíveis por softwares de backup, independentemente do protocolo utilizado.	ExaGrid Air-Gap Technology
15. ITEM 09 – SWITCH CORE	
15.1 Especificações Físicas	
15.1.1 O equipamento deve contar com, no mínimo, 48 portas SFP28 compatíveis com velocidades de 1, 10 e 25 Gigabit Ethernet.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.1.2 As interfaces devem ser auto-sensíveis, ajustando automaticamente a velocidade conforme o transceiver conectado, sem necessidade de configuração manual.	https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/statement/auto-sense-edit-protocols-bgp-group-link-bandwidth.html#protocols-bgp-group-link-bandwidth-auto-sense-statement__d398817e100
15.1.3 A altura máxima permitida é de 1 unidade de rack (1 RU).	https://www.juniper.net/us/en/products/switches/qfx-series/qfx5120-data-center-switches/specs.html
15.1.4 Deve ser compatível com racks padrão de 19 polegadas, incluindo os kits de fixação apropriados.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.1.5 As portas SFP28 devem aceitar transceivers dos tipos SFP+ 10GBase-SR, 10GBase-LR, 10GBase-ER, SFP 1000Base-SX, 1000Base-LX, 1000Base-ZX, 1000Base-T e cabos DAC.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.1.6 Devem ser entregues ao menos 10 cabos DAC 25GbE SFP28 com comprimento mínimo de 3 metros, compatíveis com os appliances do item 1.	Ciente e de acordo / Conforme Proposta Tecnica
15.1.7 O switch deve possuir pelo menos 6 portas QSFP28 de 100GbE, com suporte a velocidades de 40GbE.	Ciente e de acordo / Conforme Proposta Tecnica
15.1.7.1 Deve ser compatível com transceivers 40GBase-SR4 e 40GBase-LR4.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.1.7.2 Deve aceitar transceivers 100GBase-SR4 e 100GBase-LR4.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.1.7.3 Deve suportar cabos DAC.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.1.8 Deve acompanhar pelo menos 1 cabo DAC 100GbE com no mínimo 1 metro de comprimento, para conexão redundante entre switches.	Ciente e de acordo / Conforme Proposta Tecnica
15.1.9 A capacidade da matriz de comutação deve ser de no mínimo 4 Tbps.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.1.10 O throughput mínimo exigido é de 1,5 Bpps.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.1.11 O buffer deve ter capacidade mínima de 32 MB.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.1.12 A latência máxima permitida é de 900 nanosegundos.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.1.13 Deve suportar ao menos 160.000 endereços MAC.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.1.14 A tabela ARP deve comportar até 64.000 entradas ou mais.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.1.15 Deve aceitar jumbo frames com tamanho mínimo de 9000 bytes.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.1.16 É obrigatória a presença de pelo menos uma porta RJ-45 para gerenciamento fora de banda.	Ciente e de acordo / Conforme Proposta Tecnica
15.1.17 O equipamento deve vir com CPU e memória (RAM e Flash) suficientes para suportar todas as funcionalidades descritas.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.1.18 Fontes de alimentação internas devem ser redundantes e com ajuste automático para 110/220V.	

15.1.19 O sistema de ventilação deve ser redundante, com fluxo de ar configurável (frontal-traseiro ou traseiro-frontal), sendo fornecido com ventiladores de fluxo frontal-traseiro	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf	
15.1.20 Fontes e ventiladores devem ser hot-swappable e redundantes, permitindo substituição sem interrupção.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf	
15.1.21 O equipamento deve ser projetado para ambientes de datacenter, com comutação de pacotes de alto desempenho.	Ciente e de acordo / Conforme Proposta Tecnica	
15.2 - Funcionalidades Gerais		
15.2.1 LEDs por porta devem indicar status e atividade do link.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf	
15.2.2 A arquitetura da solução deve ser baseada em “spine-leaf”, com VxLAN como plano de dados e BGP EVPN como plano de controle.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf	
15.2.3 Deve possuir porta de console para configuração via CLI, com conector RJ-45 ou RS-232, incluindo cabos e adaptadores necessários.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf	
15.2.4 Gerenciamento via SSHv2 deve ser suportado.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf	
15.2.5 O switch deve ter criptografia FIPS 140-2 validada pelo NIST.	https://www.juniper.net/documentation/us/en/software/ccfips20.2/fips-switches-qfx5120-qfx5210-ex4650/fips-switches/topics/task/fips-mode-enable.html	
15.2.6 Deve permitir espelhamento de uma ou mais portas para outra porta específica.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf	
15.2.7 Também deve permitir espelhamento para porta remota via tunelamento, mesmo em domínios L2 distintos.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf	
15.2.8 Deve implementar Netflow, sFlow ou tecnologia equivalente.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf	
15.2.9 Gerenciamento via SNMPv3 deve ser possível.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf	
15.2.10 Deve suportar o protocolo Syslog.	https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/statement/syslog-edit-interfaces-multiservice-options.html#syslog__d849610e55	
15.2.11 Deve implementar NTPv4 ou SNTP.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf	
15.2.12 Autenticação via RADIUS deve ser suportada.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf	
15.2.13 Autenticação via TACACS+ também deve ser suportada.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf	
15.2.14 Controle de acesso por porta (IEEE 802.1x) deve estar presente.	https://www.juniper.net/documentation/us/en/software/junos/user-access/topics/topic-map/802-1x-authentication-switching-devices.html	
15.2.15 Deve haver controle de broadcast, multicast e unicast por porta.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf	
15.2.16 Deve implementar pelo menos uma fila de saída com prioridade estrita (SP Strict Priority) e divisão de banda ponderada (WRED, WRR ou similar).	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf	
15.2.17 Deve classificar, marcar e priorizar tráfego com base em IEEE 802.1p CoS.	https://www.juniper.net/documentation/us/en/software/junos/traffic-mgmt-nfx/traffic-mgmt-qfx/topics/task/cos-classifiers-qfx-series-cli.html#defining-cos-ba-classifiers-dscp-dscp-ipv-ieee--p__subsection_wpm_hcw_jwb	
15.2.18 Deve classificar, marcar e priorizar tráfego com base em DSCP (Differentiated Services CodePoint), conforme IETF.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf	
15.2.19 Deve permitir classificação de tráfego por IP, portas TCP/UDP e endereços MAC.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf	
15.3 - Virtualização de Switch		
15.3.1 Deve permitir agregação de portas multi-chassi com redundância ativa/ativa sem Spanning Tree, usando MLAG, MC-LAG, M-LAG, VLT (Virtual Link Trunking), Multi-Chassis EtherChannel ou equivalentes.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf	
15.3.2 Todos os componentes necessários para alta disponibilidade devem ser fornecidos, incluindo cabos, transceivers e licenças.	Ciente e de acordo / Conforme Proposta Tecnica	
15.3.3 Em modo virtualizado, os switches devem operar com processamento local, sem tempo de convergência em caso de falha.	Não se Aplica	

15.4 - Funcionalidades de Camada 2	
15.4.1 Suporte a até 4.000 VLANs conforme IEEE 802.1Q.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.4.2 Implementação de VLAN Trunking conforme IEEE 802.1Q, com controle de VLANs permitidas por tronco.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.4.3 Suporte a Link Aggregation (LAG) conforme IEEE 802.3ad.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.4.4 Deve suportar no mínimo 80 grupos LAG com até 16 portas cada.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.4.5 Implementação dos padrões IEEE 802.1d, 802.1s e 802.1w.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.4.6 Deve possuir mecanismo de proteção da root bridge do Spanning Tree.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.4.7 Deve permitir bloqueio de BPDUs em portas em modo fast forwarding, com desativação automática ao recebê-los.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.4.8 Implementação de LLDP e LLDP-MED para descoberta de vizinhos.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.4.9 Suporte a DCB com PFC (IEEE 802.1Qbb), ETS (IEEE 802.1Qaz) e DCBx.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.5 - Funcionalidades de Roteamento	https://www.juniper.net/documentation/us/en/software/junos/multicast-l2/topics/topic-map/irb-and-bridging.html
15.5.1 Deve realizar roteamento de camada 3 entre VLANs.	https://www.juniper.net/documentation/us/en/software/junos/multicast-l2/topics/topic-map/irb-and-bridging.html
15.5.2 Suporte ao protocolo OSPFv3.	https://www.juniper.net/documentation/us/en/software/nce/feature-guide-ospf-v3-for-ipv6-tc/topics/task/ospfv3-enabling-solutions.html
15.5.3 Suporte ao protocolo BGPv4.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.5.4 Capacidade para no mínimo 106.000 rotas IPv4.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.5.5 Capacidade para no mínimo 52.000 rotas IPv6.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf
15.5.6 Operação simultânea com IPv4 e IPv6.	https://www.juniper.net/documentation/us/en/software/junos/subscriber-mgmt-sessions/topics/topic-map/dual-stack-migration-to-ipv6.html
15.5.7 Implementação de VRF ou VRF-Light.	https://www.juniper.net/documentation/us/en/software/license/juniper-licensing-user-guide/topics/concept/licenses-for-qfx.html
15.5.8 Suporte a roteamento baseado em políticas (PBR).	https://www.juniper.net/documentation/us/en/software/northstar6.2.7/northstar-planner-user-guide/topics/concept/ipmpls-policy-based-routes-overview.html
15.5.9 Implementação do protocolo VRRPv3.	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/qfx5120-ethernet-switch-datasheet.pdf

Ao
MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS

Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

DECLARAÇÕES COMPLEMENTARES

Declaro, sob as penas da Lei, para os devidos fins junto à Comissão Permanente de Licitação que:

a) Cumpro plenamente os requisitos de habilitação, ciente de que respondo pela veracidade das informações prestadas, na forma da lei;

b) Em atenção item 5.6. e art. 14.º e seus incisos da Lei n.º 14.133/2021, não estou impedido de participar direta ou indiretamente desta licitação, e ainda, não possuo sócios, diretores ou gerentes, que sejam cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros ou de servidores ocupantes de cargo de direção, chefia ou assessoramento no âmbito do Ministério Público do Estado do Amazonas e de sua CPL;

c) Recebi o edital e todos os documentos que o integram, dispondo de todos os elementos e informações necessários à elaboração da proposta de preços com total e completo conhecimento do objeto da licitação;

d) Os documentos e declarações apresentados são fiéis e verdadeiros;

e) Caso seja vencedor do certame e não cadastrado no SISTEMA DE ADMINISTRAÇÃO FINANCEIRA E CONTABILIDADE da SECRETARIA DA FAZENDA DO ESTADO DO AMAZONAS – SEFAZ-AM, encaminharei à CONTRATANTE os documentos necessários para efetuar o referido cadastramento no prazo de 05 (cinco) dias úteis, a contar da adjudicação, sob pena de perder o direito de preferência à contratação em favor dos demais licitantes subsequentes, sem prejuízo da possibilidade de responder a procedimento administrativo de responsabilização por eventual retardamento da licitação;

f) O preço inclui além do lucro, todos os custos e despesas, com tributos incidentes e encargos devidos, materiais, serviços, transporte, a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas

infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas, bem como quaisquer outras despesas diretas e indiretas incidentes na prestação de serviços;

g) Apresentarei, quando da contratação, documento que indique o pessoal técnico operacional, das instalações e do aparelhamento adequado e disponíveis para a realização do objeto da licitação, bem como a qualificação de cada membro da equipe técnica que se responsabilizará pelos trabalhos;

h) Submeto-me e concordo integralmente com os termos do presente Edital, bem como com seus elementos e especificações, comprometendo-me a cumpri-los fielmente, inclusive no que se refere à fiscalização e ao controle técnico a serem exercidos por profissional expressamente designado para tal finalidade; e

i) A proposta apresentada para participar do presente Pregão foi elaborada de maneira independente por esta licitante e o seu conteúdo não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer outro participante potencial ou de fato, por qualquer meio ou por qualquer pessoa.

Serra (ES), 19 de janeiro de 2026.

gov.br
Documento assinado digitalmente
TATIANA MONTEIRO MONTROZE
Data: 16/01/2026 08:41:16-0300
Verifique em https://validar.iti.gov.br

CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA
Tatiana Monteiro Montroze
RG: 40.183.211-9
CPF: 354.042.638-81

Ao
MPAM
P.E 94.001/2026

DECLARAÇÃO ITEM 11.8

A empresa **CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA,** pessoa jurídica de direito privado, inscrita no CNPJ sob nº 02.092.332/0003-30, com sede na Rua Samuel Meira, nº 394, sala 29, Bairro Taquara II, Serra/ES, CEP 29167-650, por intermédio de sua representante legal, o Sra. Tatiana Monteiro Montroze , brasileira, casada, portador da cédula de identidade nº 40.183.211-9 SSP/SP, inscrito no CPF/MF sob o nº 354.042.638-81, **DECLARA** que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

Serra (ES), 19 de janeiro de 2026.

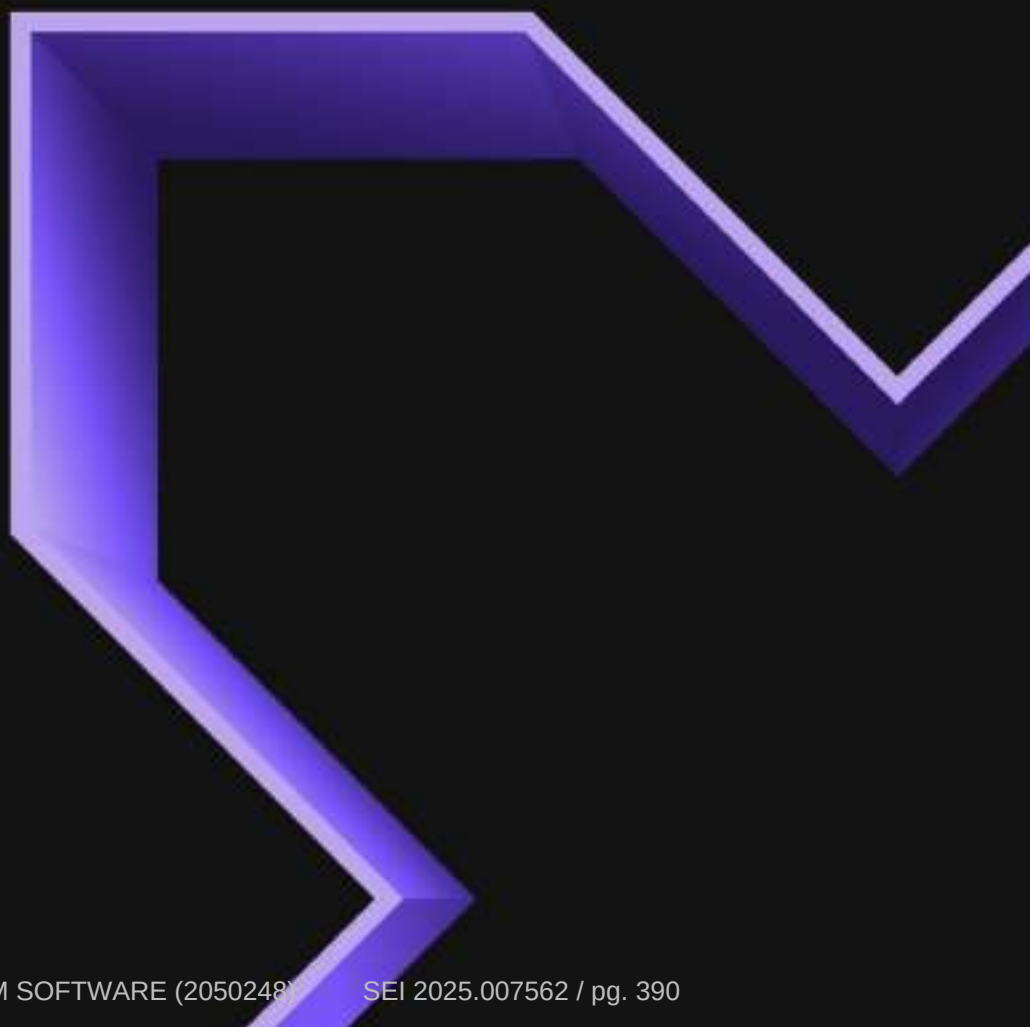
gov.br
Documento assinado digitalmente
TATIANA MONTEIRO MONTROZE
Data: 16/01/2026 18:22:33-0300
Verifique em https://validar.iti.gov.br

CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA
Tatiana Monteiro Montroze
RG: 40.183.211-9
CPF: 354.042.638-81

Nutanix Files User Guide

Files 4.4

February 22, 2024



NUTANIX

Contents

Nutanix Files Documentation Organization....6

Introduction to Nutanix Files....8
- Files Deployment....10
- Port Requirements....11
- Prerequisites....11
- Installation and Upgrades....15
  - File Server Module....15
  - Installing Files....16

Files Overview....19
- File Server View in Prism....19
- Files Console....21
  - Dashboard View....23
  - Monitoring View....24
  - Shares & Exports View....27
  - Data Management View....31
  - Alerts & Events View....31
  - Tasks View....33
  - Configuration View....34
- File Analytics....36

File Server Management....37
- Creating a File Server....37
  - Configuring File Server Basics....38
  - Configuring Networks....41
  - Configuring Directory Services and Review....47
  - Deleting a File Server....54
- File Server Updates....55
  - Updating the Network Configuration....56
  - Scaling FSVMs....59
  - Updating Memory and vCPU Resources....62
  - Updating File Server Basics....63
- Changing an FSVM Password....64
  - Logging on to a File Server VM....65
- Setting Timezones....65
  - Logging on to a File Server VM....65
- Starting a Files Cluster....66
  - Stopping a Files Cluster....66

Network Management....68
- Updating the Primary Network....68
- Managing the DNS Server....69
- Network Segmentation....69
  - Deploying Files with Network Segmentation....70

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 391

Multi-VLAN Network Management 70
Adding a Client Network 71
Listing Client Networks 73
Deleting a Client Network 73
Scaling Out A Multi-VLAN File Server 74
Configuring Client Exceptions 75
Configuring NFS Client Exceptions 75

Share and Export Management 77
Creating an SMB Share 77
Creating an NFS Export 83
Creating a Multi-Protocol Share or Export 90
Multi-Protocol Support for Files 95
Modifying a Share or Export 97
Deleting a Share or Export 98
Distributed Share Access 99
Accessing User Home Shares (Advanced) 99
Continuously Available Shares (SMB Only) 100
Connected Shares 100
Connecting Shares 101
Disconnecting Shares 101
WORM Shares 101
WORM Share Interoperability 102
Creating a WORM Share 103
Deleting a WORM Share 104
Nested Shares and Exports 105
Setting Directory-Level Quotas 106

Directory Service and Domain Management 108
Permissions 108
Directory Services and Authentication 109
Updating Directory Services 110
Setting AD Machine Account Password Expiry 111
Joining a Domain 112
Leaving a Domain 113
Updating Domain Name System (DNS) Entries 114
Disjoint Domains 117
Configuring Disjoint Domains 117

User Management 118
User Mapping 118
Configuring User Mapping 119
Managing Roles 125
Managing REST API Roles 127
Authorizing a REST API User 127
Managing Limited Local Users (SMB Only) 129
Quotas 130
Managing Quotas 133
Role-Based Access Control (RBAC) for Files 136

Files Options 137
Cloning 137

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 392

Cloning a File Server 137
Encryption 139
Files Data Collection 139
Access-Based Enumeration (SMB only) 139
Enabling SMB Symlinks 140
File Blocking 141
Blocking Files on a File Server 141
Durable SMB File Handles 142
Non-Disruptive Upgrades (NDU) for SMB 142
Antivirus (AV) Scanning (SMB Only) 143
Configuring Antivirus Scanning (SMB Only) 145
Antivirus Tab 147
Files REST APIs 148
ETag and OData Queries Overview 148
Using the Files API Explorer 149

Performance Optimization 152
Managing Performance Optimization 152
Unblocking Rebalancing 155
Workload Optimization 155
Modifying the Workload Type 155
File System Compression 156

Data Management 157
Data Protection and Recovery 157
Configuring Disaster Recovery 158
Activating Disaster Recovery 162
Metro Availability for Nutanix Files 164
Smart Tiering 166
Standard Tiering Overview 166
Smart Tiering Requirements and Recommendations 167
Smart Tiering Dashboard 169
Configuring a Tiering Location 170
Setting a Capacity Threshold 172
Creating a Tiering Policy 174
Tiering Data Manually 174
Updating a Tiering Configuration 175
Recalling Tiered Data 175
Self-Service Restore 176
Enabling Self-Service Restore 177
Adding Snapshot Schedules 178
Retrieving Files with Self-Service Restore (SSR) 180
Restoring a Share 180
Manually Restoring a Share 181
Deleting SSR Snapshots 181
Setting Custom Hourly Snapshot Times 182
Share Migration 182
Migrating Shares 183
Re-attempt Share Migration 186
Configuring Backup for Distributed Shares 186
High Availability 187

Security Hardening 188

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 393

Troubleshooting..... 193
Disable distributed file system (DFS) support on a witness share..... 193
Invalid Mounts After Authentication Change..... 193
Client Access Denial (NFS Protocol)..... 193
Clients Cannot Mount Shares..... 193
Client Side Network Mapping..... 194
Connecting to Authentication Services..... 194
Constraint Violation..... 194
Disable Directory Leasing on Snapshot..... 194
DNS Missing SRV Records..... 195
Domain Controller Issues..... 195
Finding IP Addresses..... 195
Identifying the Share Owner..... 195
Invalid Credential..... 196
NLM Locks..... 196
Network Cannot Expand..... 196
NFS Cache Expiry During Share Migration..... 196
Restore Target Share Access Upon Canceling Migration Plan..... 197
NTLM Authentication Issues..... 197
Share Copying..... 197
Stale Statistics..... 198
Time Difference..... 198
Unsuccessful Authentication..... 198

Copyright..... 199

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 394

NUTANIX FILES DOCUMENTATION ORGANIZATION

The Nutanix Files documentation is organized into two user guides and the release notes.

- The Nutanix Files User Guide describes Files concepts and administrative tasks.
- The Files Manager User Guide covers file server management in Prism Central (PC).
- The Nutanix Files Release Notes cover updates, features, and issues in each Files release.

For information on the contents of each document, see the "Documentation Organization" table below.

Table 1: Documentation Organization

Topics	Document

Feature overviews and instructions for administering and managing file servers and shares in the Prism Element web console and the Files Console, including the following:
• Network management
• Directory service and domain management
• User management and quotas
• Data management and performance optimization using the Files Console and Prism Element web console
  • NearSync, Async, and Metro Availability
  • Smart Tiering
  • Self-service restore
  • Share migration
  • High availability (HA)
• Controller VM (CVM) and file server VM (FSVM) based command-line interface (CLI) procedures
• Security Hardening
• Troubleshooting
	Nutanix Files User Guide

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 395

Topics	Document
Feature overviews and instructions for administering and managing file servers in PC, including the following: • PC-based file server creation • Role-based access control (RBAC) for Files • Smart DR • Smart Sync • Files in a virtual private cloud (VPC)	*Files Manager User Guide*
Feature descriptions and compatibility requirements, resolved issues, and known issues.	*Nutanix Files Release Notes*

Additional Resources

Solutions Documentation offers tech notes that include performance best practices, sizing recommendations, migration guidance, and an in-depth technical overview of Files architecture.

For system limits, see the Configuration Maximums page, the Nutanix Vulnerability Database page for CVE resolutions, see the Software Product Interoperability page for details on supported AOS upgrade paths.

- For system limits, see the Configuration Maximums page.
- For CVE resolutions, see the Nutanix Vulnerability Database page.
- For information on Unified Storage solutions for your environment, see the Validated Designs page.
- For details on supported AOS upgrade paths, see the Software Product Interoperability page.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 396

INTRODUCTION TO NUTANIX FILES

Nutanix Files (Files) is a software-defined, scale-out file storage solution that lets you share files in a centralized and protected location to eliminate the requirement for a third-party file server.

Files uses a scale-out architecture that provides file services to clients through the Server Message Block (SMB) and Network File System (NFS) protocols. Files combines one or more file server VMs (FSVMs) into a logical file server instance, sometimes referred to as a Files cluster. You can create multiple file servers within a single Nutanix cluster.

Files creates a volume group (VG) for every FSVM to provide stable storage for persistent states and audit events. During a service outage, the states, storage, and events of a VG fail over to another FSVM. Files also creates a dedicated container for every file server instance. If you choose to delete a file server, you can delete the container in Prism.

> **Tip:** Solutions Documentation offers tech notes that include performance best practices, sizing recommendations, migration guidance, and an in-depth technical overview of Files architecture.

Files offerings also include File Analytics, for statistics and monitoring of file servers, and the Files Manager for a unified control plane of all file servers and the deployment of file servers in Prism Central (PC). For more information on these products, see the *File Analytics Guide* and the *Files Manager User Guide*.

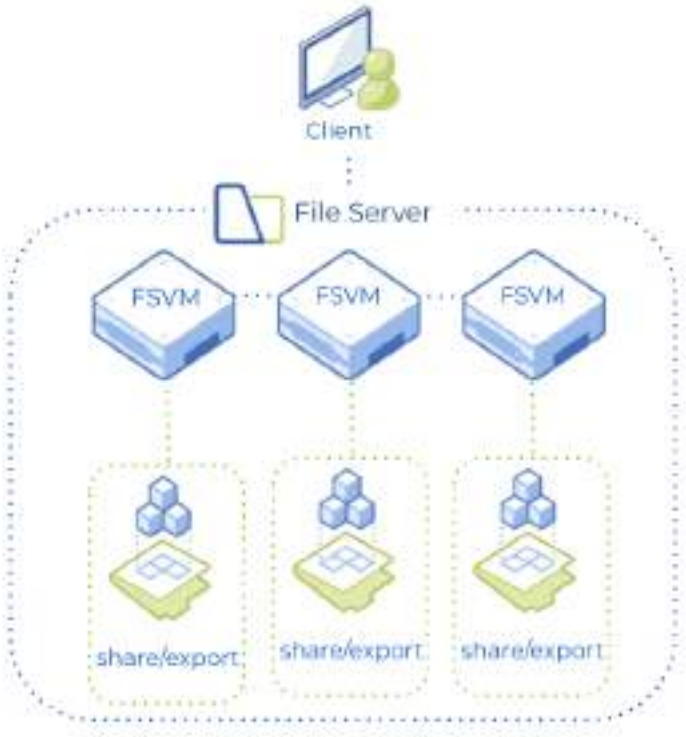


Figure 1: File Server Components

File Shares and Exports

Shares (SMB) and exports (NFS) encapsulate file directories. There are two types of shares or exports:

Distributed: A distributed share ("home") or export ("sharded") spreads data across all of the FSVMs on the file server to improve the performance and scalability of client connections.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 397

Note: Use the MMC Snap-In for Nutanix Files to manage top-level directories (TLDs) on distributed shares.

Figure 2: Distributed Share or Export

Standard: A standard share ("general purpose") or export ("non-sharded" or "non-distributed") contains all of the data on a single FSVM. A standard share or export serves data and connections from a single FSVM.

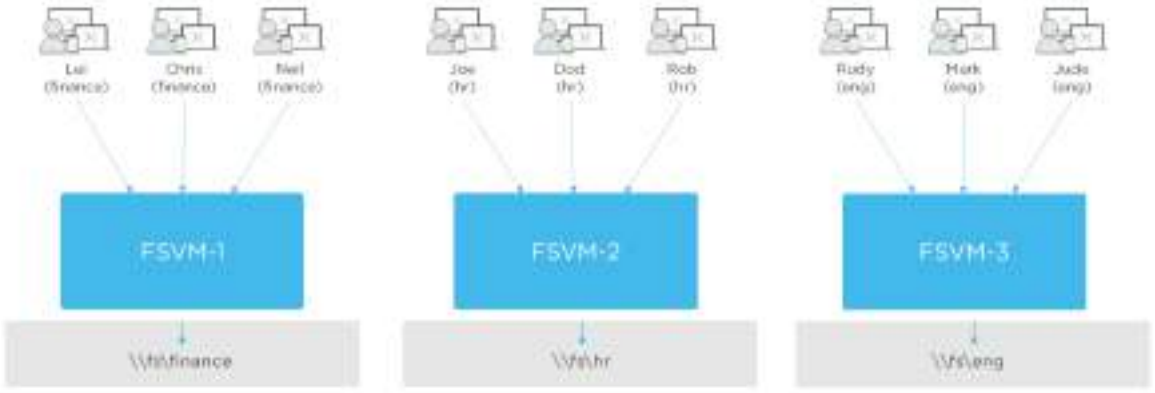


Figure 3: Standard Share or Export

Features

Files includes the following features:

- SMBv2, SMBv3, NFSv3 and NFSv4 protocol support.
- Multi-protocol support, see Multi-Protocol Support for Files on page 95.
- AHV and ESXi hypervisor support.
- High availability for both VMs and data, see High Availability on page 187.
- Load balancing through scale-up and scale-out, see Performance Optimization on page 152.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 398

- Data management including Smart Tiering, Smart Sync, Smart DR, protection domain (PD) based-DR, and Self-Service Restore (SSR). See Data Protection and Recovery on page 157 and the *Files Manager Guide* for Smart Sync and Smart DR.

You can also use Files storage for the deployment of Kubernetes clusters on Nutanix Kubernetes Engine (NKE) using the CSI Volume Driver. For more information, see NKE and CSI Volume Driver documentation.

For a description of features added with every major Files release, see the *Nutanix Files Release Notes*.

Networking

Files uses storage and client networks.

- **Storage network**: The storage network enables communication between the FSVMs and the Controller VMs.
- **Client network**: The client network enables communication between the clients and the FSVMs, allowing clients to access the Files shares. Files also uses the client network to communicate with the directory services.

For more information, see the Network Management on page 68 section. To separate Files iSCSI connections to a segmented network and to deploy Files, see Network Segmentation on page 69.

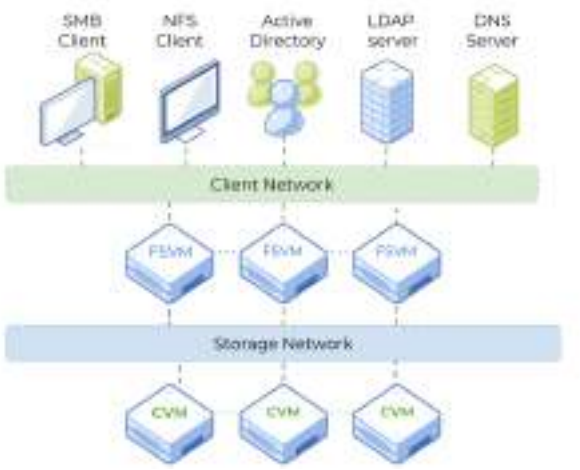


Figure 4: Files Networking

Files Deployment

On overview of Nutanix Files deployment.

To deploy Files in a Nutanix cluster, do the following:

> **Note:** To segregate Files iSCSI connections to a segmented network and to deploy Files, see Network Segmentation on page 69.

1. Satisfy the prerequisites and port requirements, see Prerequisites on page 11 and Port Requirements on page 11.
2. Install the Files software using the Life-Cycle Manager (LCM), see Installation and Upgrades on page 15.
3. Create a file server instance (Files cluster), see Creating a File Server on page 37.
4. Create one or more file shares (SMB) or exports (NFS), see Share and Export Management on page 77.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 399

To deploy Files in a network-segmented environment, see Network Segmentation on page 69.

Port Requirements

Files has various firewall requirements depending on the protocols and services being used.

The Port Reference provides detailed port information for Nutanix products and services, including port sources and destinations, service descriptions, directionality, and protocol requirements.

Prerequisites

Ensure you satisfy the prerequisites before attempting to deploy Files.

Requirements

Do the following before deploying Files:

- Install the File Server Module (FSM) from the **Downloads** page on the **Support Portal**, or upgrade to a compatible version using the Life-Cyle Manager (LCM). See Installation and Upgrades on page 15.
- Configure and define the storage network.
- Configure and define the client network.
- Have at least one network (two networks recommended).
- Set up a network time protocol (NTP) server.
- If you use Active Directory for user authentication, have credentials of the domain administrator or a user with delegated permissions.
- If using SMB shares, enable the distributed file system (DFS) for Windows clients (on by default).
- If you plan to use LDAP for NFS with permissions required for search, have credentials of the bind distinguished name (DN).
- [ESXi clusters only] register all ESXi host nodes in the AOS cluster to the same vCenter.
- Have an assigned iSCSI Data Services IP configured for the clusters.
- NFS clients should have unique host names.

File servers require the following minimum configurations.

- A minimum of four vCPUs per host.
- A minimum of 12 GiB of memory per host.
- For each file server, the number of CVMs must be equal to or greater than the number of file server VMs (FSVMs) to ensure availability if there is a node failure.

Limitations

The Configuration Maximums page provides details on Files system limits.

> **Note:** See the *Nutanix Files Release Notes* for release-specific details on supported configurations and software compatibility.

Network Requirements

The storage network requires at least one additional IP address than the number of FSVMs. The client network requires the same number of IP addresses as the number of FSVM nodes.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 400

- Storage network: Number of FSVMs + 1 (available IP addresses)
- Client network: Number of FSVMs

Single-FSVM deployments require one IP address for the storage network and one IP address for the client network.

If the client and storage networks are separate, they must be on different subnets. If you use the same network for both client and storage, then the IP addresses must be unique. Clients on the same subnet as the storage network cannot access the shares or exports.

To segregate Files iSCSI connections to a segmented network, see Network Segmentation on page 69.

Required Information

Collect the following information before deploying Files.

Table 2: Network Time Protocol

NTP Server	Used for the time synchronization between the file server and AD service.

Table 3: Domain Name System

DNS server names	Files uses DNS to resolve FSVM names and access external services.

Table 4: Active Directory (Optional)

Active Directory (AD)	Windows AD domain name.
AD admin account	Admin with domain administrator or delegated permissions.

Table 5: LDAP (Optional)

LDAP URL	LDAP server name or IP address (with optional port number).
Base DN	Distinguished name of the entry where to start the search for records.
Bind DN	Distinguished name of entry to use to perform search (optional when anonymous bind is disallowed).
Bind password	Password to use for bind DN.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 401

Table 6: iSCSI Data Services

iSCSI data services IP address	Files uses iSCSI to connect the storage to the FSVMs. See the *Nutanix Volumes Guide* for more information about iSCSI storage.

To segregate Files iSCSI connections to a segmented network, see Network Segmentation on page 69.

Table 7: Managed Networks

Storage network	The VLAN that connects the Controller VM to the FSVM.
Client network	The VLAN that connects the FSVM to the AD and DNS.

Table 8: Unmanaged Networks

Storage network gateway	The VLAN that connects the Controller VM to the FSVM.
Storage network subnet	The storage network subnet value.
Storage network IP address range	If there is more than one FSVM, the number of IP addresses is the total number of FSVMs (one FSVM per node) plus one more address. For example, in a three-node cluster you will need four IP addresses, and in a four-node cluster you will need five. Single-FSVM deployments require only one storage network IP address.
Client network gateway	VLAN connects the FSVM to the AD and DNS.
Client network subnet	Subnet of client network.
Client network IP address range	One IP address for each FSVM in the file server. For example, a three FSVM file server needs three IP addresses.

Table 9: Active Directory Parameters

Provide the following parameters to join the domain.

Element	Definition	Required
Domain Name	The fully qualified domain name.	Required

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 402

Element	Definition	Required
Organizational unit	**Note:** By default, Files creates the computer account in the Computers container. The forward slash (/) is allowed to denote hierarchies but not in the organizational unit name. The organizational unit (OU) contains the computer account Files creates. List the AD users permissions for the machine account on the OU. In an organization with complex hierarchies, create the computer account in a specified container by using a forward slash mark to denote hierarchies (for example, organizational_unit/inner_organizational_unit).	Optional
Password	The password for the account used to connect to the AD server. Files uses the password to authenticate to AD and to create the Files computer account.	Required
Preferred domain controller	**Note:** • Files does not support read-only domain controllers (RODC) for joining domains because RODC cannot create machine accounts. • If the preferred domain controller is not reachable, the enabling AD operation fails. Files discovers a local domain controller for all communications. If you do not configure Files to a specific site, then it uses a domain-level domain controller. This parameter lets you specify a preferred domain controller Files uses for the join domain operation. The preferred domain controller must be reachable and allow write access privileges to the domain controller.	Optional

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 403

Element	Definition	Required
User name	The user name that authenticates on the Active Directory on the domain. A domain user authenticates to the file server on the domain controller and creates Files computer accounts, related SPN entries, and Files DNS entries (when using Microsoft DNS). If you are in the same domain, you can use the user principal name (UPN) or SamAccountName. If you are outside of the domain but in the same forest, then use the UPN. **Note:** • Files only allows the "at" symbol (@) symbol to specify the domain. Files does not allow UPNs with multiple @ symbols. For example, "user@mydomain.com" is valid but "user@name@mydomain.com" is not valid. • Files does not allow the forward slash (/) and the backward slash (\) in the UPN.	Required

Installation and Upgrades

Install and upgrade Nutanix Files and the required components.

Before installing or upgrading Files, check LCM to ensure you have compatible AOS and File Server Module (FSM) versions.

For information on performing inventory, installation, and upgrades in LCM, see the *Life Cycle Manager Guide*.

For FSM or the Files Manager, perform inventory followed by installation or upgrades in LCM. For more on these components see, File Server Module on page 15 or the Files Manage User Guide.

To install Files, use the 1-click feature, see Installing Files on page 16. To upgrade Files, perform inventory and upgrades in LCM.

Note: For upgrades from older versions (AOS 5.17 and LCM 2.3.1.1 or earlier), use Prism Element (PE).

Note: If you do not see a target Files version, check Nutanix Files Upgrade Paths on the Support Portal to confirm that the version is 1-click enabled.

Tip: For compatibility requirements, see "Nutanix Files Software Compatibility" in the *Nutanix Files Release Notes*, which also provide details on updates in each Files and FSM version.

File Server Module

Files requires a compatible version of the FSM.

The FSM provides Files life-cycle and GUI components. Files relies on AOS for some control plane components.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 404

Before upgrading or installing Files, upgrade or install a compatible version of the FSM using the Life Cycle Manager. For more information about steps on performing inventory and upgrades in LCM, see the *Life Cycle Manager Guide*.

Installing Files

Install Nutanix Files.

About this task

> **Caution:** Nutanix recommends performing Files upgrades during non-business hours. Upgrading Files can cause a brief FSVM downtime and a temporary disconnection of connected clients.

Use the 1-click feature in Prism Element (PE) to install Files.

> **Note:** Consider the following before a Files upgrade:
>
> - After an AOS upgrade, compression on the Files container resumes after a one-hour delay.
> - [ESXi only] When performing one-click hypervisor upgrades that have Files, disable the anti-affinity rules on all FSVMs. After the hypervisor successfully upgrades, enable the anti-affinity rules on the FSVMs.
> - ESXi hosts that belong to multiple vSphere clusters or are deployed across multiple data-centers might experience limitations. See KB 5369 for more information.

Follow the steps as indicated.

Procedure

1. Log onto Prism Element (PE) with your credentials.
2. Click the **gear icon** > **Upgrade Software**.
3. In the **Settings** menu, click **Upgrade Software**.
4. In the **Upgrade Software** window, select the **File Server** tab.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 405

5. Complete install process by doing one of the following.

   » To download the Files version you want to install, see step 6.

   » Upload the Files binary from a different source skip to step 7.

   Note: If you do not see a target Files version, check Nutanix Files Upgrade Paths on the Support Portal to confirm that the version is 1-click enabled.

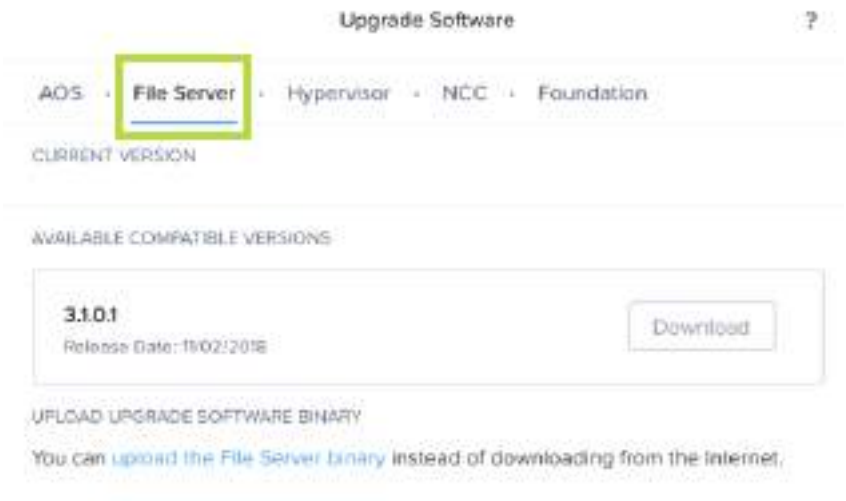


Figure 5: Upgrade Software: File Server tab

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 406

6. To download software, click the **Download** button for the target version.

   a. Once the download completes, click **Continue**.

   b. In the **New File Server: Pre-check** dialog box, review the requirements and best practices.

   c. Click **Continue.**

   d. In the **Upgrade Software** window, click the **Upgrade** button.

      The install or upgrade process takes a few minutes. For upgrades, once the process is complete, a message indicates the number of file servers successfully upgraded.

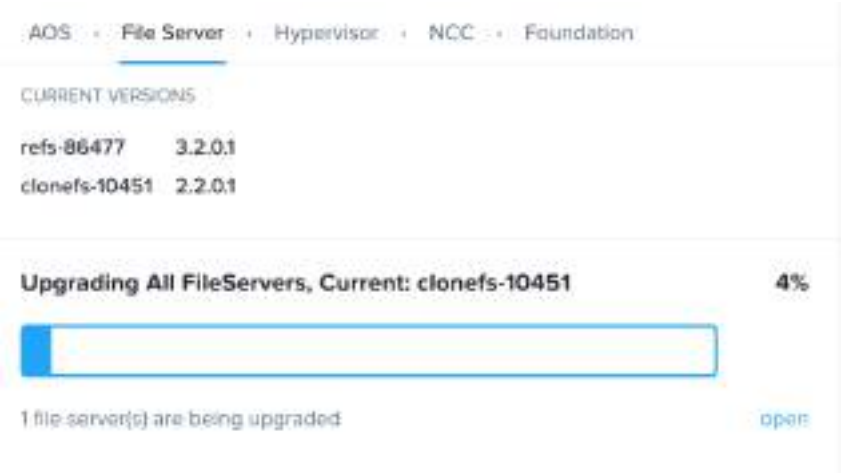


Figure 6: File Server: Upgrading

7. To install uploaded software, click the **upload the File Server binary** link, and perform the following steps as indicated.

   a. **File server metadata file**: click the **Choose File** button and select the target Files metadata file.

Figure 7: Upload Software Binary

   b. **File server binary file**: click the **Choose File** button and select the target Files binary file.

   c. To upload the installation files, click the **Upload Now** button.

      The install or upgrade process takes a few minutes. For upgrades, once the process is complete, a message indicates the number of file servers successfully upgraded.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 407

FILES OVERVIEW

Manage file servers and shares from the Files Console and the **File Server** view in Prism Element (PE).

The **Files Server** view in Prism Element is the landing page for Files. The **File Server** view provides an overview of your file servers on a PE cluster and basic file server management options.

The Files Console is a GUI for the management of file servers and shares. To access the Files Console from the **File Server** view in PE, click **Launch Files Console** next to the target file server.

To manage file servers created in Prism Central, access the Files Console by navigating to file servers from the Files Manager, see the *Files Manager User Guide*.

File Server View in Prism

The **File Server** view in Prism Element provides basic information about each file server in the cluster.

To get to the **File Server** view, select **File Server** from the pull-down menu in Prism Element.

File Server View Layout

The **File Server** view includes the following sections and options:

- Action buttons to create a file server (see Creating a File Server on page 37), to configure the network (see Updating the Network Configuration on page 56), and to deploy File Analytics (see File Analytics).
- An entities table displays information about each file server. You can filter the table contents by entering a string in the search field located above the table.

  Note: The **Recommendations** column is disabled. See **Recommendations** in the Files Console dashboard.

- A **File Summary** pane displays high-level details about file servers on the cluster, and, after selecting a file server, the **File Server Details** pane displays summary information for that file server.
- A **gear icon** with options to download the table content in the CSV or JSON format.
- A list of operations to perform on the file server that includes the following: **Launch Files Console** (see Files Console on page 21, **Clone** (see Cloning on page 137), **Update** (see File Server Updates on page 55), **Protect** (see Data Management on page 157), and **Delete** (see Deleting a File Server on page 54). You can perform some of these operations through the Files Console.

  Note: The values for the parameters do not account for features applied by AOS or space used at the storage container level.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 408

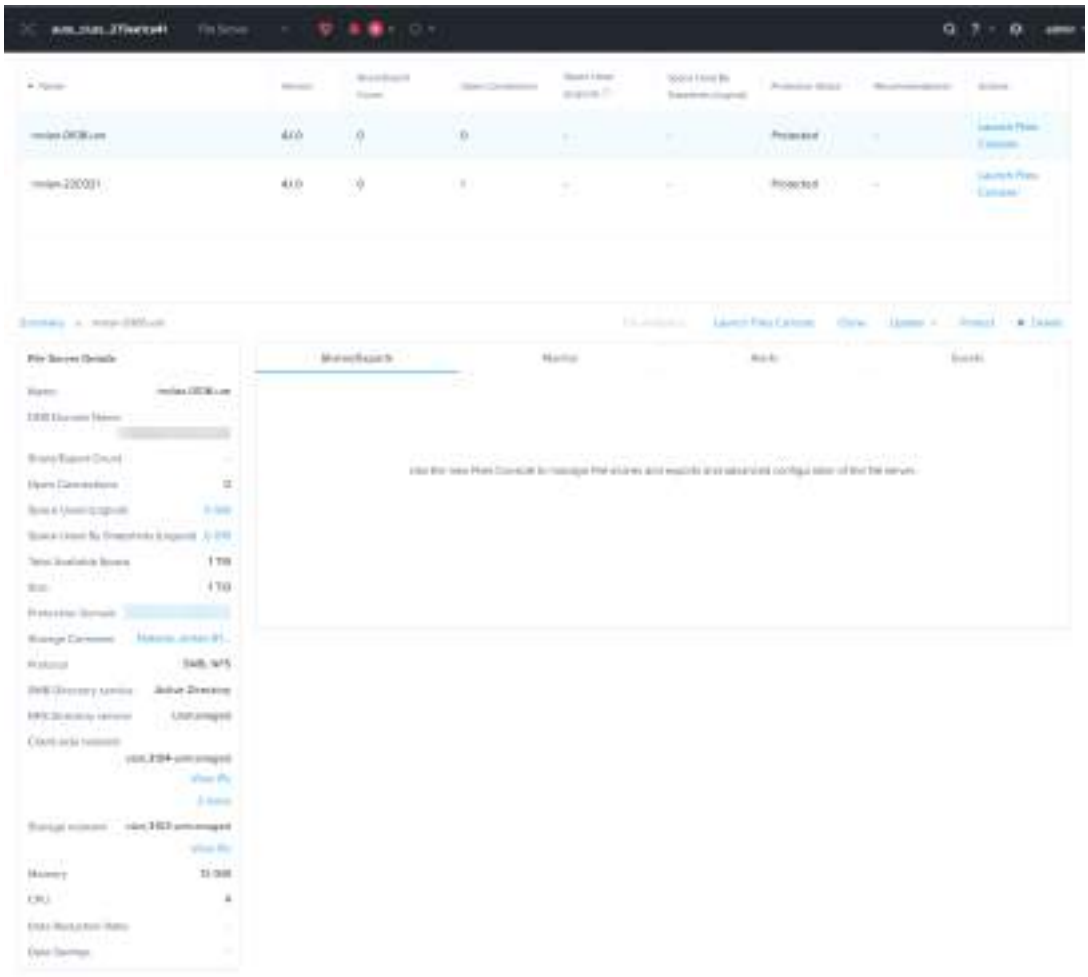


Figure 8: File Server View

Details Pane

Selecting a file server in the table presents detailed information in the **File Server Details** pane. The following tables describe the fields.

Table 10: File Server Details Fields

The parameters described in this table represent values from the perspective of the file server.

Parameter	Description	Values
Name	The file server name.	(name)
DNS domain name	The name of the domain that the file server is registered to. "Not Protected" indicates that the file server is not currently in a protection domain.	(DNS domain name)
Open connections	The number of open connections.	(integer)
Share/Export Count	The total number of shares or exports.	(integer)
Space used	The total amount of storage space used within the file server currently.	xx [GiB|TiB]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 409

Parameter	Description	Values
Space used by snapshots	The amount of space used within the file server to store snapshots currently.	xx [MiB|GiB|TiB]
Total available space	The amount of available (unused) storage space currently on the file server.	xx [MiB|GiB|TiB]
Size	The size of the file system of the file server.	xx [TiB]
Protection domain	The name of the protection domain that includes this file server. Clicking the name displays the **Data Protection** view for that protection domain. "Not Protected" indicates that the file server is not in a protection domain. See the *Data Protection and Recovery with Prism Element* guide for information on protection domains.	(protection domain name)
Storage container	The name of the storage container of the file server. Clicking the name displays the **Storage Container** view for that storage container.	(storage container name)
Protocol	The protocols used by the file server.	SMB, NFS, or both
SMB directory service	The SMB protocol always uses Active Directory as the directory service.	Active Directory
NFS directory service	The NFS protocol has multiple options for the directory service.	Unmanaged, Active Directory, or LDAP
Client-side network	The name of the primary network used by clients. Click **View IPs** to view all the IPs for the primary network. Click **More** to view the additional client networks.	(network name)
Storage network	The name of the network used for storage.	(network name)
Memory	Used memory.	GiB
CPU	Total CPUs.	Numerical
Data reduction ratio	Data reduced using file-system-level compression.	x:x (numerical)
Data savings	Amount of data saved using file-system-level compression.	MiB

Alerts Tab

The **Alerts** tab displays a table of alerts for the selected file server. You can also see alert details in the Files Console, see Alerts & Events View on page 31.

Events Tab

The **Events** tab displays a table of events for the selected file server. You can also see events details in the Files Console, see Alerts & Events View on page 31.

Files Console

The Files Console provides administrative tools and dynamically updated information for a single file server and its shares.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 410

Access the Files Console from the **File Server** view in Prism Element (PE) by selecting **Launch Files Console** or by clicking the name of a file server in the Files Manager.

The Files Console consists of the following primary tabs:

- The **Dashboard** tab is the home page in the files console provides an overview of file server dataDashboard View on page 23.
- The **Shares & Exports** tab provides detailed information on every share on the file server, see Share Details View on page 28.
- The **Data Management** tab provides options for configuring disaster recovery, self-service restore, and Smart Tiering, se Data Management on page 157.
- The **Alerts & Events** tab provides details of file server events and alerts on the file server with an option to acknowledge each occurrence, see Alerts & Events View on page 31.
- The **Tasks** view displays a list of recent tasks and the current status of each task, s Tasks View on page 33.
- The **Configuration** tab includes configuration options for the file server and a **Platform** view that provides a configuration summary, see Configuration View on page 34.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 411

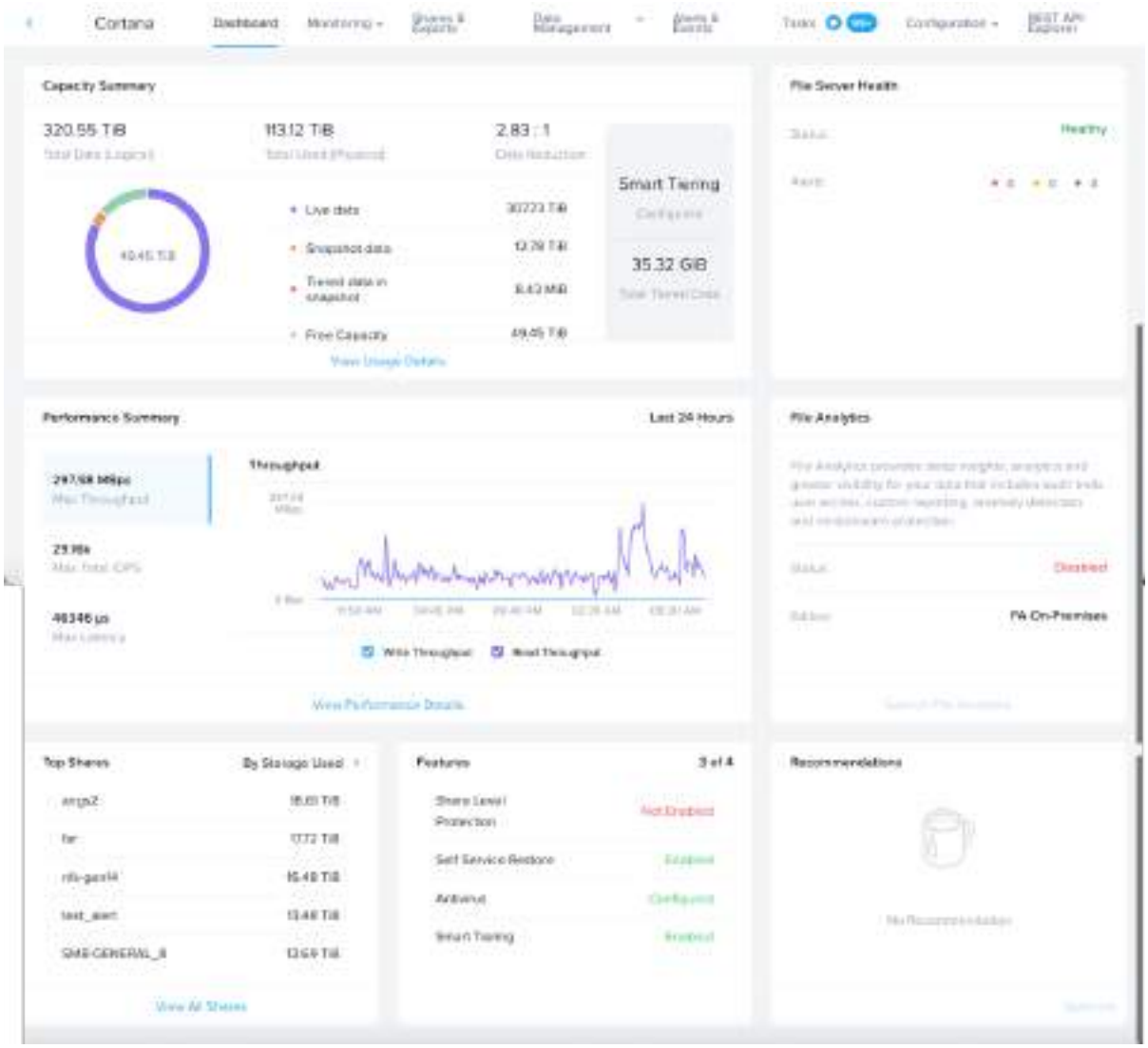


Figure 9: Dashboard View

Dashboard View

This **Dashboard** view is the landing page in the Files Console.

Dashboard

The **Dashboard** view includes the following elements.

- A **Capacity Summary** pane that visualizes the data usage on the file server.
- A **File Server Health** pane indicates the health status of the file server.
- A **Performance Summary** pane that consists of a graph that displays current throughput, current total IOPS, and current latency data.
- A **File Analytics** pane indicates whether you have or have not enabled File Analytics on the file server, see the File Analytics User Guide for more information.
- A top **Top Shares** pane includes a drop-down option to sort top-shares by storage used, connections, and files.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 412

- A **Features** pane that lists the features enabled on the file server.
- A **Recommendations** pane lists recommendations for improving the file server performance.

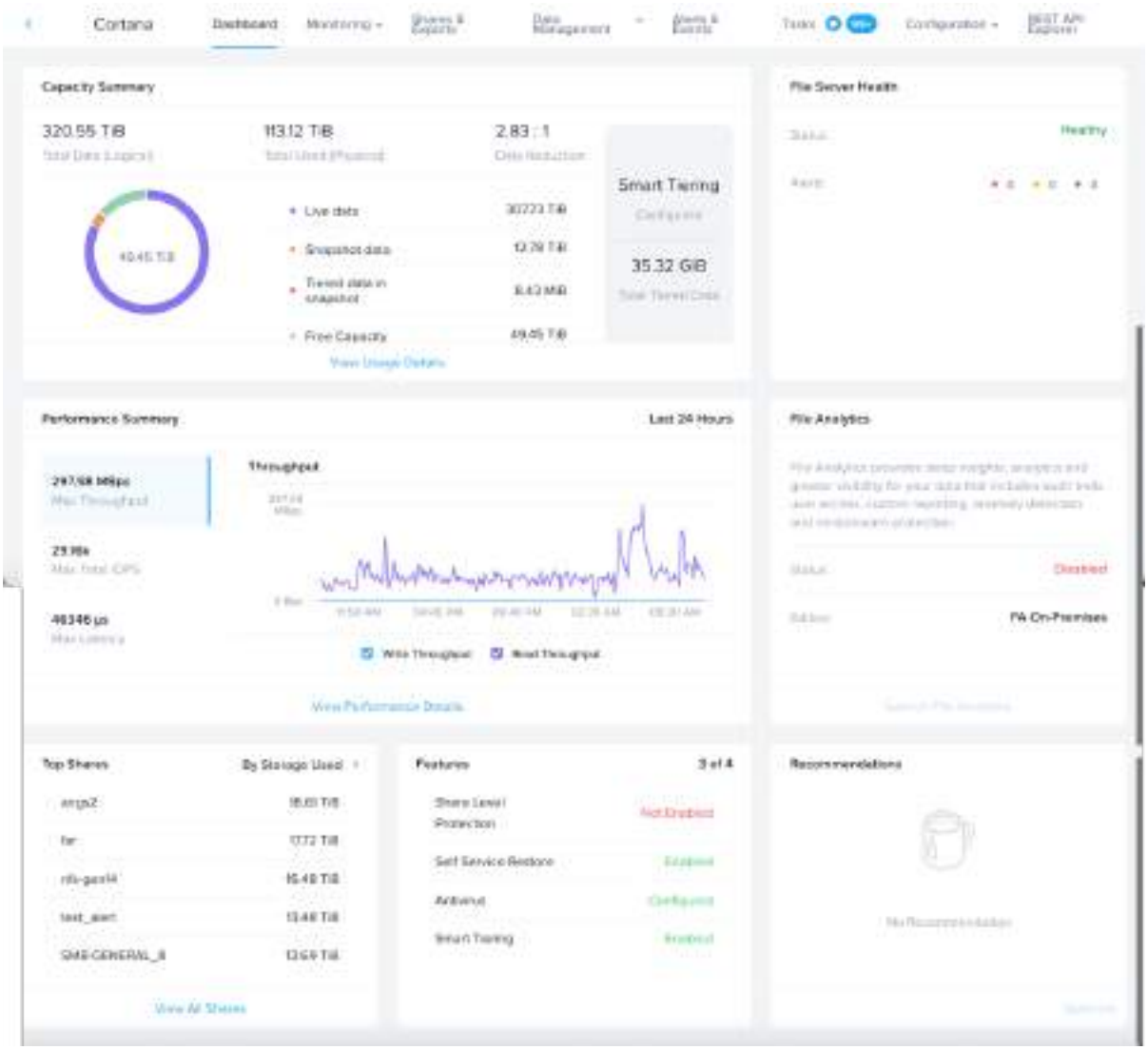


Figure 10: Dashboard View

Monitoring View

The **Monitoring** dropdown menu includes subtabs with granular monitoring details.

Usage Tab

The **Usage** tab displays these graphs.

- The **Storage Used** graph displays a rolling time interval monitor of the storage space used for data and snapshots on the file server. Hovering over the data displays the value for the time specified on the horizontal axis. To isolate a data set, check or uncheck the **Spaced Used by Dataset** and **Space Used For Snapshots** boxes.
- The **Open Connections** graph displays a rolling time interval monitor of the open connections on the file server.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 413

- The **Number of Files** graph displays a rolling time interval monitor of the total number of files in the file server. Hovering over the data displays the value for the time specified on the horizontal axis.
- The **Top Shares by Current Capacity** graph indicates the top shares using the most storage capacity.
- The **Top Shares by Current Connections** graph indicates the top shares with the most open connections.

Pull down lists above the graphs let you sort the data. You can select the time interval (last week, last 24 hours, last 6 hours, or last 3 hours). You can also select to display data for all shares or specific shares.

Performance Tab

The **Performance** tab includes the following elements.

- The **Latency** graph displays average latency across a rolling time interval monitor. Hovering over the data displays the value for the time specified on the horizontal axis. Selecting the **Show I/O and Metadata Breakdown** option above the graphs adds **Write Latency**, **Read Latency,** and **Metadata Latency** data set options.
- The **Throughput** graph displays average throughput. Hovering over the data displays the value for the time specified on the horizontal axis. Selecting the **Show I/O and Metadata Breakdown** option above the graphs adds **Write Throughput** and **Read Throughput** data options.
- The **IOPS** graph displays total I/O operations per second. Hovering over the data displays the value for the time specified on the horizontal axis. Selecting the **Show I/O and Metadata Breakdown** option above the graphs adds **Write IOPS**, **Read IOPS**, and **Metadata IOPS** data options.
- The **Top Shares by Current Latency**pane displays the shares with the most latency.
- The **Top Shares by Current Throughput** pane displays the shares with the most throughput.
- The **Top Shares by Current IOPS** pane displays the shares with the most I/O operations per second.

Pull-down lists above the graphs let you sort the data. You can select the time interval (last week, last 24 hours, last 6 hours, or last 3 hours) and select to dspecific shares.

Antivirus Tab

> **Note:** This tab is only visible with SMB or multi-protocol shares.

The **Antivirus** tab displays antivirus scanning information (see Antivirus (AV) Scanning (SMB Only) on page 143) in a set of subtabs:

The **ICAP Servers** tab displays a pane that lists the configured ICAP servers and panes with the following details:

- The **All ICAP Servers** pull-down list lets you choose to scan data for all ICAP servers or a specific server based on its IP address.
- The **ICAP Server** pane indicates the scanned server.
- The **Connection Status** pane indicates whether the server is connected to Files.
- The **Number of Shares** pane indicates the number of shares and exports scanned.
- The **Average Latency** graph displays the average response latency.
- The **Files Scanned** and **Data Processed** switches reveal the **Files Scanned** or the **Data Processed** graphs. The **Files Scanned** graph displays the number of files scanned by the server. The **Data Processed** graph displays the amount of data the server processes.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 414

The **Reports** tab provides two tables, one summarizing the latest scan and a second listing the identified threats. The following table describes the fields. The first table provides a scan summary, which includes the following fields:

- **Scan Period**: the antivirus scan period (24, six, or 3 hours).
- **Total Files Scanned**: the number of files scanned.
- **Threats Detected**: the number of threats detected. The **Events** table details each threat.
- **Files Cleaned**: the number of files cleaned.
- **Files Quarantined**: the number of files quarantined.
-

The second table provides event details, which include the following columns:

- **Share/Export**: the name of the share or export in which the affected file resides.
- **File Path**: the path to the affected file.
- **Threat Description**: describes the detected threat.
- **ICAP server**: the IP address of the ICAP server that detected the threat.
- **Time**: the time when the threat Files detected the threat.
- **Action Taken**: the action taken to address the threat (quarantined, unquarantined, reset).
- **Quarantined Files** and **Unquarantined Files** tabs include tables that describe each of the quarantined or unquarantined files and an action pull-down menu.

Table 11: Quarantine Fields

Parameter	Description	Values
Share/Export name	The name of the share or export where the affected file resides.	(name)
File path	The path to the affected file.	(file path)
Threat description	Describes the detected threat.	(text string)
ICAP server	The name of the ICAP server that detected the threat.	(server name)
Scan time	The time when the file was quarantined (unquarantined).	(time)

File Server VMs

The **File Server VMs** tab displays the following graphs:

- The **Load Average** graph displays a rolling time interval monitor of the CPU usage on the file server as a percentage of the total available CPU. Placing the cursor anywhere on the horizontal axis displays the value then.
- The **Memory Usage** graph displays a rolling time interval monitor of the memory usage on the file server in GB. Placing the cursor anywhere on the horizontal axis displays the value then.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 415

You can select the time interval (last week, last 24 hours, last 6 hours, or last 3 hours). You can also select to display data for all shares or specific shares.

Tiering

The **Tiering** tab has a table that lists all shares on the file server and their tiering status. The table is organized by share name, with the following details for each share: tiering enabled (or disabled), total data, live data, snapshots data, tiered data, files tiered and tiered data in the snapshot.

Smart DR Replication

The **Smart DR** tab consists of a graph illustrating the outward replication throughput of Smart DR for all policies on the file server.

Shares & Exports View

The **Shares & Exports** view in the Files Console.

The **Shares & Exports** view lists all shares on the file server and includes the following elements:

- A **+ New Share or Export** action button to create new shares.
- A table with information on each share on the file server. By default, the table displays the **General** view, but you can use the **View By** dropdown in the upper right to switch to the **Metrics** view.
- Clicking a share name in the share table redirects you to the share details view, which includes the following tabs: **Summary**, **Snapshots**, **Quota Policies**, **Antivirus**, and **Metrics**, see Share Details View on page 28.

  The **General** view consists of the following columns and details:

Table 12: Shares - General

Column	Description
Name	The name of the share or export. Clicking the share opens the share **Summary** in the share details view.
Share/Export path	The file path to the share or export.
Protocol type	The primary protocol of the share or export (NFS or SMB).
Share type	The data distribution type of the share. *Standard* shares and exports contain all data on a single FSVM. *Distributed* shares and exports load balance data across all FSVMs of the file server.
Share protection	The disaster recovery policy status on the share. See Data Protection and Recovery on page 157.
Self-service restore	The status of self-service restore for the share or export (enabled or disabled). See Self-Service Restore on page 176.
Access Based Enumeration	The status of Access Based Enumeration of the share: the green checkmark icon indicates enabled ABE, and the gray **x** icon indicates disabled ABE, see Access-Based Enumeration (SMB only).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 416

Column	Description
Compression	The status of file-system level compression: the green checkmark icon indicates enabled compression, and the gray **x** icon indicates disabled compression. See File System Compression on page 156
[three dots menu]	Clicking the three-dots menu displays the following share options: edit, delete, add quota policy, restore share, pause snapshots.

The **Metrics** view consists of the following columns and details:

Table 13: Shares- Metrics

Column	Description
Name	Name of the share.
Share/export path	Path to the share or export.
Max size	The maximum share size limit.
Space used	The sum of space used by active data, space used by snapshots (logical), and space used by file metadata.
Space used by snapshots	The space used by self-service restore snapshots.
Connections	The average number of open connections on the share.
IOPS	The average number of input and output operations per second.
Throughput	The average throughput.
Latency	The average latency.

Share Details View

Clicking the name of a share in the Files Console opens the share details view, which includes several tabs that detail share properties and operations.

The share details view consists of the **Summary**, **Snapshots**, **Quota Policies**, **Antivirus**, and **Metrics** tabs.

Summary

The **Summary** tab includes the following elements:

- An **Update** button to update the share details.

  For more information on the fields of the **Update Share** window, see Creating an SMB Share on page 77.
- An **Actions** dropdown menu includes options to update some of the share configurations.
- A **Capacity Summary** pane visualizes the share capacity used by snapshot and actual data.
- A **Share Properties** pane includes details on the configuration of the share (see the "Share Properties" table for more details).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 417

- A **Performance Summary** pane consists of a graph that displays current throughput, current total IOPS, and current latency data.
- A **Features** pane lists the features enabled on the share.

Table 14: Share Properties

Parameter	Description	Values
Name	The share or export name.	(share/export name)
Description	The description of the share provided during share creation.	(description text)
Share path	The file path to the share or export.	(share path)
Mount path	The mount path to the share or export.	(mount path)
Primary protocol	The primary protocol of the share.	[NFS | SMB]
Max Size	The maximum size of the share.	(value) GiB
Multi-protocol access	Indicates the multi-protocol access status on the share.	[enabled | disabled]
Share type	The data distribution type of the share. *Standard* shares and exports contain all data on a single FSVM. *Distributed* shares and exports load balance data across all FSVMs of the file server.	[standard | distributed]
Block File Types	The status of file blocking, see File Blocking on page 141.	[enabled | disabled]
Share compression	The status of file-system level compression, see File System Compression on page 156	[enabled | disabled]
Compression Ratio	Compression ratio from file-system compression.	x:x (numerical)
Data Savings	Data savings based on file-system compression.	(value) MiB
Authentication	Authentication method. **Note:** Files with NFSv3 protocol does not support Kerberos 5, Kerberos 5i, and Kerberos 5p.	[none | system | Kerberos (AD) | Kerberos 5 | Kerberos 5i | Kerberos 5p]
Client Access	Type of client access. **Note:** For native SMB shares, SMB client access is always read-write. Access-control lists (ACLs) specify user and group access permissions.	[read-write | read-only | or no access]
Squash	(NFS only) type of squash option. For more information, see Creating an NFS Export on page 83.	[none | root_squash | all squash]
Message encryption	Indicates enabled SMB3 message encryption. See, Encryption on page 139.	[enabled | disabled]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 418

Parameter	Description	Values
File system compression	Indicates enabled file-system level compression. See File System Compression on page 156	[enabled | disabled]

Snapshots

The **Snapshots** tab includes a table that displays all snapshots of the share. The table includes column with the following details:

- The **Create Time** indicates the time that Files took the snapshot.
- The **Snapshot ID** indicates the unique identified for the snapshot.
- The **Total Space** indicates the size of the snapshot.
- The **Reclaimable Space** indicates the amount of space that you can recover by deleting the snapshot.

Figure 11: Snapshots

Quota Policies

The **Quota Policies** tab includes a **New Quota Policy** button and a table that displays all quota policies on the share.

Antivirus

The **Antivirus** tab includes the following subtabs: **Infected Files**, **Quarantined Files**, **Unquarantined Files**.

The **Infected Files** tab includes a list of infected files.

The **Quarantined Files** tab includes a list of infected files.

The **Unquarantined Files** tab includes a list of files that were previously quarantined. An administrator removed the file from quarantine. An unquarantined file typically indicates a false-positive.

Metrics

The **Metrics** tab includes two more tabs: **Usage** and **Performance**.

The **Usage** tab includes the following dynamically updated graphs:

- **Storage Usage**: Displays the amount of storage used over time.
- **Open Connections**: Displays the number of open connections over time.
- **Number of Files**: Displays the number of files on the share over time.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 419

The **Performance** tab includes an option to **Show I/O and Metadata Breakdown** and the following dynamically updated graphs:

- **Latency**: Displays latency on the share over time.
- **Throughput**: Displays throughput on the share over time.
- **IOPS**: Displays the number of input and output operations per second over time.

The **Tiering** tab includes a dynamically updated graph of tiering latency.

Data Management View

Manage file server data from the **Data Management** tab.

The **Data Management** tab consists of the following views.

- The **Protection** view includes **Disaster Recovery** and **Self-Service Restore** tabs.
  - In the **Disaster Recovery** tab, configure Smart disaster recovery (DR) or protection-domain-based DR. See Data Protection and Recovery on page 157.
  - In the Self-Service Restore tab, configure snapshot schedules. See Self-Service Restore on page 176.
- The **Tiering** view includes an option to configure Smart Tiering using Data Lens. See Smart Tiering on page 166.
- The **Synchronization** view, lists **Data Sync** policies on the file server.

Alerts & Events View

The **Alerts & Events** tab in the Files Console.

The **Alerts & Events** view consists of the **Alerts** and the **Events** tab.

Alerts Tab

The **Alerts** tab includes the following elements:

- A search bar to filter by alert name.
- A table displaying a list of recent alerts.

Table 15: File Server Alerts Fields

Parameter	Description	Values
(selection box)	To select the alert, click this box. Clicking the **Acknowledge** or **Resolve** buttons acknowledges or resolves all the selected alerts.	n/a
Title	Description of the alert.	(string)
Impact type	Displays the impact category.	[availability | capacity| configuration | performance]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 420

Parameter	Description	Values
Acknowledged	Displays the acknowledgment status.	[auto | yes | no | (unspecified)]
Resolved	Displays the resolution status.	[auto | yes | no | (unspecified)]
Source entity	Displays the entity name (**File Server**) to which this alert applies. Clicking the name displays the details for that file server.	(entity name)
Severity	Displays the severity level of this condition. There are three levels: Critical A "critical" alert is one that requires immediate attention, such as a failed Controller VM. Warning A "warning" alert is one that might need attention soon, such as an issue that could lead to a performance problem. Informational An "informational" alert highlights a condition to be aware of, for example, a reminder that the support tunnel is enabled.	Critical, warning, informational
Create time	Displays the date and time when the alert occurred.	(time and date)

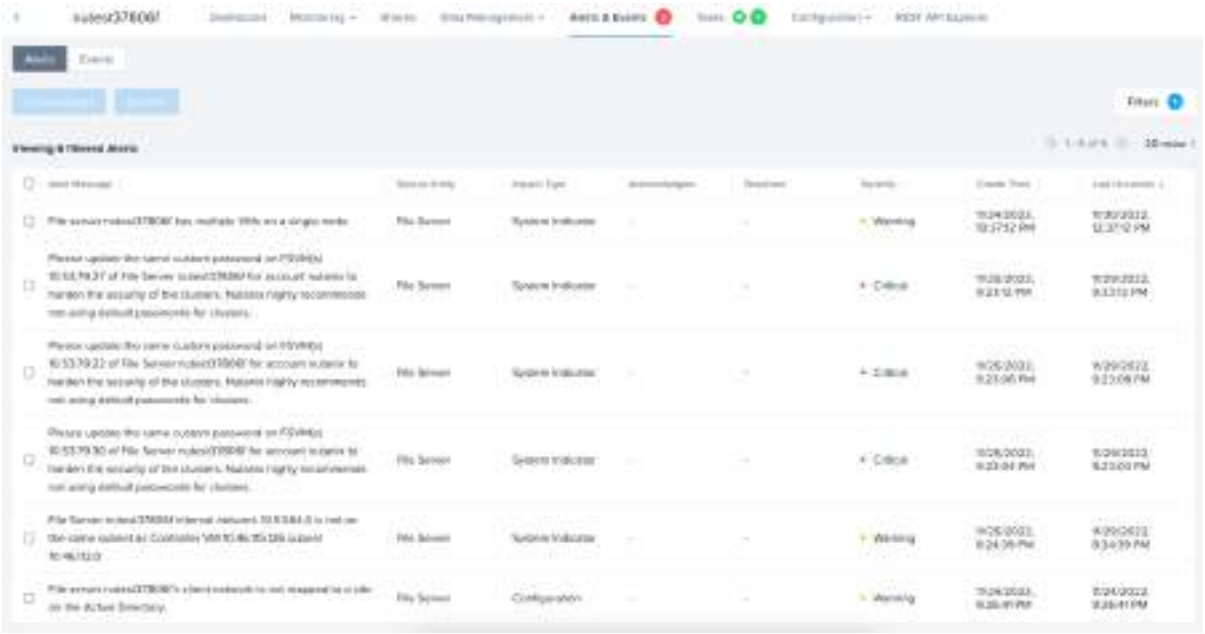


Figure 12: Alerts

The **Events** tab displays a table of events across all file servers. The following table describes the event table fields.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 421

Table 16: File Server Events View Fields

Parameter	Description	Values
Title	Displays the event title and indicates related entities.	(message text)
Entities	Displays the type of entity (**File Server**, **Share**) to which the event applies. A comma-separated list appears if it applies to multiple entities. Clicking the entity name displays the details for that file server, share, or export.	[share, file server]
Event type	Displays the category for the event.	[storage, user action]
(create time)	Displays the date and time when the event occurred.	(time and date)

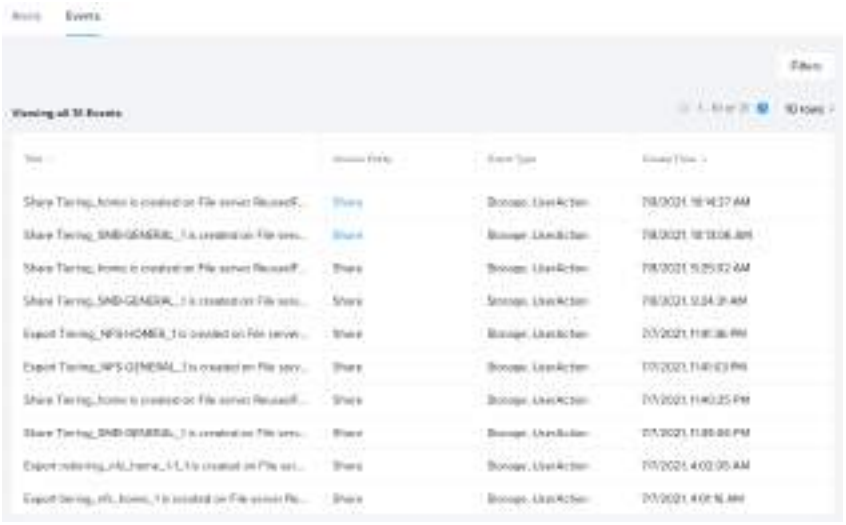


Figure 13: Events Tab

Tasks View

The **Tasks** view in the Files Console.

The **Tasks** view indicates the tasks running on the file server and includes the following elements:

- A **tasks table** that lists each administrative operation initiated on the file server.
- A **filters** menu to filter using pre-configured filters.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 422

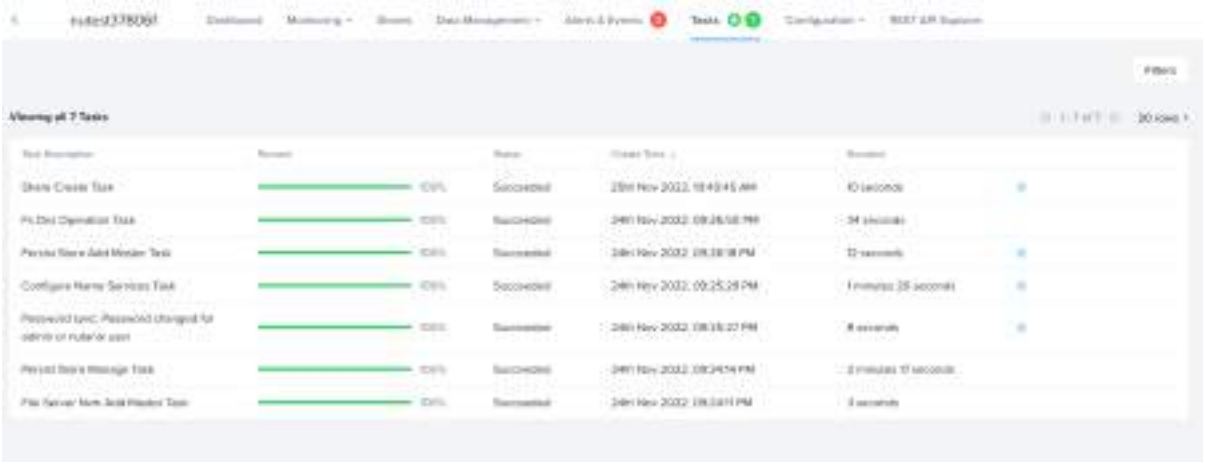


Figure 14: Tasks View

The following tables describe the columns in the **Tasks** table.

Table 17: Table

Column	Description	Values
Task description	Describes the operation that triggered the task.	(name of operation such as "create share")
Percent	Indicates the current completeness of the task as a percentage.	(0%-100%)
Status	Indicates the status of the task.	[succeeded, running, failed, queued]
Create time	Indicates when the task began.	(x) [seconds, minutes, hours, days]
Duration	Indicates how long the task has been running.	(x) [seconds, minutes, hours, days]

Configuration View

The **Configuration** view in the Files Console.

The **Configuration** view includes the following tabs:

- Authentication
- Blocked file types
- Manage roles
- Update DNS entries
- Antivirus
- Platform

The **Platfrom** view includes the following elements:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 423

- An **Update** drop-down menu includes options to update file server basics, scale up/ scale down, and update the DNS and NTP servers.
- The **Configuration Summary** provides details about the configuration of the file server.
- The **Files Cluster** diagram provides a visual diagram of the file server configuration.

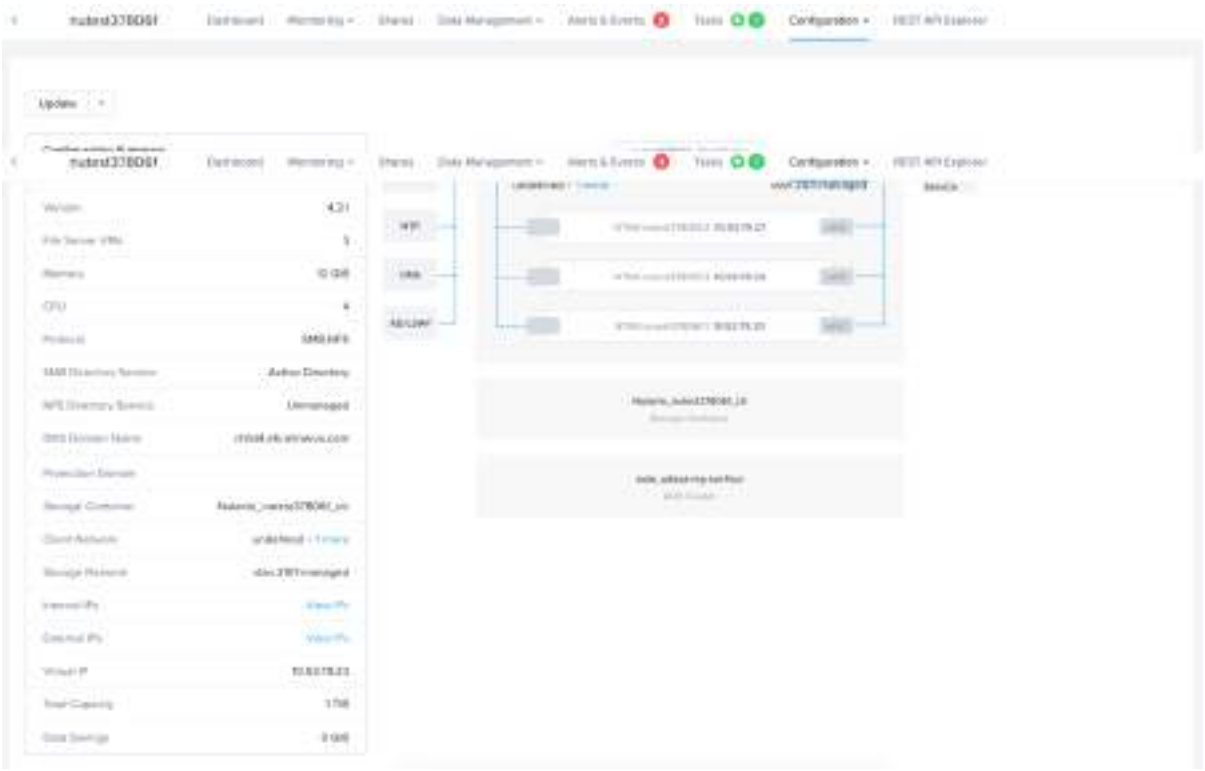


Figure 15: Platform View

Table 18: Configuration Summary

Parameter	Description
Name	The name of the file server.
Version	The Files version.
File Server VMs	Number of file server VMs on the file server.
Memory	Maximum configured memory.
CPU	Maximum configured CPU.
Protocol	The primary protocol and, when applicable, the secondary protocol (see Multi-Protocol Support for Files on page 95).
SMB directory service	The configured directory service for SMB shares.
NFS directory service	The configured directory service for NFS shares.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 424

Parameter	Description
DNS domain name	The name of the domain name system (DNS) for the file server.
Protection domain	The name of the protection domain.
Storage container	The name of the storage container.
Client network	The name of the client network. Click More to view the additional client networks.
Storage network	The name of the storage network.
Internal IPs	The internal IP addresses of the file server.
External IPs	The external IP addresses of the file server.
Virtual IPs	The virtual IP addresses of the file server.
Total capacity	The maximum capacity for the file server.
Data savings	The amount of data saved on the file server.

File Analytics

File Analytics provides data and statistics on the operations and contents of a file server.

Once you deploy File Analytics, Files adds a File Analytics VM (AVM) to the Files cluster. A single AVM supports all file servers in the cluster, but you must enable Analytics separately for each file server. Files protects the data on the AVM and keeps it in a separate volume group.

For deployment steps and administrative guidance, see the *File Analytics Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 425

FILE SERVER MANAGEMENT

Create a new file server and manage its configuration.

Creating and managing a file server requires administrator privileges. You can perform most file server management tasks in the **File Server** view in Prism Element and through the Files Console. You can start, stop, and manage file server VMs (FSVMs) through the VM tab in Prism Element, see "VM Management" in the *Prism Web Console Guide* for more details.

A file server usually consists of three or more FSVMs combined into a logical group. The Scaling FSVMs on page 59 section describes restrictions for increasing and reducing the number of FSVMs.

Single-FSVM deployments have the following limitations:

- No High Availability (HA) support. Single-FSVM deployments do not include other FSVMs that an out-of-service FSVM can fall back on, see High Availability on page 187.
- No distributed share support. Since distributed shares and exports spread data across multiple FSVMs, single-FSVM deployments only support standard shares.

> **Important:** When the file server capacity or the container capacity reaches 100 percent, all shares or exports within the file server become read-only and Files blocks write privileges. Prism displays alerts when the file server capacity or the container capacity reaches 90 percent and when either reaches 100 percent capacity.

Creating a File Server

Follow the procedure to create a file server with one or multiple file server VMs (FSVMs).

About this task

> **Important:** To create Prism Central-managed file servers, see "Creating a File Server" in the Files Manager User Guide.

Procedure

1. Go to the **File Server** view in Prism Element (PE) (see File Server View in Prism on page 19), and click **+ File Server** in the upper right.
2. If a **New File Server: Pre-Check** window appears, review the displayed information and address any unsatisfied prerequisites before continuing.

   Files checks your current environment and either verifies it satisfies the prerequisites or identifies where it does not meet the requirements (see Prerequisites on page 11). A blue check mark indicates a satisfied prerequisite. Any unchecked items need attention. The checks are for the Files software

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 426

version, available data services IP addresses, available networks, and, for ESXi, if vCenter registered the cluster.

> **Note:** To use the high-availability (HA) and DRS features, add all ESXi hosts under the same ESXi cluster and have one FSVM per ESXi host.

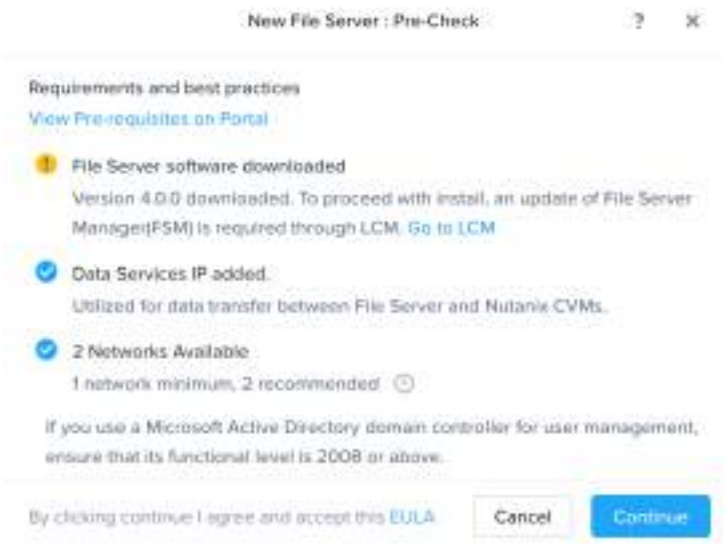


Figure 16: New File Server: Pre-Check Window

3. To configure a file server, do the following as described in the sections below:
   a. Configure file server basics.
   b. Configure networks.
   c. Configure directory services
   d. Review the summary section and create the file server.

Configuring File Server Basics

Procedure

In the **Basics** tab of the **Create File Server** window, do the following in the indicated fields:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 427

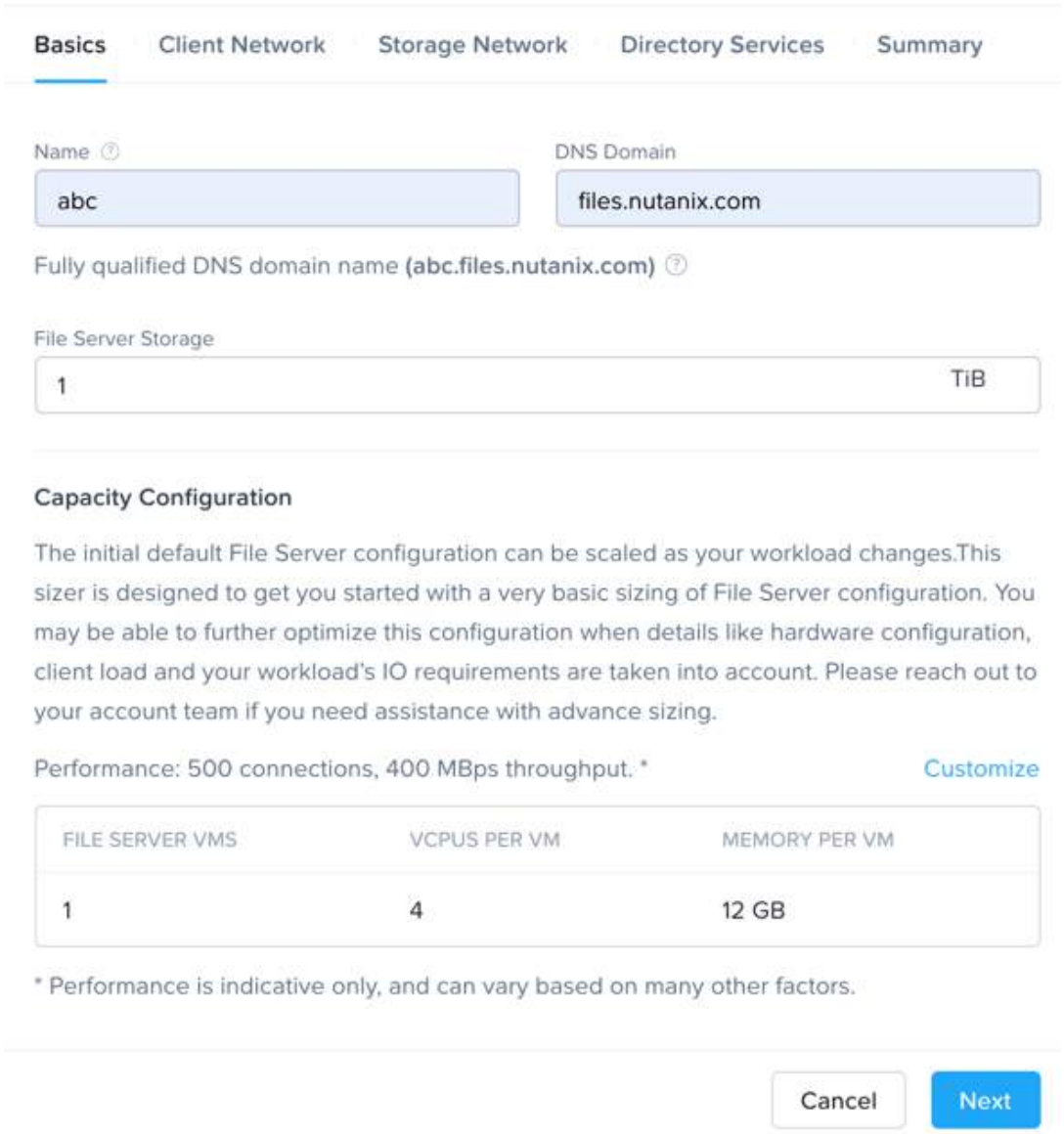


Figure 17: Create File Server: Basics Tab

a. **Name**: Enter a name for the file server.

   Clients use the file server name to access the file server. The fully qualified name (file server name + domain) must be unique.

b. **DNS Domain**: Enter a fully qualified domain.

c. **File Server Storage**: Enter the file server total storage size (minimum 1 TiB).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 428

d. **Capacity Configuration**: Files automatically recommends the number of file server VMs, vCPUs per VM, and memory per VM. Review the performance values (connections and throughput) and then do one of the following:

> **Note:** For single-FSVM deployments, the number of suggested FSVMs is always one.

- If you are satisfied with the recommended configuration, click **Next** button.
- To change the configuration, click **Customize**. The **File Server Capacity Configuration** window displays. To change the configuration based on performance requirements, enter the target number of connections and throughput amount (in MBps) in the **SMB Concurrent Connections** and **NFS Throughput in MBps** fields and then click **Save**.

Figure 18: File Server Capacity Configuration window

- To manually specify the FSVM parameters, click**Customize** > **Configure manually**. The **File Server Capacity Configuration** window displays. Enter the number and capacity of the FSVMs in the **Number of File Server VMs**, **VCPUs Per VM**, and **Memory Per VM** (in GIB) fields, and then click **Save**.

Figure 19: File Server Capacity Configuration window

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 429

Configuring Networks

Procedure

1. In the **Client Network** tab, do the following in the indicated fields:

   Note: Provide two static IP addresses for each new FSVM, one for the client-side network and one for the storage network.

   Note: If clients or the AD domain controllers are in the same subnet as the controller VM (CVM) or the storage network, configure the same client-side and storage-side networks. Otherwise, use separate client and storage networks. If you use the same network for both clients and storage, use unique IP addresses; otherwise clients on the same subnet as the storage network cannot access the shares.

   Note: Nutanix Files does not support advanced VLAN network configurations.

   a. **VLAN** (AHV) or **Port Group** (ESXi): Select the target VLAN or port group from the drop-down list.

   After selecting the target, configured network parameters display if the target is a managed network.

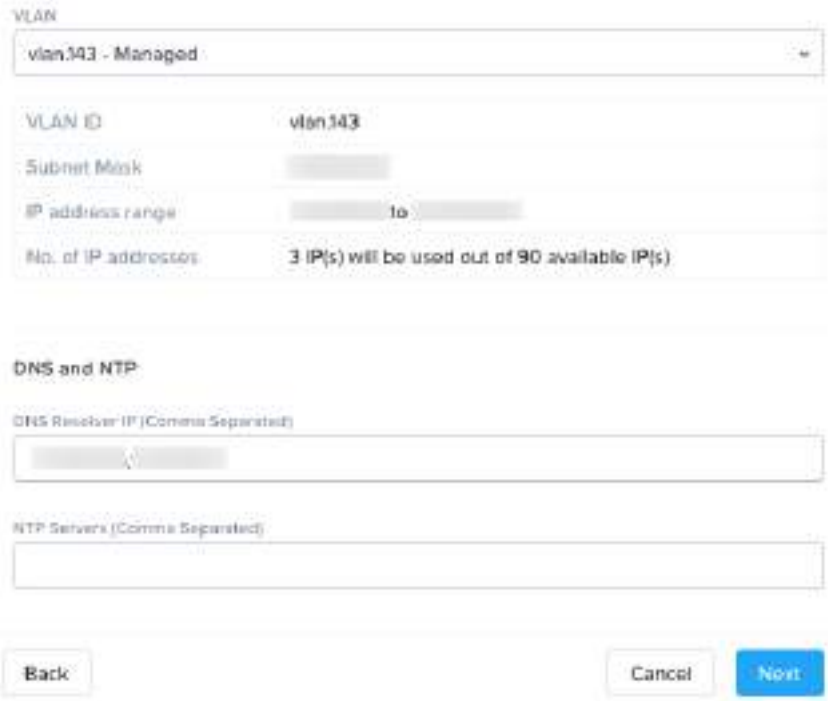


Figure 20: Client Network Details (managed VLAN)

   b. For unmanaged networks, the following fields appear:

   - **Subnet Mask**: Enter the subnet mask value.
   - **Gateway**: Enter the IPv4 gateway IP address.
   - **# IP addresses required**: Click the **+ IP Addresses** button to display a row for entering IP addresses. Enter the starting IP address in the **From** field, the ending IP address in the **To** field,

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 430

and click **Save**. (Usually, Files requires three IP addresses. Files requires one IP address for single-FSVM deployments.)

- **Add IPv6**: Check this box to enable the IPv6 protocol.
- **Prefix Length**: Enter an integer for the prefix length (the default IPv6 prefix is 64).
- **Gateway**: Enter the alpha-numeric, colon-separated IPv6 gateway address.
- Click the **+ IP Addresses** button to display a row for entering IP addresses. Enter the starting IP address in the **From**, and enter the total number of IP addresses in the **No. of IPs** field (usually Files requires three IP addresses). Click **Save**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 431

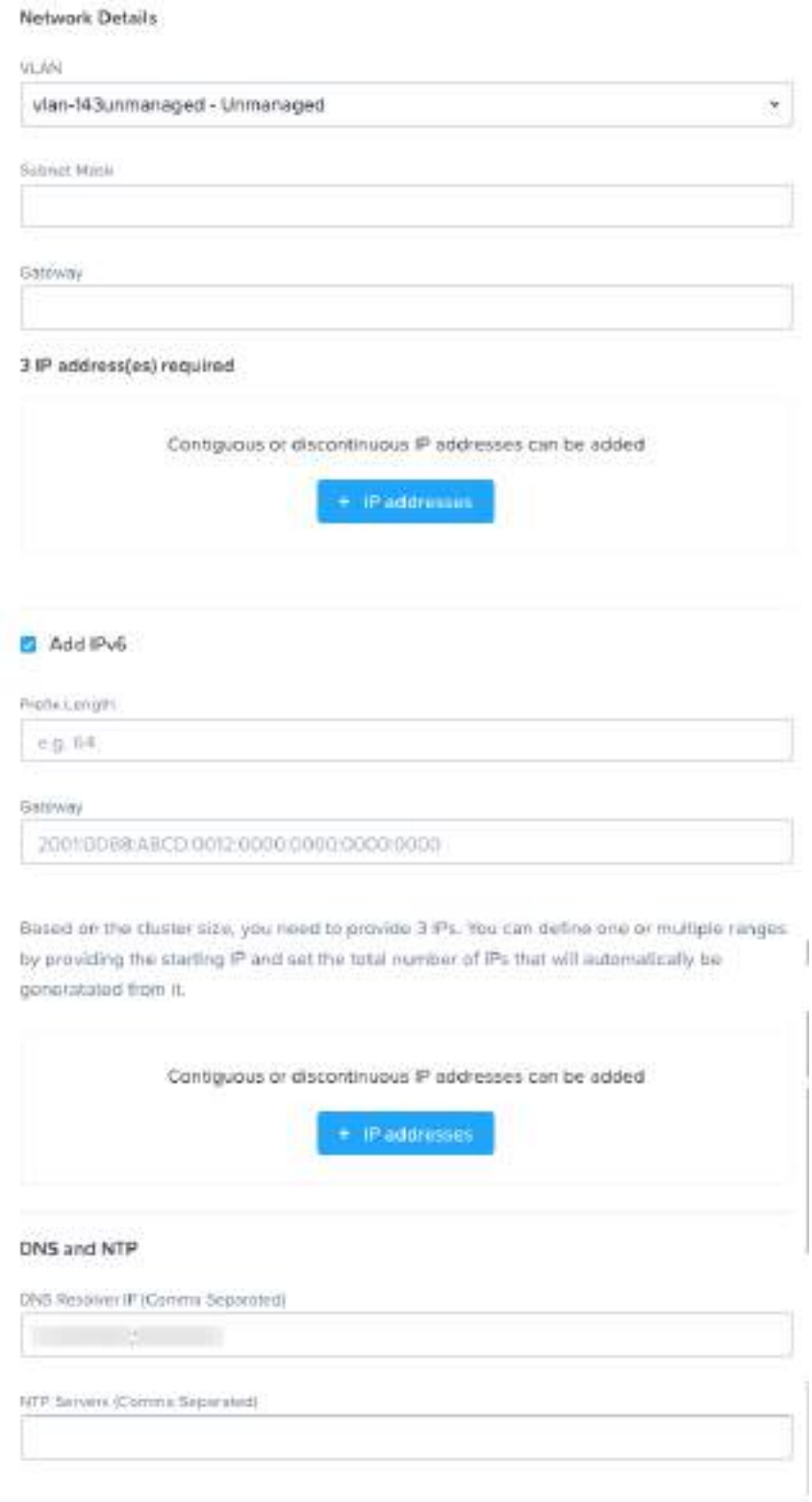


Figure 21: Client Network Details (unmanaged VLAN)

c. **DNS Resolver IP**: Enter IP addresses for one or more DNS servers (IPv4 only). Use a comma-separated list for multiple entries.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 432

> **Note:** The DNS Resolver IP and the NTP servers fields can pre-populate based on the target VLAN or port group.

d. **NTP Servers**: Enter the server names or IP addresses for the NTP servers. Use a comma-separated list for multiple entries.

e. When all the entries are correct, click **Next**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 433

2. In the **Storage Network** tab, do the following in the indicated fields:

> **Note:** For ESXi, do not use the Controller VM (CVM) backplane network. The CVM backplane network is not supported and any later upgrade operations might fail.

> **Note:** Nutanix Files does not support advanced VLAN network configurations.

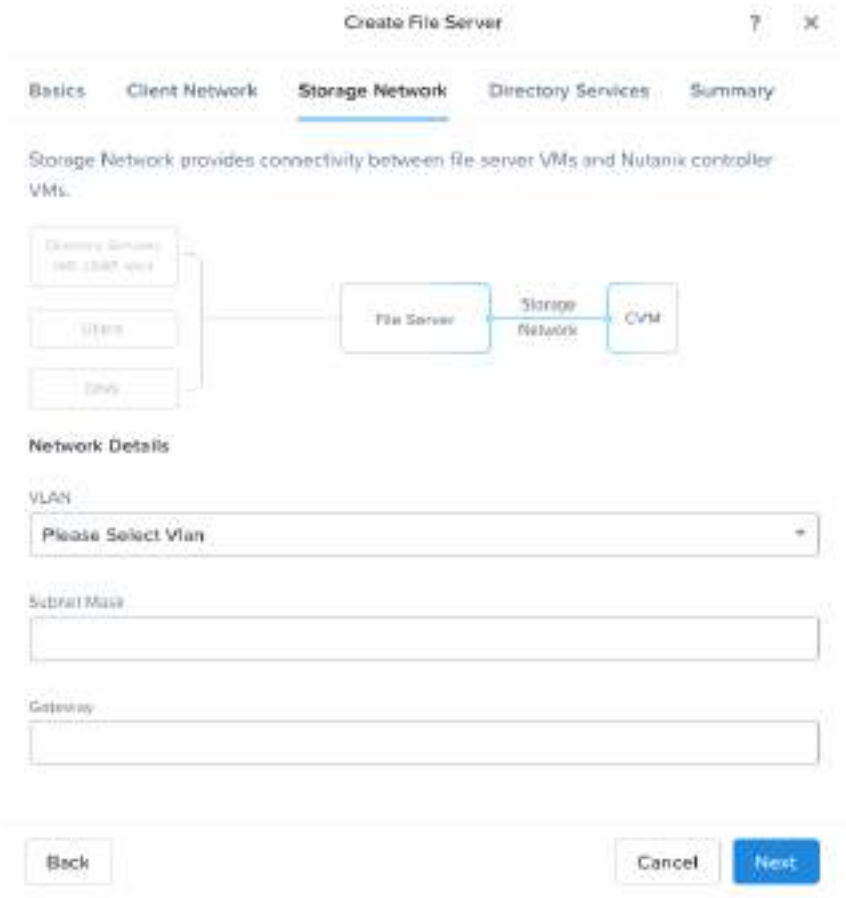


Figure 22: Create File Server: Storage Network Tab

a. **VLAN** (AHV) or **Port Group** (ESXi): Use the pull-down list to select the desired VLAN or port group for the storage network.

   Once you select the target, if the target is a managed network, Files displays configured network parameters.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 434

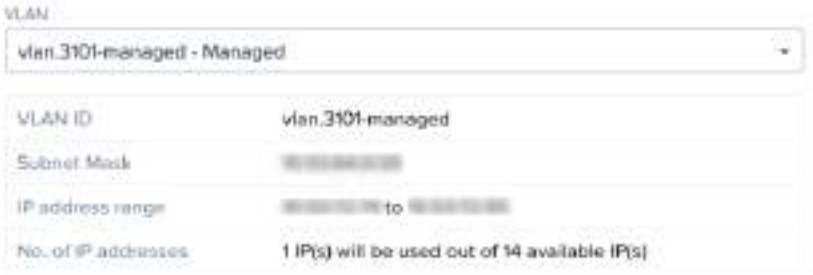


Figure 23: Storage Network Details (managed VLAN selected)

b. For unmanaged networks, the same fields appear as for the client network (**Subnet Mask**, **Gateway**, and **# IP addresses required**). Enter the appropriate values for the storage network. In this case, Files normally requires four IP addresses.

c. When all the entries are correct, click **Next**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 435

Configuring Directory Services and Review

Procedure

1. In the **Directory Services** tab, select one or more protocols to use (check the **Use SMB Protocol** box, **Use NFS Protocol** box, or both boxes).

> **Note:** You can skip this step and select the protocols later, but you cannot use the file server until this step is complete.

> **Note:** Files supports using LDAP for AD.

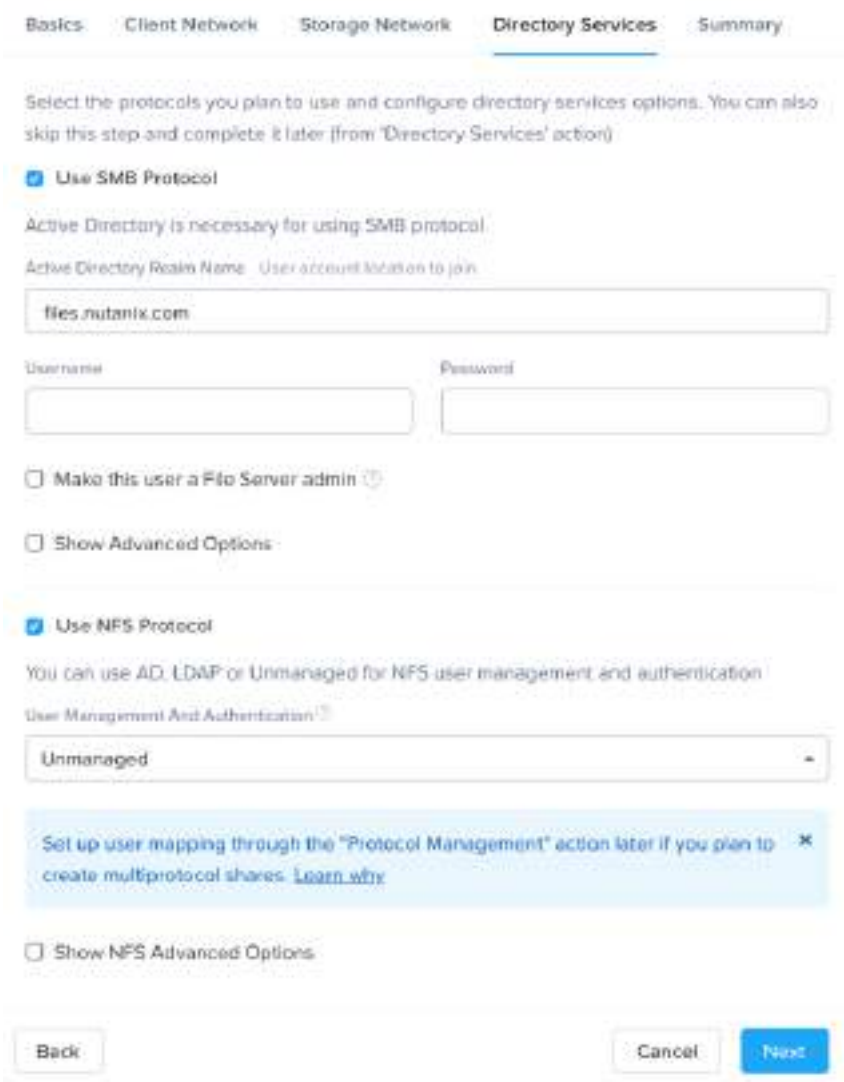


Figure 24: Create File Server: Directory Services Tab

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 436

2. If you selected the SMB protocol, do the following in the indicated fields:

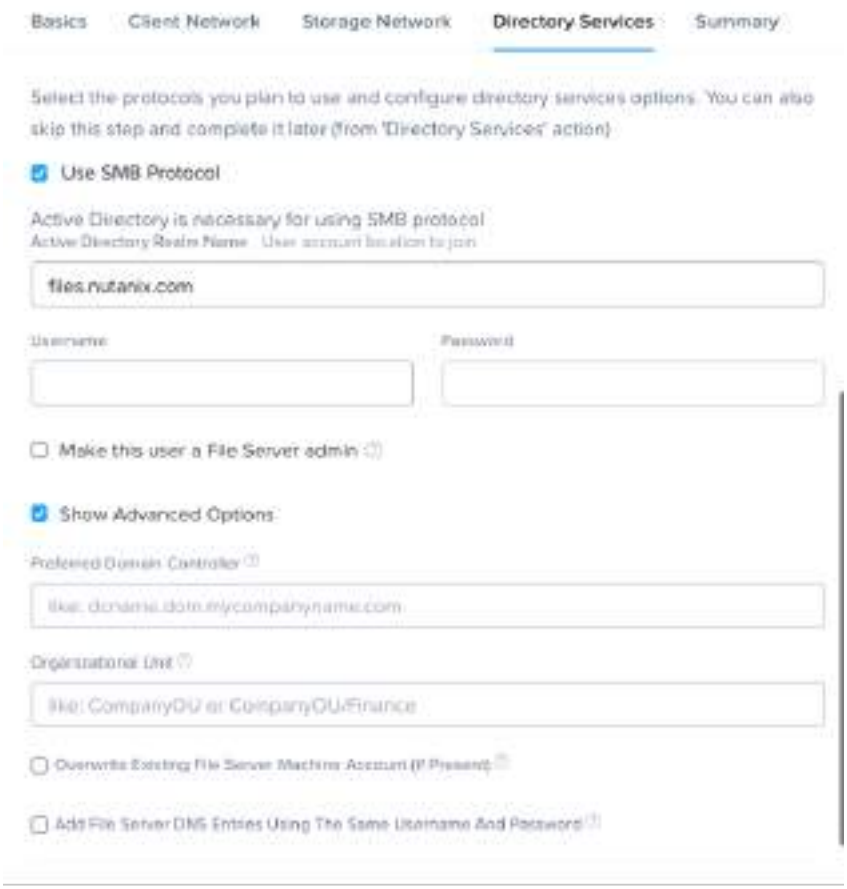


Figure 25: SMB Fields

a. **Active Directory Realm Name**: Enter the Active Directory realm name for join domain operations.

b. **Username**: Enter an AD username in the *domain*|*username* format or in the UPN format *username@ADrealm*. You must have an administrator account or the following required permissions for the relevant AD organizational unit (OU) realm:

   - **Create computer objects**: Allows the delegated admin to create a machine account in the specified OU path, which is a requirement for Files to join the domain.
   - **Read service principal names**: Helps set the service principal names (SPNs) for the machine account. Kerberos access to Files requires SPNs.

   Note:

   - Do not remove the file-server computer object in AD, as that can cause file-server services to be disrupted.
   - If the DNS domain name of the file server is different from the AD domain name, the following permission is also required:
     - Read/Write DNS host name

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 437

c. **Password**: Enter the password for the username.

d. **Make this user a File Server admin**: Check this box if you want to make this user an administrator for the file server.

e. **Show Advanced Options** (optional): Check this box to display three more fields to enter your preferred domain controller and organizational unit name for identification purposes.

f. [advanced option] **Preferred Domain Controller**: Specify a domain controller for join-domain operations in a multi-DC Active Directory configuration. Files discovers and uses a site local domain controller by default.

g. [advanced option] **Organizational Unit**: Enter your preferred organizational unit name. Files creates the machine account in the "Computers" OU container by default. If there is a **Sub-OU** field, use the following format: `parentcompanyOU/sub-ou1/sub-ou2/sub-oux`.

   For example, if the distinguished name is OU=Infrastructure, OU=Servers, OU=Test, OU=Services,DC=contoso, DC=com enter the OU path using the following format, Services/Test/Servers/Infrastructure.

   > **Note:** The default machine account password expiry period is 0, meaning the password does not expire. To update the machine account password expiry period, see Setting AD Machine Account Password Expiry on page 111.

h. [advanced option] **Overwrite Existing Files Machine Account (if present)**: Check this box to overwrite an existing machine account during the join-domain operation if one exists with the same name as the file server.

i. [advanced option] **Add Files Server DNS Entries Using the Same Username And Password**: Check this box to use AD credentials for adding DNS entries.

   Ensure that the AD user account has DNS admin rights (when using Microsoft DNS).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 438

3. If you selected the NFS protocol, select the authentication method to use from the pull-down list in the **User Management and Authentication** field and then do the following:

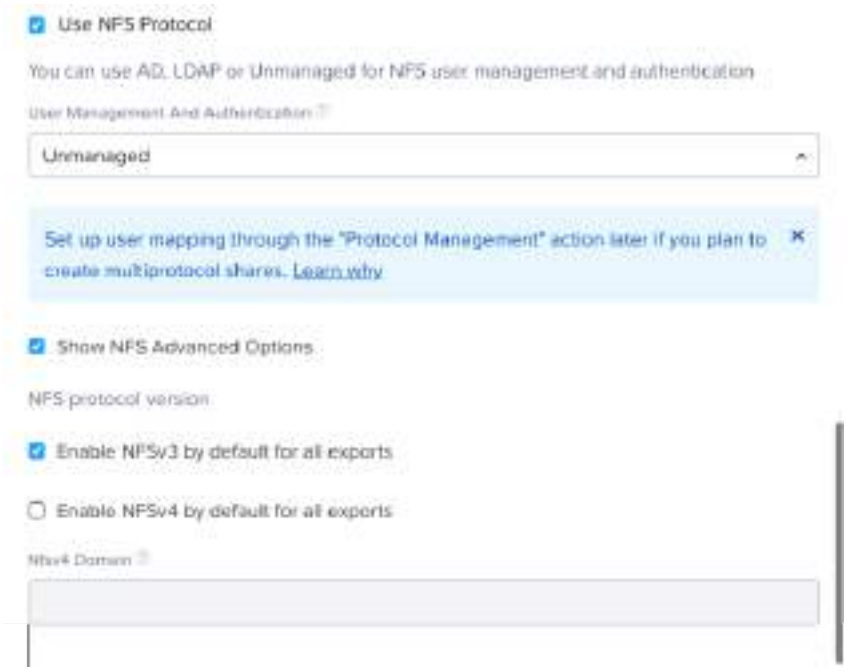


Figure 26: NFS Fields (Unmanaged + advanced options)

a. **User Management and Authentication: Unmanaged**: If you select unmanaged as the authentication method, there is nothing else to specify here.

b. **User Management and Authentication: LDAP**: If you select LDAP as the authentication method, there are several more fields:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 439

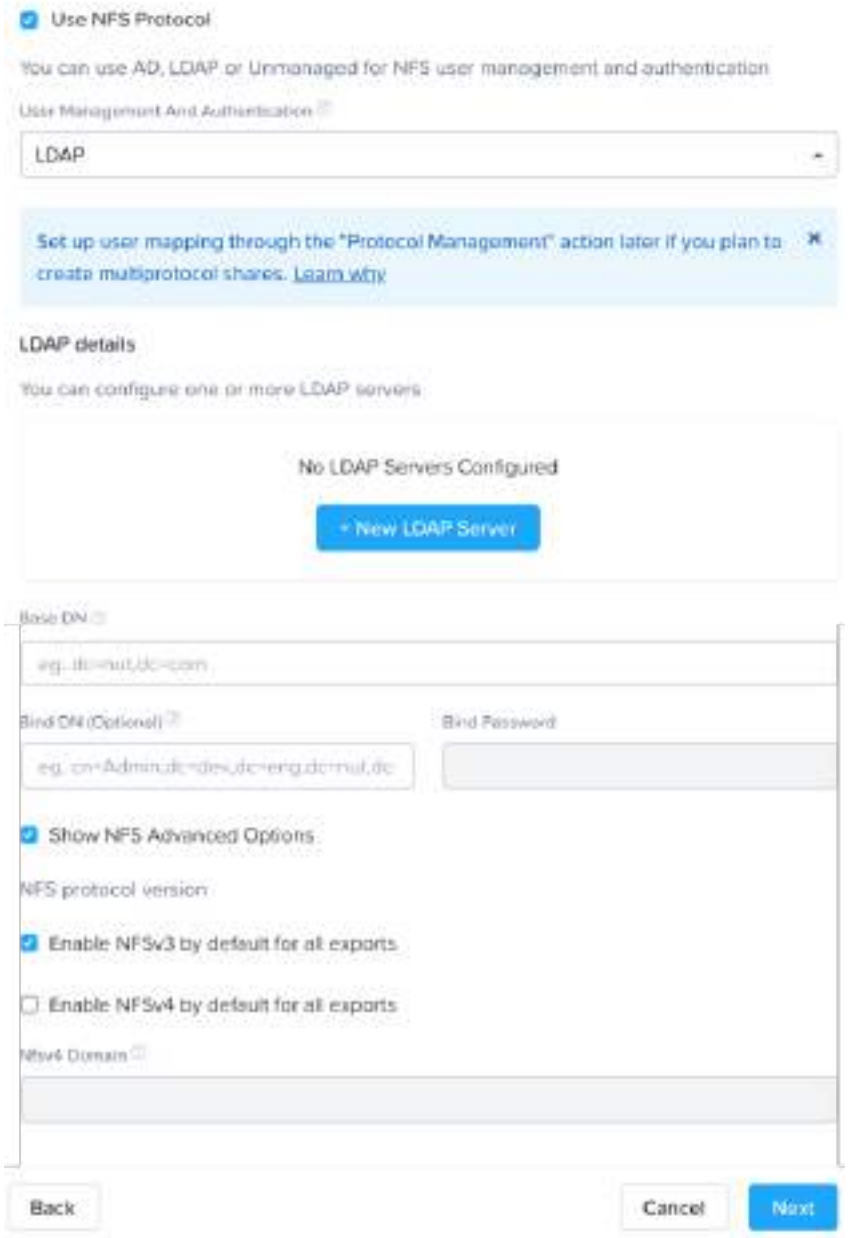


Figure 27: NFS Fields (LDAP)

- **LDAP details**: This section displays available LDAP (and LDAPS) servers. If there is no data or the target server is not listed, click the **+ New LDAP Server** button. A line appears in the table. Enter the URI address for the server in the **Server URI** column and then click **Save** in the **Action** column for that row. Repeat for any additional LDAP servers. For LDAPS servers, use the LDAPS format ldaps://ldap-servername.company.com:port.
- **Base DN**: Enter the base distinguished name (search starting point).
- **Bind DN** (optional): Enter the distinguished name at which to bind to the server.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 440

- **Bind password**: Enter the bind password.

If you configured LDAP or LDAPS settings, you may skip the next step.

c. **User Management and Authentication: Active Directory**: If you select Active Directory as the authentication method, there are several extra fields:

> **Note:** When NFS uses AD, you do not need to configure user mapping for multi-protocol access.

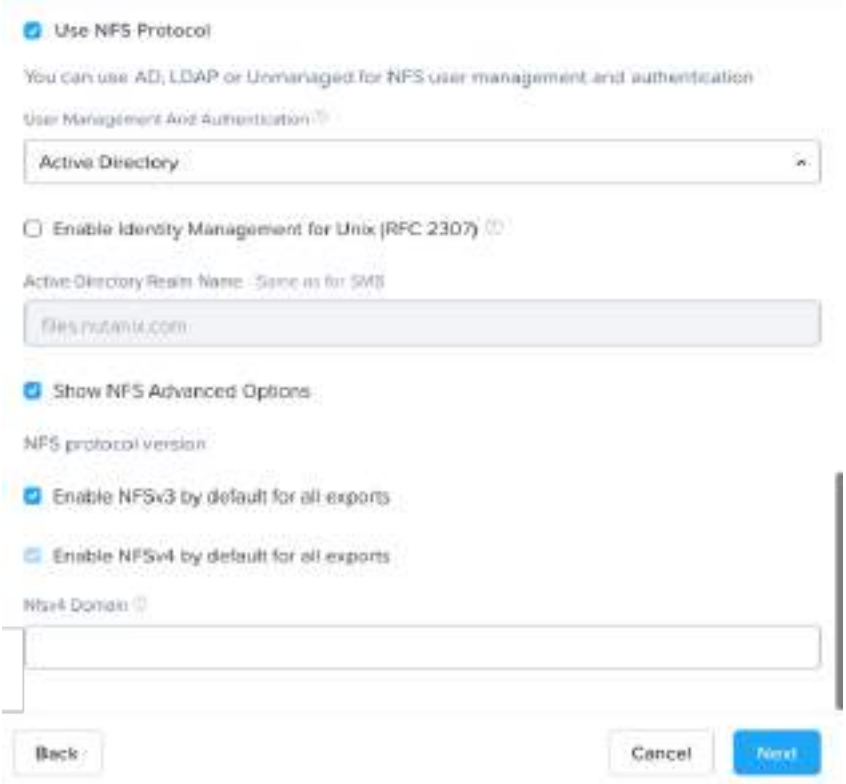


Figure 28: NFS Fields (Active Directory)

- **Enable Identity Management for Unix (RFC 2307)**: Check this box if you have RFC 2307 configured for Active Directory.
- **Active Directory Realm Name**: Displays the Active Directory realm name (read-only).

  > **Note:** If you previously configured SMB, the following fields do not appear because they are already configured for the SMB protocol.

- **Username**: Enter an AD username in the *`domain|username`* format or in the UPN format *`username@ADrealm`*. You must have an administrator account or the following required permissions for the relevant AD organizational unit (OU) realm:

  - Create computer objects
  - Read/Write service principal names

  > **Note:** If the DNS domain name of the file server is different from the AD domain name, the following permission is also required:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 441

- Read/Write DNS host name

- **Password**: Enter the password for the user.
- **Show Active Directory Advanced Options** (optional): Check this box to display the following three more fields.
- **Preferred Domain Controller**: Specify a specific domain controller for join-domain operations in a multi-DC Active Directory configuration. Files discovers and uses a site local domain controller by default.
- **Organizational Unit**: Enter your preferred organizational unit name. Files creates the machine account in the "Computers" OU container by default.

  Note: The default machine account password expiry period is 0, meaning the password does not expire. To update the machine account password expiry period, see Setting AD Machine Account Password Expiry on page 111.

- **Overwrite Existing Files Machine Account (if present)**: Check this box to overwrite an existing machine account during the join-domain operation if one exists with the same name as the file server.

d. **Show NFS Advanced Options** (optional): By default Files supports both NFSv3 and NFSv4 protocols for exports. Check this box to modify the default NFS protocol version for all exports on the file server.

   - **Enable NFSv3 by default for all exports**: Un-check to disable NFSv3 by default for all exports.
   - **Enable NFSv4 by default for all exports**: Un-check to disable NFSv4 by default for all exports.
   - In the **NFSV4 Domain** field, enter the NFSv4 domain name. Files uses the DNS domain name to map NFSv4 names to UIDs and GIDs; clients and servers must agree on the mapping.

e. When all the fields in the **Directory Services** tab are correct, click **Next**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 442

4. In the **Summary** tab, review the displayed information.

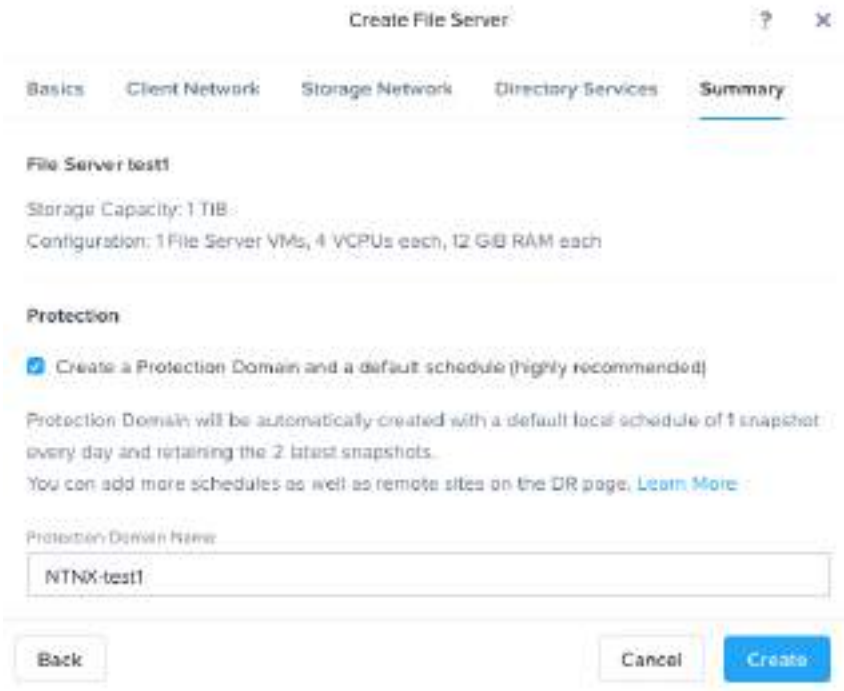


Figure 29: Create File Server: Summary Tab

   a. Review and verify the file server information you entered.

   b. The default protection domain name is NTNX-*file_server_name*, but you can change that name by entering a new name in the **Protection Domain Name** field.

   c. When all the information is correct, click **Create**.

   Creating the file server begins. Monitor the progress through the **Tasks** page. (Either select **Tasks** from the main menu or click the tasks icon and then **View All Tasks** .)

What to do next

- If you choose to add DNS entries, see Updating Domain Name System (DNS) Entries on page 114.
- On deployments using the ESXi hypervisor, disable VM monitoring. See the VMware vSphere documentation for procedures describing how to enable or disable VM monitoring.

Deleting a File Server

Delete a file server in Prism.

About this task

Do not delete FSVMs or power off a file server prior to deleting it. If you delete FSVMs, you will need to force delete the file server.

To delete a file server, do the following:

> **Caution:** Deleting a file server is permanent, and none of the deleted files can be recovered.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 443

Procedure

1. Go to the File Server view (see File Server View in Prism on page 19), select the target file server, and click the **Delete** action button.
2. In the dialog box, choose one of the following options:

   » Retain all the related entities.

   » Delete specific related entities.

   Deleting a file server deletes all the underlying user data related to that file server. However, depending on your AOS version, you may not see the option to delete the storage container and protection domain created for that file server. You can delete that storage container and protection domain manually.
3. Click the **Delete** button.

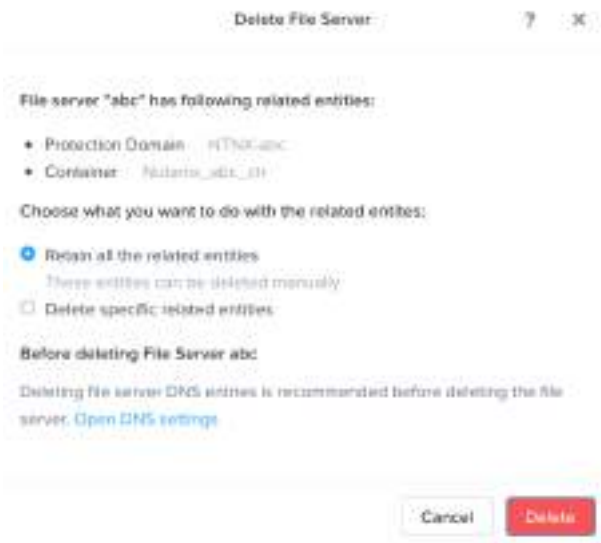


Figure 30: Delete Window

   a. If you decide to delete specific related entities, choose which entities to delete from the following options (otherwise continue to the next step):

      - **Snapshots, schedules, and protection domain**
      - **Container**
4. (Optional) delete file server DNS entries. Click **Open DNS settings**, see Updating Domain Name System (DNS) Entries on page 114.

   Deleting DNS and AD records requires administrator privileges.
5. Click **Delete**.

File Server Updates

Update or expand the configuration of an existing file server.

You can modify an existing file server in the following ways:

- Update the name, domain, or storage capacity, see Updating File Server Basics on page 63.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 444

- Update the number of file server VMs (FSVMs), see Scaling FSVMs on page 59.

  Note: You cannot update the number of FSVMs on single-FSVM deployments.

  Note: The number of CVMs must be equal to or greater than the number of FSVMs.

- Update the vCPU count and memory size for each FSVM, see Updating Memory and vCPU Resources on page 62.
- Update the network configuration (client network, storage network, domain name server [DNS], NTP server).
  - Go to the file server dashboard (see File Server View in Prism on page 19), select the target file server, and click **Network Config**. Follow the steps as indicated in File Server Updates on page 55.
- Update blocked file types, see Blocking Files on a File Server on page 141.

Updating the Network Configuration

Change the client or storage network IP address configuration of a file server (also referred to as "re-IP").

Before you begin

Stop a file server before updating the network to reduce traffic during the update process, see Stopping a Files Cluster on page 66.

About this task

To configure a virtual network for guest VMs, see "Configuring a Virtual Network for Guest VM Interfaces" in the *Prism Web Console Guide*. To modify network connections, see "Modifying Network Connections" in the *Prism Web Console Guide*.

To update the client or storage network configuration, follow the steps as indicated.

Note: Updating the network configuration requires a temporary downtime. Nutanix recommends performing network updates during off-peak hours.

Procedure

1. In the **file server** view, select the target file server.
2. In the options bar go to **Update** > **Network Configuration**.
3. Do the following in the **Update File Server Network** window.

   Note: You can change the client network, storage network, DNS, and NTP IP addresses for a file server VM. This lets you move a file server from one data center to another. If you intend on changing the domain, you must un-join the domain first.

   a. In the **Client Network** tab, verify or update the client network details (VLAN, IPv6 (optional), DNS, and NTP entries) as needed and click **Next**.

   Files displays the following message when client networks are configured on the file server: `Number` Clients Networks are configured for the file server. Only the primary network can be updated through the UI

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 445

below. Once the primary network is updated the additional clients networks already configured will be cleared. Use the CLI to re-configure additional external networks..

See Creating a File Server on page 37 for more information about these fields.

> **Note:** If you change the client network configuration, click the **file server DNS entries** link and delete the existing DNS entries (see Updating Domain Name System (DNS) Entries on page 114).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 446

Client Network | Storage Network

Set up a network which communicates between the File Server VMs as well as connectivity to DNS, AD and LDAP.

Network Details

Please remove existing file server DNS entries before changing the client network.

VLAN

vlan-143unmanaged - Unmanaged

Subnet Mask

Gateway

4 IP address(es) required

FROM	TO	NO OF IPS	ACTIONS
		4	

Add IPv6

Prefix Length

64

Gateway

Based on the cluster size, you need to provide 3 IPs. You can define one or multiple ranges by providing the starting IP and set the total number of IPs that will automatically be generatated from it.

4 IP address(es) required

FROM	NO OF IPS	ACTIONS
	4	

DNS and NTP

DNS Resolver IP (Comma Separated)

NTP Servers (Comma Separated)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 447

b. In the **Storage Network** tab, verify or update the storage network details and click **Save** .

See Creating a File Server on page 37 for more information about these fields.

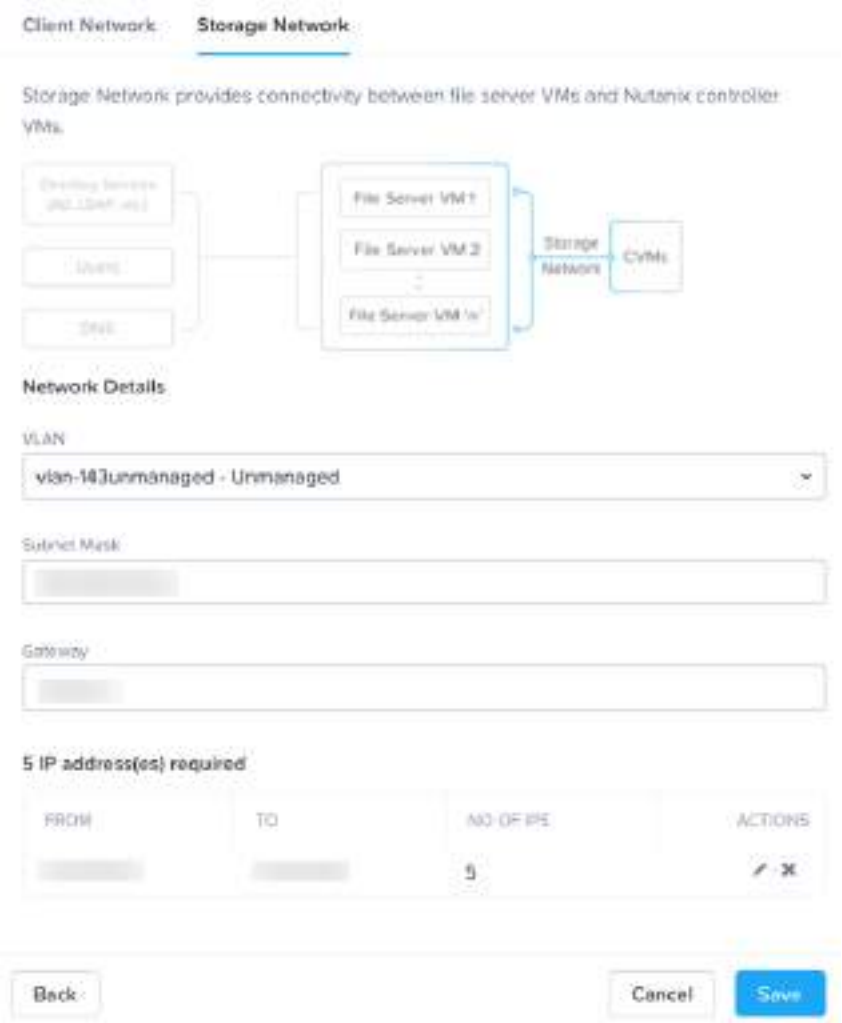


Figure 32: Update File Server Network: Storage Network tab

Note: If the network update operation is unsuccessful, use the original IP address details and try the update operation again.

Scaling FSVMs

Scale out to add new file server VMs (FSVMs) to a file server cluster or scale in to remove FSVMs.

About this task

Scale-out and scale-in operations might cause a momentary connection drop while accessing file servers. Nutanix recommends performing scale-out and scale-in operations during non-business hours.

Do the following to change the number of FSVMs.

The following limitations apply to changing the number of FSVMS:

- You cannot reduce file servers of three FSVMs.
- You cannot expand single-FSVM deployments.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 448

- Single or dual-node AOS clusters only support single-FSVM deployments.
- You can only scale in by three FSVMs at a time.

Procedure

1. In the Files Console, go to **Configuration** > **Platform**.
2. Click **Update** > **Scale Out / Scale In**.
   The **Scale Out or Scale In** window appears.
3. Under **New Capacity**, enter an integer for the new number of FSVMs.
4. Review the settings in the **Client Network** and **Storage Network** sections.

   > **Note:** For information on configuring network settings, see the client network and storage network sections in Creating a File Server on page 37.

5. Click **Update**.

Scaling FSVMs in Prism Element (PE)

Add or remove file server VMs (FSVMs) on your file server in PE.

About this task

The following limitations apply to changing the number of FSVMS:

- You cannot reduce file servers of three FSVMs.
- You cannot expand single-FSVM deployments.
- Single or dual-node AOS clusters only support single-FSVM deployments.
- You can only scale-in by three FSVMs at a time.

Do the following to change the number of FSVMs.

Procedure

1. In the **file server** view, select the target file server.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 449

2. In the options bar go to **Update** > **Scale in/out FSVMs**.
   The **Scale in/out FSVMs** window appears.

Figure 33: Scale in Scale out FSVMs

3. To expand the FSVM, click the up arrow to increase the FSVM count in **Number of file server VMs** and click **Next**.
   The **Client Network** tab appears.
4. In the **Client Network** tab, verify the client network details (VLAN ID, Subnet Mask, IP address range, No. of IP addresses) and click **Next**.
   The **Storage Network** tab appears.
5. In the **Storage Network** tab, verify the storage network details and click **Save**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 450

6. Review the settings in the **Client Network** and **Storage Network** sections.

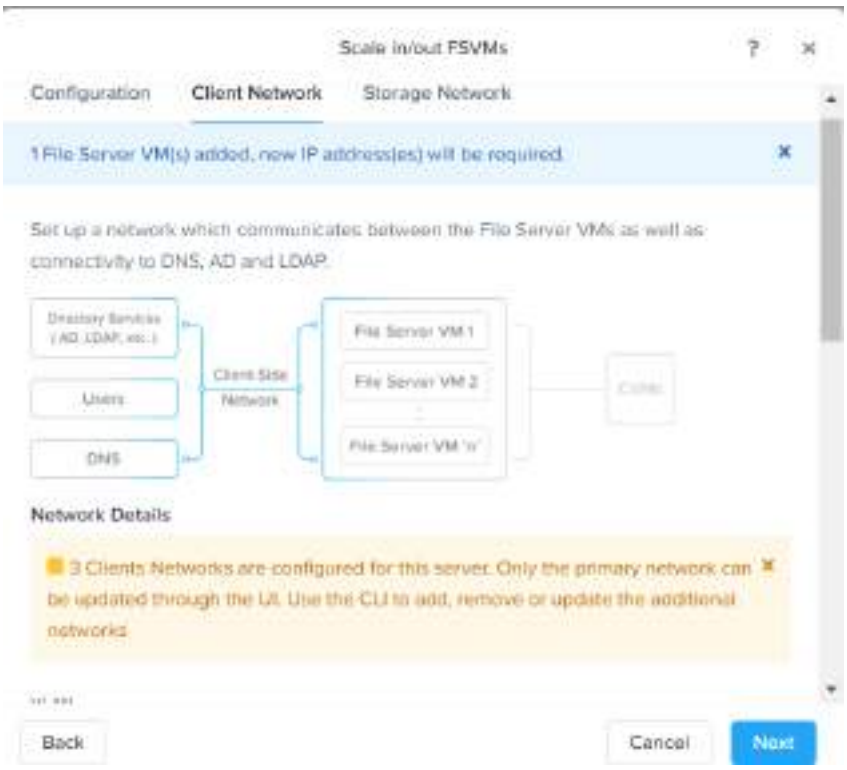


Figure 34: Update File Server Network: Client Network tab

> **Note:** For information on configuring network settings, see the client network and storage network sections in Creating a File Server on page 37.

7. Click **Next**.
8. Review the settings in the **Storage Network** section.

> **Note:** For information on configuring network settings, see the client network and storage network sections in Creating a File Server on page 37.

9. Click **Save**.

Updating Memory and vCPU Resources

Change the vCPUs and memory resources per FSVM.

Before you begin

Make sure to keep CD-ROM with ISO attached to each FSVM before updating the resources.

About this task

> **Note:** Scale-up is a non-disruptive operation, but scale-down causes system downtime.

Scale-up to add CPU and memory to the existing FSVMs. Scale-down to remove memory or CPU. To update the memory and vCPU capacity, follow the steps as indicated.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 451

Procedure

1. In the Files Console, go to **Configuration** > **Platform**.
2. Click **Update** > **Scale Up / Scale Down**.
   The **Scale Out or Scale In** window appears.
3. Do the following in the **Updated Configuration** section.
   a. In the **vCPUs** field, select the target (total) number of vCPUs for each FSVM in the cluster.

Figure 35: Scale Up/ Scale Down File Server

   b. In the **Memory** dropdown, select the target (total) number of memory (GiB) for each FSVM in the cluster.
   c. Click **Update**.

Updating File Server Basics

Update the name, the domain, and the size of a file server.

About this task

Follow the steps as indicated.

Procedure

1. Do one of the following.
   » In the Files Manager **File Server** view, select a file server and, from the **Actions** drop-down, select **Update File Server Basics**.
   » In Prism Element, click **Launch Files Console**.
2. In the Files Console, go to **Configuration** > **Platform**
3. Click **Update** > **File Server Basics**.
   The **File Server Basics** window appears.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 452

4. Do the following in the indicated fields:

   Tip: Before changing the file server or domain name, click the **Leave Domain** link to leave the current domain (see Leaving a Domain on page 113). Changing a file server name does not remove existing DNS entries, which you must remove manually.

   a. To change or update the file server name, enter the new name in the **File Server Name** field.

   b. To change the DNS domain name, enter the new name in the **Domain** field.

      Tip: After changing the file server or domain names, delete any old DNS entries from the DNS servers, add the new DNS entries (see Updating Domain Name System (DNS) Entries on page 114), and update the Directory Services configuration as needed (see Updating Directory Services on page 110).

   c. To change the size of the file server, enter a value in the **File Server Size (Logical)** field.

      Note: You cannot reduce the size of the file server. This operation does not impact current client connections.

5. When the entries are correct, click the **Update** button.

Changing an FSVM Password

Steps for updating the password of a file server VM (FSVM).

About this task

Follow the steps as indicated.

Procedure

1. Log on to a FSVM with SSH, see Logging on to a File Server VM on page 65

2. Change the Nutanix password.

```
nutanix@fsvm$ sudo passwd nutanix
```

3. Respond to the prompts, providing the current and new nutanix user password.

```
Changing password for user nutanix.
Old Password:
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

   The password must meet the following complexity requirements:

   - At least 8 characters long
   - At least 1 lowercase letter
   - At least 1 uppercase letter
   - At least 1 number
   - At least 1 special character
   - At least 4 characters difference from the old password

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 453

- Should not be among the last 10 passwords

The operation updates the password of every FSVM on the file server.

Logging on to a File Server VM

The following procedure describes how to SSH onto a file server VM (FSVM).

About this task

Procedure

1. Retrieve the IP address for the FSVM.
   a. SSH onto the CVM.
      ```
      $ ssh nutanix@CVM_IP_address
      ```
   b. Enter the CVM password.
   c. List the FSVM IP addresses.
      ```
      nutanix@cvm$ ncli fs ls
      ```
   FSVM IP addresses appear in the following format `Nvm IP Addresses: external IP,internal IP.`
2. SSH onto the FSVM using the internal IP address.
   ```
   nutanix@cvm$ ssh internal_ip_address
   ```

Setting Timezones

About this task

Set the time of your timezone for all the FSVMs.

This time zone persists across all FSVMs when Files upgrades.

Procedure

1. SSH into any FSVM in your cluster, see Logging on to a File Server VM on page 65.
2. Get the timezone for your region. The command returns your timezone into a region and city format.
   ```
   nutanix@fsvm$ afs fs.get_timezone
   ```
   > **Note:** To list all available timezones, see the contents of the `zoneinfo` file for the desired region using the `ls /usr/share/zoneinfo/region`command.
3. Set the timezone according to the output.
   ```
   nutanix@fsvm$ afs fs.set_timezone "region_name/city_name"
   ```
   Replace *region_name* and *city_name* with the region and city name specified in the timezone output. For example, afs fs.set_timezone Asia/Kolkata.

Logging on to a File Server VM

The following procedure describes how to SSH onto a file server VM (FSVM).

About this task

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 454

Procedure

1. Retrieve the IP address for the FSVM.
   a. SSH onto the CVM.
      ```
      $ ssh nutanix@CVM_IP_address
      ```
   b. Enter the CVM password.
   c. List the FSVM IP addresses.
      ```
      nutanix@cvm$ ncli fs ls
      ```
   FSVM IP addresses appear in the following format `Nvm IP Addresses: external IP,internal IP.`
2. SSH onto the FSVM using the internal IP address.
   ```
   nutanix@cvm$ ssh internal_ip_address
   ```

Starting a Files Cluster

Start a Files cluster on a CVM using the commands listed in this topic.

About this task

A deployed filer server creates multiple file server VMs (FSVMs) on the cluster. A Files cluster is a set of FSVMs. To start a Files cluster, do the following:

Procedure

1. Using SSH, log on to a Controller VM of the Nutanix cluster that deployed Files.
2. Get a list of file servers.
   ```
   nutanix@cvm$ afs info.fileservers
   ```
3. Choose to start a single file server or all file servers.
   » Start a single file server.
   ```
   nutanix@cvm$ afs infra.start fs_names
   ```
   Replace *fs_names* with the name of a single file server or with a comma-separated list of multiple file servers.
   » Start all file servers.
   ```
   nutanix@cvm$ afs infra.start *
   ```

> **Note:** For steps on stopping and starting a Nutanix cluster, see "Node Management" in the administrative guide for the target hypervisor.

Stopping a Files Cluster

Stop a Files cluster using the provided commands.

About this task

Before you stop a Nutanix cluster that is running Files, first stop the Files cluster (set of file server VMs running on the nodes). To stop a Files cluster, do the following:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 455

Procedure

1. Using SSH, log on to a Controller VM of the Nutanix cluster that is running Files.
2. List file server names.

   ```
   nutanix@cvm$ ncli file-server list
   ```

3. Stop a single file server.

   ```
   nutanix@cvm$ afs infra.stop fs_name
   ```

   Replace *fs_name* with the name of the file server.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 456

NETWORK MANAGEMENT

A file server uses internal and external networks.

During file server creation, Files requires configuring an external network for client communication and an internal (backend) network for controller VM (CVM) communication. The external client network configured during file server creation becomes the primary network, which Files uses for Active Directory (AD) and domain name system (DNS) mapping. You cannot delete the primary network, but you can modify it after file server creation by adding additional client networks, see Multi-VLAN Network Management on page 70. The Files Console only displays the primary network.

When a file server has multiple networks, the first network configured remains the primary network, unless you update the network configuration. After you add an additional network using the CLI, you can update the primary network through the user interface. Changing the primary network requires leaving the domain, which causes service disruptions.

Network management includes the following operations:

- Adding a Client Network on page 71
- Listing Client Networks on page 73
- Deleting a Client Network on page 73
- Updating the Primary Network on page 68
- Scaling Out A Multi-VLAN File Server on page 74

> **Note:** Nutanix Files does not support advanced VLAN network configurations.

Updating the Primary Network

After adding additional networks, you can update the primary client network.

About this task

Follow steps as indicated.

Before you begin

Before updating the primary network, you need to have other networks configured and you need to leave the domain. For more information, see Multi-VLAN Network Management on page 70 and Leaving a Domain on page 113.

Procedure

1. Log on to a file server VM (FSVM) with SSH, see Logging on to a File Server VM on page 65.
2. Update the primary network.

   ```
   nutanix@fsvm$ afs net.update_external_primary_network network_uuid
   ```

   Replace `network_uuid` with the network unique universal identifier (UUID) for the primary network.

What to do next

After updating the primary network, join the domain, see Joining a Domain on page 112.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 457

Managing the DNS Server

Files manages domain name system (DNS) mappings for the primary network.

Before you begin

For multi-VLAN file servers, ensure that the netmask ordering policy is enabled on the DNS server.

About this task

Files only handles DNS auto-registration and un-registration for the primary network. For a non-primary network, configure the DNS mapping manually on the DNS server. Files requires DNS registration after you perform scale out operations. Files requires you to un-register from a DNS server after you perform network delete or scale in operations.

Follow the steps as indicated to get the required DNS mapping for manual configuration:

Procedure

1. Log on to a file server VM (FSVM).
2. Get the JSON file with network information.

   ```
   nutanix@fsvm$ afs dns.get_register_info
   ```

   Note: This command creates the JSON file /tmp/tmp*file_name*.json. *file_name*, which is a temporary file name. The JSON file contains a mapping of NVM node name to the IP addresses for all of client networks.
3. (Optional) if you need to include or exclude the network IP addresses for registering to the DNS server, edit the JSON file .
4. Manually register all of the networks to the DNS server.

   ```
   nutanix@fsvm$ sudo net ads dns register_nodes --user=username jsonfilename=filename
   ```

   Replace *username* with the file server administrator. Replace *filename* with the JSON file containing the network information.
5. (Optional) check the configured DNS mappings.

   ```
   nutanix@fsvm$ afs dns.verify_external_networks show_reverse_ptr_records=true
    external_network_uuid=external_network_uuid
   ```

   Replace *external_network_uuid* with the unique user identifier (UUID) of the manually configured external network.

Network Segmentation

Deploying Files in a Volumes network segmented environment isolates the file server communication between FSVMs and CVMs onto a dedicated subnet, a Volumes segment.

Important: Before using network segmentation with Files, meet the following conditions.

- Enable network segmentation for Nutanix Volumes, see "Service-Specific Traffic Isolation" and "Service-Specific Settings and Configurations" section in the *AOS Security Guide*.

Consider using network segmentation with Files for the following use cases:

- You do not have enough IP addresses in the management network of CVM to allocate them for Files internal network. Also, you do not want to use the IP addresses from another routable subnet for Files

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 458

internal IP address as you have set up firewall rules and do not want data traffic (iSCSI) between Files and CVM to go through firewalls.

- You have networks with varying capacity, and you want to use the one with maximum bandwidth for storage and the one with lesser bandwidth for management. For example, 10G network for storage and 1G network for management.

Network segmentation enhances security, resilience, and cluster performance by isolating a subset of traffic to its own network. By configuring network segmentation on a cluster, Files does the following:

- Files storage data uses its own network, segmented from other services as well as from the cluster backplane.
- Files management uses its own network, segmented from default management network on the cluster.

> **Note:** Files only supports using network segmentation with Nutanix Volumes.

To deploy Files in a Volumes network segmented environment, see Deploying Files with Network Segmentation on page 70.

Deploying Files with Network Segmentation

Steps for deploying Files in a Volumes network-segmented environment.

Before you begin

Make sure you have met the requirements for network segmentation, see Network Segmentation on page 69.

About this task

To deploy Files in a Volumes network-segmented environment, do the following:

Procedure

1. Enable Volumes network segmentation on the AOS cluster.

   For more information, see the "Service-Specific Traffic Isolation" and "Service-Specific Settings and Configurations" sections in the *AOS Security Guide*.

2. During deployment, configure the Files storage network in the same subnet as Volumes network segment.

   > **Note:** To use network segmentation on existing file servers, re-IP the storage network to a Volumes network segment subnet.

Multi-VLAN Network Management

Management of multiple client networks after file server deployment.

You can configure multiple non-routable client networks on a single file server. You can also configure share access over a subset of configured client networks. Only file servers configured in a dual-VLAN network state support multi-VLAN networks.

The following non-exhaustive list describes some instances when a multi-VLAN network is an appropriate solution:

- A single client network runs out of IP addresses.
- Logical isolation on a single client network becomes complex.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 459

- Routing traffic from multiple client networks to a single client network leads to complex routing and firewall management.
- Multi-tenancy of client networks requires a multi-VLAN configuration.

> **Important:** Ensure that you create an unmanaged network with VLAN ID = 0 for AHV, or, for the ESXi hypervisor, create an unmanaged network with VLAN ID = 4095. For information on creating a network on the AHV hypervisor, see *Network Management*. For information on creating VLAN4095 on ESXi, see the *vSphere Administration Guide for Acropolis*.

Notes and Limitations

Consider the following limitations before deploying files on a multi-VLAN network:

- You can have a maximum of 10 client networks.
- File servers configured in a single-VLAN network state do not support multi-VLAN.
- Only IPv4 networks support multi-VLAN (IPv6 networks do not). If you have already configured an IPv6 network, remove the IPv6 network before using multi-VLAN.
- You cannot add storage or Controller VM (CVM) networks as client networks.
- Nutanix on AWS does not support multi-VLAN.
- An active multi-VLAN configuration has the sysctl parameter enabled (arp_ignore=2). An in-active multi-VLAN confiugation has the arp_ignore parameter disabled (arp_ignore=0).

By default, support of multiple VLANs for a single-file-server deployment only applies to VLANs existing on a single virtual switch, determined by the native network associated with the external interface (eth1) of the FSVM. When configuring VLANs from multiple switches, allow L2 traffic across physical switches.

> **Note:** Nutanix Files does not support advanced VLAN network configurations.

Adding a Client Network

Add additional client networks to a file server.

Before you begin

Before you can add a network to a file server, you must configure the network on the CVM. For more information see the *AHV Administration Guide* and the vSphere Administration Guide for Acropolis.

About this task

To add client networks, do the following:

Procedure

1. Log on to the CVM using SSH.

```
ssh nutanix@cvm_ip_address
```

2. To discover existing networks on the CVM, list existing client networks.

```
nutanix@cvm$ acli net.list
```

3. Log on to a file server VM (FSVM) with SSH, see Logging on to a File Server VM on page 65.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 460

4. Add a client network from one of those configured on the CVM.

```
nutanix@fsvm$ afs net.add_external input-json-file-path
```

Replace *input-json-file-path* with the file path to a local JSON that contains the input parameters file.

Refer to the following JSON template.

```
[
  {
    "virtual_network_uuid": "virtual_network_uuid",
    "gateway_ip": "gateway_ip",
    "netmask_ip": "netmask_ip",
    "ip_list": [
      "ip_address",
      "ip_address",
      "ip_address"
    ]
  }
]
```

```
For multiple virtual switches that contain networks with the same VLAN ID, refer to
 the following JSON template.

 [
    {
      "virtual_network_uuid": "virtual_network_uuid",
      "trunk_virtual_network_uuid": "trunk_virtual_network_uuid",
      "gateway_ip": "gateway_ip",
      "netmask_ip": "netmask",
      "ip_list": [
        "ip_address",
        "ip_address",
        "ip_address"
      ]
    }
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 461

```
  ]
```

For managed networks, the JSON only requires the *virtual_network_uuid* field. For unmanaged networks, the JSON also requires *gateway_ip*, *netmask_ip*, and ip_list fields. The number of *ip_address* entries should match the number of FSVMs on the file server.

> **Note:** For ESXi, use `nutanix@CVM$ acli uhura.network.list` to list UUIDs.

Replace *virtual_network_uuid* with the universal unique identifier for the CVM network you want to add from the list in step 2.

For multiple virtual switches that contain networks with the same VLAN ID, provide the *trunk_virtual_network_uuid* .

> **Note:** The *trunk_virtual_network_uuid* should match the primary network in the same virtual switch.

Replace *gateway_ip* with the gateway IP address for the CVM network you want to add from the list in step 2.

Replace *netmask_ip* with the netmask IP address for the CVM network you want to add from the list in step 2.

> **Note:** The IP addresses must be sequential.

> **Important:** When using a distributed virtual switch (DVS) with ESXi, add both of the following additional parameters to the JSON: to explicitly specify the VLAN ID for the network, add `"vland_id"`, and to explicitly specify the trunk virtual network add `"trunk_virtual_network_uuid"`.

> **Note:** Use the `afs help net.add_external` command to view the JSON file format.

Listing Client Networks

Lists the configured client networks on the file server.

About this task

To list the client networks, do the following:

Procedure

1. Log on to a file server VM (FSVM) with SSH, see Logging on to a File Server VM on page 65.
2. List the configured external client networks.
   ```
   nutanix@fsvm$ afs net.list_external
   ```
   A list of configured networks appears.

Deleting a Client Network

Remove configured client networks from a file server.

About this task

To remove a client network, do the following:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 462

Procedure

1. List existing client networks, see Listing Client Networks on page 73.
2. Log on to a file server VM (FSVM) with SSH, see Logging on to a File Server VM on page 65.
   a. To delete networks, list the universally unique identifiers (UUIDs).

      ```
      nutanix@fsvm$ afs net.delete_external network_uuid_list [key=val ...]
      ```

      Replace *network_uuid_list* with a comma-seperated list of network UUIDs for the networks you want to delete.

      > **Note:** To view a list of network UUIDs, use the `afs net.list_external` command.

Scaling Out A Multi-VLAN File Server

Add additional networks to scaled out FSVMs.

About this task

Scaling out FSVMs configures the new nodes with the primary network only, which creates a partial network state on the file server. In a partial network state, you cannot create shares or rebalance volume groups (VGs). (But you can perform upgrade and scale-in tasks.) To add the remaining non-primary networks to the scaled out nodes, use the network patch operation.

To scale out a multi-VLAN file server, follow the steps as indicated.

Procedure

1. List existing client networks, see Listing Client Networks on page 73.
2. Add FSVMs to the cluster, see Scaling FSVMs on page 59.
   After adding FSVMs, the **Alerts** tab displays the following: The file server is in a partial network state.
3. Log on to a file server VM (FSVM) with SSH, see Logging on to a File Server VM on page 65.
4. Resolve the partial network state using a JSON file that includes details of the remaining networks.

   ```
   nutanix@fsvm$ afs net.patch_external input-json-file
   ```

   Replace *input-json-file* with the path to a local JSON file formatted as indicated in the following template:

   ```
   [
     {
       "uuid": "uuid",
       "ip_list": [
         "ip_address",
         "ip_address"
       ]
     },
     {
       "uuid": "uuid"
     }
   ]
   ```

   For unmanaged networks, replace the *uuid* with the universally unique identifier (UUID) of the network and replace *ip_address* with IP addresses for the network, adding as many comma separated values

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 463

as newly added FSVMs. For managed networks, only replace the *uuid*. The above template includes parameters for an unmanaged and a managed network.

> **Important:** For distributed virtual switch support on ESXi, also add the "trunk_virtual_network_uuid" parameter and provide the details.

> **Note:** You can also use the `afs help net.patch_external` command to view the JSON file format.

Performing the procedure resolves The file server is in a partial network state alert.

Configuring Client Exceptions

Configure the client networks exception list for exports and shares.

About this task

Configuring client exceptions defines the share availability on a subset of client networks. By default, all shares are available on all client networks. After you have added multiple client networks, the shares can be made available only on a subset of configured client networks.

> **Note:** Client exception values created using a command-line interface (CLI) do not appear in the UI.

Procedure

To configure client exceptions for SMB shares, do the following:

a. Log on to an FSVM with SSH.

b. Allow the client networks subset exceptions for an SMB share:

```
nutanix@fsvm$ afs smb.client_exceptions <smb-share-name> whitelist
 ip_net_list=<subnet1>,<subnet2>
```

Replace *smb-share-name* with the name of the SMB share.

Replace *subnet1* and *subnet2* with the subnet IP addresses in classless inter-domain routing (CIDR) notation.

> **Note:** For more information, see Share and Export Management on page 77.

Configuring NFS Client Exceptions

Procedure

To configure client network exceptions for NFS exports, do the following:

a. From the **File Server** view in Prism Element (PE), click **Launch Files Console**.

b. From the File Console, select an NFS share and click **Update**.

c. Provide the required information in the **Basics** tab.

d. Change **Default Access** to No Access in the **Settings** tab.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 464

e. Click **Add Exceptions**, and then add the subnets in CIDR format in **clients with read-only access** and **clients with read-write access**.

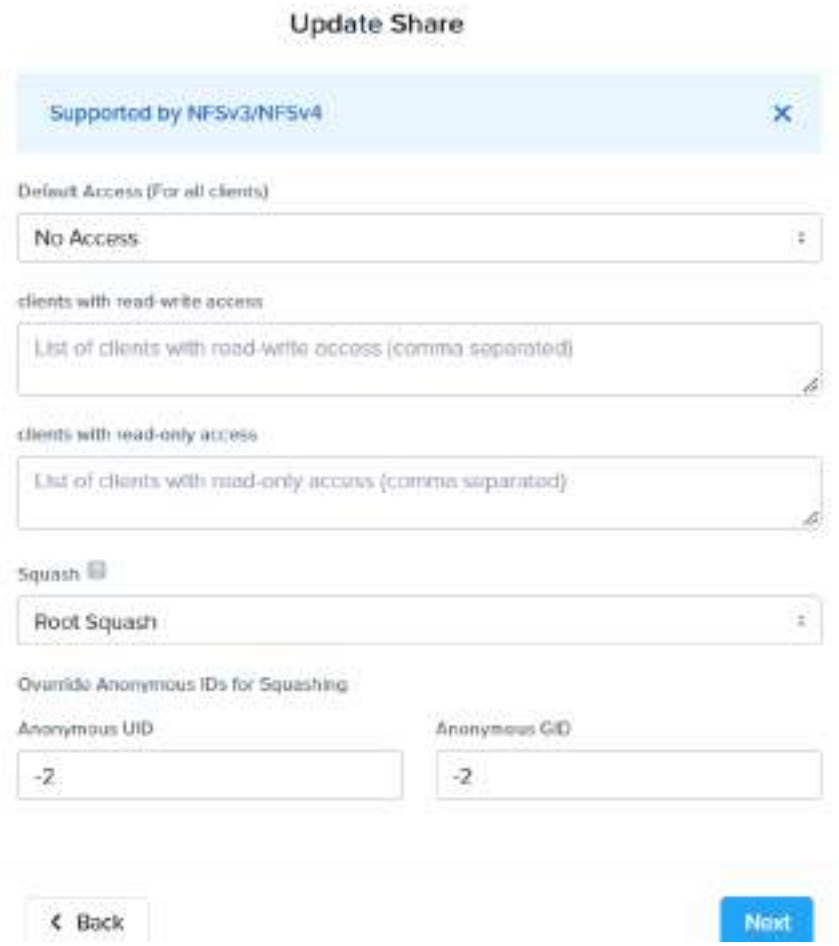


Figure 36: Update NFS Share

f. Click **Next** to view the **Summary** tab.

g. Verify the details on the **Summary** tab and click **Update**.

> **Note:** For more information, see Share and Export Management on page 77.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 465

SHARE AND EXPORT MANAGEMENT

Before creating a share or export, review the available features and configurations.

You can create file shares (SMB), exports (NFS), or multi-protocol shares for a file server.

You have the option of creating distributed or standard shares and exports. A distributed share or export is the repository for the personal files of a user, and a standard share is the repository shared by a group. A distributed share or export distributes data across all file server VM (FSVM) in a cluster, while standard shares store all data on a single FSVM. You can store files in the root directory of a distributed NFS share but not in the root directory of a distributed SMB share. For information about share and export permissions, see Permissions on page 108.

To create a share or export, see one of the following:

- Creating an SMB Share on page 77
- Creating an NFS Export on page 83
- Creating a Multi-Protocol Share or Export on page 90

Limitations

The following limitations apply to shares and exports:

- Distributed shares are only available on deployments of three or more FSVMs.
- Do not use Windows Explorer to create new top-level directories, as you then cannot rename any folders created with the default New Folder name (see Troubleshooting on page 193).
- Windows clients do not support using UTF8 encoding for naming files and directories on NFSv3 exports.
- You cannot access top-level directories (TLDs) or shares through the FSVM short name.
- You cannot modify TLDs from Mac clients.
- Files does not support custom extended attributes (EA) on SMB shares.
- For a list of additional limitations, see Configuration Maximums.

Creating an SMB Share

About this task

Create an SMB share.

> **Note:** Nutanix recommends using multi-protocol shares for mounting SMB shares to Linux clients, see Creating a Multi-Protocol Share or Export on page 90.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 466

Procedure

1. Go to the **Shares** view in the Files Console and click **+New Share or Export**.

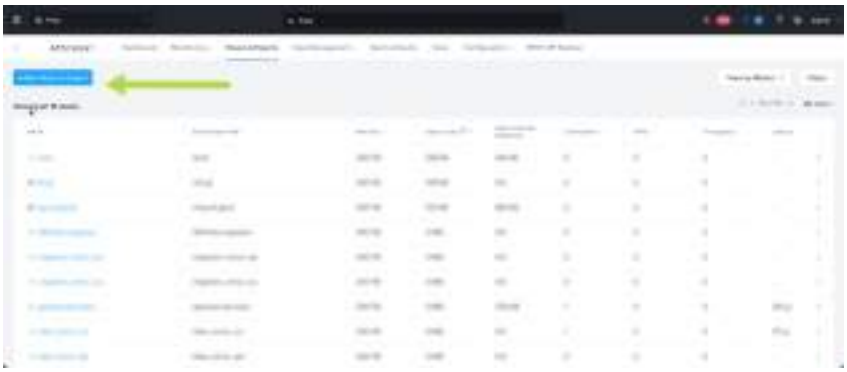


Figure 37:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 467

2. The **Create a Share** window appears and displays the **Basics** tab. Do the following in the indicated fields:

   a. **Name**: Enter a name for the share.

      Note the following naming conventions:

      - Files does not allow the following names:
        - `Global`
        - `Printers`
        - `admin$` (reserved)
        - `ipc$` (reserved)
        - `homes` (reserved)
      - Share names are not case-sensitive.
      - Each share name must be unique.
      - A share name must not start or end with a blank space.
      - A share name must not start with a dot (.)
      - A share name must follow a regular expression: `^[^!@#%~'\"^&$()\\[\\]|+=*{}\\/\\\ \<>:;,’`]*[$]?$`
      - Names that end with the $ are hidden shares.
      - See Configuration Maximums for name length limits.

   b. **Description** (optional): Enter a description for the share.

   c. **Share path** (optional): You can create nested shares by specifying the path. Nested shares inherit some properties from the parent directory. See Nested Shares and Exports on page 105 for details.

   d. **Max Size** (optional): Enter the maximum share size in GiB, see Configuration Maximums for size limit details.

      Leaving the field blank means there is no upper limit to the size of the share. If you want to set an upper size limit, enter a value. Setting a value changes the capacity in the client view.

   e. **Primary Protocol Access**: Select the **SMB (Ideal for Windows Clients)** option.

   f. **Enable multi-protocol access for NFS clients**: Check the box to enable the multi-protocol feature. Follow the steps in Creating a Multi-Protocol Share or Export on page 90 to configure multi-protocol settings. Otherwise, continue to the next step.

      > **Note:** For information on the multi-protocol feature, see Multi-Protocol Support for Files on page 95.

   g. Click **Next**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 468

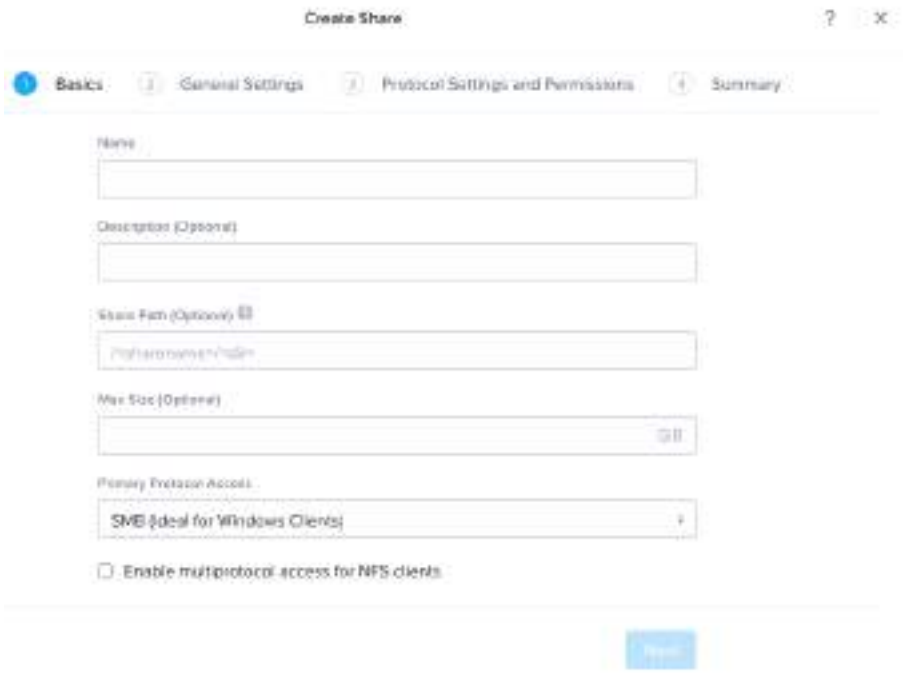


Figure 38: Create a Share: Basics tab

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 469

3. In the **General Settings** tab, do the following in the indicated fields:

   a. Check the **Use "Distributed" share type instead of "Standard"** to create a distributed share:

      Note: Shares on single-FSVM deployments are standard by default.

      - A *Distributed share*, also known as a home share, load-balances user data across multiple FSVMs by distributing top-level directories.
      - A *Standard share*, also known as a general-purpose share, serves data and connections from a single FSVM.

      A distributed share is frequently used as the repository for the personal files of a user, while a standard share is frequently the repository shared by a group.

      Tip: When using a distributed share for user profiles, facilitate better load distribution by creating a top-level directory (TLD) for each user.

   b. **Enable Self Service Restore**: Check this box to enable snapshots of the share contents, see Self-Service Restore on page 176.

   c. **Enable Compression:** Check this box to save space and reduce data on the share through in-line compression of written data, see File System Compression on page 156.

      Note: Enabling compression at the container level makes the **Enable File System Compression** option unavailable. The option does not appear on clusters upgraded from earlier versions that do not support file system compression.

   d. **Blocked File Types**: Check this box to block files with specific character patterns in their names, see File Blocking for more information.
   A field appears for blocked file types. Enter a comma-separated list of character patterns of directories and file names blocked from the share.

   e. Click **Next**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 470

4. In the **Protocol Settings and Permissions** tab, follow the steps as indicated.

   a. **Enable Access Based Enumeration (ABE)**: Check this box to restrict user access when browsing the contents of top-level directories to only those files and folders that they have access permissions for, see Access-Based Enumeration (SMB only) on page 139.

   b. **Allow Long Names for Files and Folders:** Check this box to let users create file names up to 1023 bytes (255 characters) long.

   c. **Encrypt SMB3 Messages:** Check this box to enable message encryption between the file server and client. See Encryption on page 139.

   d. **SMB Continuous Availability (CA):** Check this box to enable CA on the share, see Continuously Available Shares (SMB Only) on page 100.

   e. **Share Permissions (SMB):** This section displays the default share permissions for all users and groups on the share.

      (Optional) To customize the permissions, click **Add User or Group**.

      - In the **User or Group** column, specify whom to apply the target permissions to. Specify a user or a group in the sAMAccountName or NETBIOS\sAMAccountName format where sAMAccountName shares the domain with the file server.
      - In the **Type** column, specify to **deny** or **allow** the target user or group.
      - Specify the denied or allowed actions for the target user or group in the **Read**, **Change**, and **Full Control** columns.
      - Click the **check mark** icon to add the permissions, or click the **x** icon to remove the permissions.

      For more information about permission assignment, see Permissions on page 108.

   f. Click **Next**.

5. In the **Summary** tab, review the following details in the indicated fields:

Table 19: Basics

Property	Configuration
Share name	The name of the new share
Share path	The file path to the new share
Primary protocol	SMB
Multi-protocol access	Disabled
Share or export type	Distributed or standard
Self service restore	Enabled or disabled
Blocked file types	Enabled or disabled
Share compression	Enabled or disabled

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 471

Property	Configuration
Continuous availability	Enabled or disabled

Table 20: Protocol Access

Property	SMB Clients
Authentication	Authentication type (Kerberos, AD, etc)
Client Access	Read-write **Note:** For SMB shares, SMB client access is always read-write.
Long Names for Files and Folders	Allowed or not allowed
ABE	Disabled or enabled
Message Encryption	Disabled or enabled

Table 21: Sharing Permissions (SMB)

User or Group	Type	Permissions
Everyone, [user name], or [group name]	Allow or deny	Read, change, or full control

6. When all the information is correct, click **Create**.

What to do next

Map the newly created share in your name-space.

Creating an NFS Export

Administrators can create exports using the file server dashboard.

About this task

Follow the steps as indicated to create an export (NFS).

Note: Files does not support mounting NFSv4 exports on Windows clients. Use NFSv3 exports or multi-protocol shares.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 472

Procedure

1. Go to the **Shares** view in the Files Console and click **+New Share or Export**.

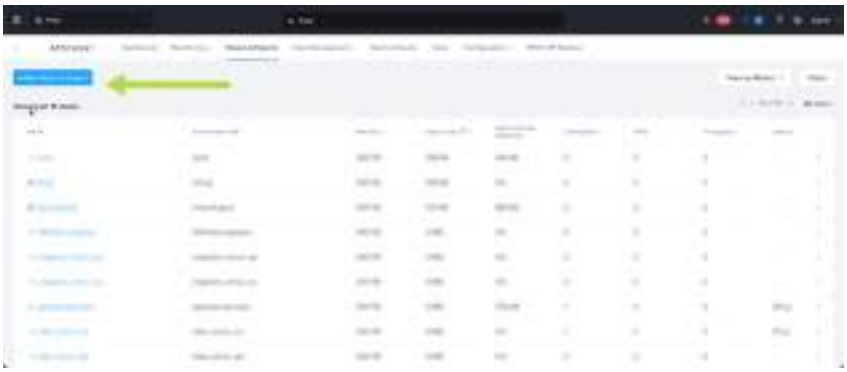


Figure 39: Create a New Share Button

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 473

2. The **Create a Share** window appears and displays the **Basics** tab. Do the following in the indicated fields:

   a. **Name**: Enter a name for the share.

      Note the following naming conventions:

      - Files does not allow the following names:
        - `Global`
        - `Printers`
        - `admin$` (reserved)
        - `ipc$` (reserved)
        - `homes` (reserved)
      - Names are not case-sensitive.
      - Each name must be unique.
      - Files allows unicode characters.
      - A blank space or space character cannot appear as the first or last character in the name.
      - Names that end with the $ are hidden shares.
      - See Configuration Maximums for name length limits.

   b. **Description** (optional): Enter a description for the share.

   c. **Share path** (optional): You can create standard nested shares by specifying the path. Nested shares inherit some properties from the parent directory. See Nested Shares and Exports on page 105 for details.

   d. **Max Size** (optional): Enter the maximum share size in GiB, see Configuration Maximums for size limit details.

      Leaving the field blank means there is no upper limit to the size of the share. If you want to set an upper size limit, enter a value. Setting a value changes the capacity in the client view.

   e. **Primary Protocol Access**: Select the **NFS** option.

   f. **Enable multi-protocol access for SMB clients**: Check the box to enable the multi-protocol feature. Follow the steps in Creating a Multi-Protocol Share or Export on page 90 to configure multi-protocol settings. Otherwise, continue to the next step.

      > **Note:** For information on the multi-protocol feature, see Multi-Protocol Support for Files on page 95.

   g. Click **Next**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 474

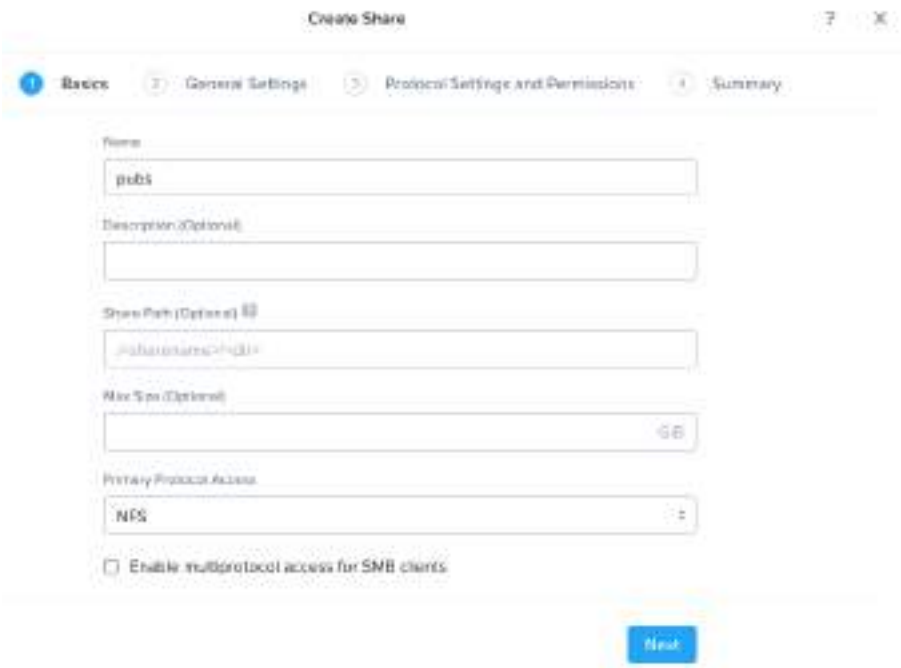


Figure 40: Create a Share: Basics tab

3. In the **General Settings** tab, do the following in the indicated fields:

   a. Check the **Use "Distributed" share type instead of "Standard"** to create a distributed share:

      Note: Shares on single-FSVM deployments are standard by default.

      - A *Distributed share*, also known as a home share, load-balances user data across multiple FSVMs by distributing top-level directories.
      - A *Standard share*, also known as a general-purpose share, serves data and connections from a single FSVM.

      A distributed share is frequently used as the repository for the personal files of a user, while a standard share is frequently the repository shared by a group.

      Tip: When using a distributed share for user profiles, facilitate better load distribution by creating a top-level directory (TLD) for each user.

   b. **Enable Self Service Restore**: Check this box to enable snapshots of the share contents, see Self-Service Restore on page 176.

   c. **Enable Compression:** Check this box to save space and reduce data on the share through in-line compression of written data, see File System Compression on page 156.

      Note: Enabling compression at the container level makes the **Enable File System Compression** option unavailable. The option does not appear on clusters upgraded from earlier versions that do not support file system compression.

   d. **Blocked File Types**: Check this box to block files with specific character patterns in their names, see File Blocking for more information.
   A field appears for blocked file types. Enter a comma-separated list of character patterns of directories and file names blocked from the share.

   e. Click **Next**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 476

4. In the **Protocol Settings and Permissions** tab, follow the steps as indicated.

   a. **Authentication**: Select the authentication method from the pull-down list.

      The authentication options are **None**, **System**, **Kerberos 5**, **Kerberos 5i**, and **Kerberos 5p**.

      For LDAP or an unmanaged directory service, use none or system authentication – both are client-based but have different authorization rules. For AD, you can use none, system, or user-based authentication with Kerberos.

      See Directory Services and Authentication on page 109 for more information.

      > **Note:** Files does not support Kerberos 5, Kerberos 5i, and Kerberos 5p with the NFSv3 protocol.

      > **Note:** Changes to the authentication method can result in invalid mounts. Resolve the issue by remounting the authentication type as a value for parameter sec in the mount command on the client. Example: "-o sec=krb5" if you change the export authentication type to Kerberos 5.

   b. **Default Access (For all clients)**: Select the default access permissions from one of the following in the pull-down list:

      - **Read-Write**: Client can mount the export and write to it.
      - **Read-Only**: Client can mount the export and read data but not write to it.
      - **No Access**: Client cannot mount the NFS export nor read or write from it.

   c. **Squash**: Select the squash value from the pull-down list. The squash option controls the access privileges of root client users (users with UID 0). The **None** value gives root users super-user access privileges to the export, letting them create, edit, and delete files from any user. The **Root Squash** value disables super user access and maps all roots users to anonymous users. The **All Squash** value maps all users to anonymous ones.

   d. **Override anonymous IDs for squashing**: check this box to enter anonymous user identifier (UID) and group identifier (GID) value other than the default value. Both the anonymous UID and GID default have a default value of -2.

      - **Anonymous UID**: Enter the anonymous user identifier value for the export.
      - **Anonymous GID**: Enter the anonymous group identifier value for the export.

      You can map regular users to anonymous ones to restrict access to the NFS export. Setting the NFS authentication type to **None** maps all client users to anonymous ones.

   e. **Add Exceptions** (optional): If you want to refine the read, write, and no-access permissions to other than the the default, click the **Add Exceptions** link.

      The **Add Exceptions** dialogue box displays **Clients**, **Access**, and **Squash** fields. In the **Clients** fields, enter a comma separate list of clients for the target **Access** permission level. Exceptions

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 477

take precedence over the default, so any client listed in one of the exception fields gets that level of permission instead of the default permission.

For IPv4 clients, exceptions can be complete IP addresses, wildcards, or subnets. For IPv6 clients, Files only accepts complete IP addresses as exceptions. Use one of the following formats:

- Absolute IPs (for example 129.144.0.0)
- Hostname of client (for example client.domain.com)
- CIDR format for specifying subnets (for example 129.144.0.0/24)
- Netgroups (for example @it_admin)

  Note: Netgroups can limit access to hosts, but Files does not support Netgroups that limit access to users. If you add or remove a client from a Netgroup, it reflects on the client after 30 minutes.

- Wildcards (for example clients*.domain.com).

  Note: To use wildcards, configure reverse domain name system (DNS) records for the clients.

Caution: If a client IP address matches more than one exception rule, the client may experience access issues.

Once you add an exception, it appears on the **Protocol Settings and Permissions** tab under **Exceptions for Client Access**.

For more information about permission assignment, see Permissions on page 108.

5. Click **Next**.
6. In the **Summary** tab, review the following details in the indicated fields:

Table 22: Basics

Property	Configuration
Share name	The name of the new export
Share path	The file path to the new export
Primary protocol	NFS
Multi-protocol access	Disabled
Share or export type	Distributed or standard
Self service restore	Enabled or disabled
Blocked file types	Enabled or disabled
Share compression	Enabled or disabled
NFS version	NFSv3 or NFSv4
Continuous availability	Enabled or disabled

Table 23: Protocol Access

Property	NFS Clients
Authentication	System or none

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 478

Property	NFS Clients
Client Access	Read-write or read-only
Squash	All squash, root squash, or none

7. When all the information is correct, click the **Create** button.

Creating a Multi-Protocol Share or Export

Create a multi-protocol share or export.

About this task

> **Note:** Multi-protocol feature is not supported on the shares which are already enabled with longname.

For information on the multi-protocol feature, see Multi-Protocol Support for Files on page 95. Perform the following steps as indicated to create a multi-protocol a share or export.

Procedure

1. Go to the **Shares** view in the Files Console and click **+New Share or Export**.

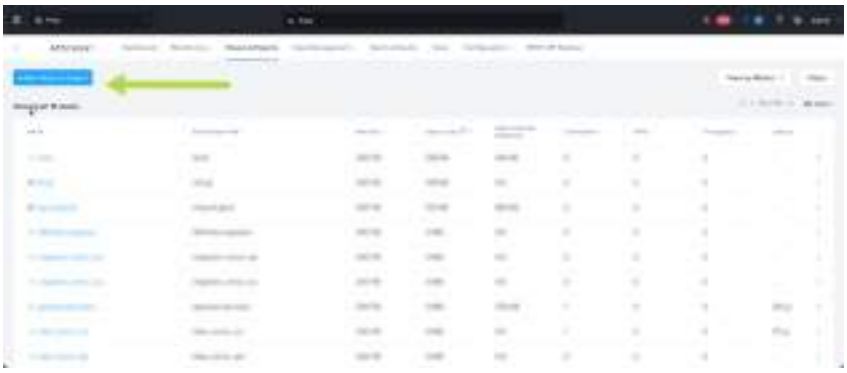


Figure 41: Create a New Share Button

The **Basics** tab

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 479

2. Do the following in the indicated fields:

   a. **Name**: Enter a name for the share or export.

      Note the following naming conventions:

      - Files does not allow the following names:
        - `Global`
        - `Printers`
        - `admin$` (reserved)
        - `ipc$` (reserved)
        - `homes` (reserved)
      - Names are not case-sensitive.
      - Each name must be unique.
      - Files allows Unicode characters.
      - You cannot use a blank space or space character as the first or last character in the name.
      - Names that end with the $ are hidden shares.
      - See Configuration Maximums for name length limits.

   b. **Description** (optional): Enter a description for the share or export.

   c. **Share path** (optional): You can create standard nested shares by specifying the path. Nested shares inherit some properties from the parent directory. See Nested Shares and Exports on page 105 for details.

   d. **Max Size** (optional): Enter the maximum size in GiB, see Configuration Maximums for size limit details.

      Leaving the field blank means there is no upper limit to the size of the share. If you want to set an upper size limit, enter a value. Setting a value changes the capacity in the client view.

   e. **Primary Protocol Access**: Choose **SMB (Ideal for Windows Clients)** or **NFS** as the primary protocol.

   f. **Enable multi-protocol access**: Check the box to enable the multi-protocol feature.

   g. Click the **Next** button.

General Settings tab

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 480

3. Do the following in the indicated fields:

   a. Check the **Use "Distributed" share type instead of "Standard"** to create a distributed export:

      Note: Exports on single-FSVM deployments are standard by default.

      - A *distributed export*, also known as a sharded export or home share, load balances user data across multiple FSVMs.
      - A*standard export*, also known as a general-purpose share or export, for any other purposes.

   b. **Enable Self Service Restore**: Self-service restore lets you restore files from previous snapshots, see Self-Service Restore on page 176.

   c. **Enable Compression:** Check this box to save space and reduce data on the share through inline compression of written data, see File System Compression on page 156.

      Note: Enabling compression at the container level makes the **Enable File System Compression** option unavailable. The option does not appear on clusters upgraded from earlier versions without file system compression support.

   d. **Blocked File Types:** Check this box to specify blocked file types, see File Blocking on page 141.

   e. Click **Next**.

Protocol Settings and Permissions tab

Note: The primary protocol determines which protocol settings appear first.

4. Do the following for the indicated field in the **SMB Protocol Access** section.

   a. **Enable Access Based Enumeration (ABE)**: Check this box to restrict user access when browsing the contents of top-level directories to only those files and folders that they have access permissions for, see Access-Based Enumeration (SMB only) on page 139.

   b. **Allow Long Names for Files and Folders:** Check this box to allow the creation of file names up-to 1023 bytes (255 characters) long.

   c. **Encrypt SMB3 Messages:** Check this box to enable message encryption between the file server and client. See Encryption on page 139.

   d. **SMB Continuous Availability (CA):** Check this box to enable CA on the share, see Continuously Available Shares (SMB Only) on page 100.

   e. **Share Permissions (SMB):** This section displays the default permissions for all users and groups on the share.

      (Optional) To customize the permissions, click **Add User or Group**.

      - In the **User or Group** column, specify whom to apply the target permissions to. Specify a user or a group in the sAMAccountName or NETBIOS\sAMAccountName format.
      - In the **Type** column, specify to **block** or **allow** the target user or group.
      - Specify the blocked or allowed actions for the target user or group in the **Read**, **Change**, and **Full Control** columns.
      - Click the **check mark** icon to add the permissions, or click the **x** icon to remove the permissions.

      For more information about permission assignment, see Permissions on page 108.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 481

5. Do the following for the indicated field in the NFS section.

   a. **Authentication**: Select the authentication method from the pull-down list.

      The authentication options are **None**, **System**, **Kerberos 5**, **Kerberos 5i**, and **Kerberos 5p**.

      For LDAP or an unmanaged directory service, use none or system authentication – both are client-based but have different authorization rules. For AD, you can use none, system, or user-based authentication with Kerberos.

      See Directory Services and Authentication on page 109 for more information.

      Note: Files does not support Kerberos 5, Kerberos 5i, and Kerberos 5p with the NFSv3 protocol.

      Note: Changes to the authentication method can result in invalid mounts. Resolve the issue by remounting the authentication type as a value for parameter sec in the mount command on the client. Example: "-o sec=krb5" if you change the export authentication type to Kerberos 5.

   b. **Default Access (For all clients)**: Select the default access permissions from one of the following in the pull-down list:

      - **Read-Write**: Client can mount the export and write to it.
      - **Read-Only**: Client can mount the export and read data but not write to it.
      - **No Access**: Client cannot mount the NFS export nor read or write from it.

   c. **Squash**: Select the squash value from the pull-down list. The squash option controls the access privileges of root client users (users with UID 0). The **None** value gives root users super-user access privileges to the export, letting them create, edit, and delete files from any user. The **Root Squash** value disables super user access and maps all roots users to anonymous users. The **All Squash** value maps all users to anonymous ones.

   d. **Override anonymous IDs for squashing**: check this box to enter anonymous user identifier (UID) and group identifier (GID) value other than the default value. Both the anonymous UID and GID default have a default value of -2.

      - **Anonymous UID**: Enter the anonymous user identifier value for the export.
      - **Anonymous GID**: Enter the anonymous group identifier value for the export.

      You can map regular users to anonymous ones to restrict access to the NFS export. Setting the NFS authentication type to **None** maps all client users to anonymous ones.

   e. **Add Exceptions** (optional): If you want to refine the read, write, and no-access permissions to other than the the default, click the **Add Exceptions** link.

      The **Add Exceptions** dialogue box displays **Clients**, **Access**, and **Squash** fields. In the **Clients** fields, enter a comma separate list of clients for the target **Access** permission level. Exceptions

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 482

take precedence over the default, so any client listed in one of the exception fields gets that level of permission instead of the default permission.

For IPv4 clients, exceptions can be complete IP addresses, wildcards, or subnets. For IPv6 clients, Files only accepts complete IP addresses as exceptions. Use one of the following formats:

- Absolute IPs (for example 129.144.0.0)
- Hostname of client (for example client.domain.com)
- CIDR format for specifying subnets (for example 129.144.0.0/24)
- Netgroups (for example @it_admin)

  Note: Netgroups can limit access to hosts, but Files does not support Netgroups that limit access to users. If you add or remove a client from a Netgroup, it reflects on the client after 30 minutes.

- Wildcards (for example clients*.domain.com).

  Note: To use wildcards, configure reverse domain name system (DNS) records for the clients.

Caution: If a client IP address matches more than one exception rule, the client may experience access issues.

Once you add an exception, it appears on the **Protocol Settings and Permissions** tab under **Exceptions for Client Access**.

6. Do the following in the **Multi Protocol Access** section.
   - **Allow simultaneous read access to same files**: check to enable.
   - **Symlink creation from non-native NFS**: check to enable.
7. Click **Next**.

The **Summary** tab

8. Review the share or export configuration in the **Basics**, **Protocol Access**, **Sharing Permissions (SMB)**, and **Multi Protocol Access** tables.

Table 24: Basics

Property	Configuration
Share name	The name of the new export or share
Share path	The file path to the new export or share
Primary protocol	NFS or SMB
Multi-protocol access	Enabled
Share or export type	Distributed or standard
Self service restore	Enabled or disabled
Blocked file types	Enabled or disabled
Share compression	Enabled or disabled
NFS version	NFSv3 or NFSv4

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 483

Property	Configuration
Continuous availability	Enabled or disabled

Table 25: Protocol Access

Property	SMB Clients	NFS Clients
Authentication	Authentication type (Kerberos, AD, etc)	System or none
Client Access	Read-write **Note:** For SMB shares, SMB client access is always read-write.	Read-write or read-only
ABE	Disabled or enabled	N/A
Squash	n/A	All squash, root squash, or none
Message Encryption	Disabled or enabled	N/A

Table 26: Sharing Permissions (SMB)

User or Group	Type	Permissions
Everyone, [user name], or [group name]	Allow or deny	Read, change, or full control

Table 27: Multi Protocol Access

Property	Status
Allow simultaneous read access to same files	Enabled or disabled
Symlink creation from non-native NFS	Enabled or disabled

9. When all of the information is correct, click **Create**.

What to do next

To configure user mapping between NFS and SMB users, see User Mapping on page 118.

Multi-Protocol Support for Files

Multi-protocol support for Files provides SMB and NFS clients read-and-write access to the same share or export.

When you choose a native protocol, it determines access-control options for that share or export. You can then manage all access-control options using the native protocol. Once you create a share or export, you cannot change the native protocol.

Note: For non-native NFS access, group membership for trusted domain users cannot contain all groups when the groups are local groups from remote trusted domains.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 484

Consider the following protocol-specific options and caveats before deciding on a primary protocol.

Authentication

SMB clients have only one authentication type, Active Directory (AD), that they can use to access exports. NFS clients can access SMB shares using AD, LDAP, system, or unmanaged protocols. Files uses the native protocol to authenticate all non-native shares.

Authorization

Files uses user mapping to map IDs and user or group names, which authorizes access to shares and exports from native and non-native protocols. Configure user mapping when the NFS authentication of a multi-protocol share is not Kerberos (when NFS uses Kerberos, the users and groups for NFS and SMB are the same).

An IT administrator must configure user mapping, see User Mapping on page 118.

Access-Based Enumeration

Files supports access based enumeration (ABE) for native and non-native SMB shares.

Access Control Lists (ACLs)

ACLs are stored in the format of the native protocol. Modify ACLs using the native protocol. NFS clients do not honor share-level ACLs. When you create an object using a non-native protocol client, the object inherits access control details from the parent folder.

Alternative Data Stream (ADS)

Files supports alternative data streams (ADS) for native and non-native SMB shares.

Antivirus

Files supports antivirus protection on native and non-native SMB shares.

If you access a file that has a virus through an NFS client-created symlink or hard-link, only the path of the first access appears in the quarantine table.

Audit

Files supports audits for native and non-native shares.

Backup and Restore

Files supports back-up and restore only using the native protocol.

> **Caution:** Backup using a non-native client can result in metadata and ADS loss.

Change Notifications

There is no directory change notification support across protocols. Namespace changes made to a share from one protocol take up to a minute to reflect for a client of the second protocol.

Concurrent Access

Files supports concurrent read-access but not concurrent write-access for multi-protocol shares.

High-Availability

Files equips multi-protocol enabled shares and exports with high-availability. Files does not honor the NFS grace period on SMB clients.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 485

Namespace Compatibility

Since all SMB lookups are case insensitive, and all NFS lookups are case-sensitive, SMB clients can encounter multiple objects with the same name string but different cases.

NFS clients can create multiple files on SMB shares that use the same name-string but different cases. This leads to issues for Windows clients that find files with the same name but in different cases. Files maps NFS objects with illegal or special characters in the namespace to a new SMB name.

Quota

Files supports quota for multi-protocol shares, see Quotas on page 130.

Stats

Files combines stats for native and non-native shares.

Symlinks

NFS clients can create symlinks on native and non-native NFS shares and follow them using a native or non-native protocol.

Limitations

- Files silently ignores permission change requests for non-native protocol clients.
- NFS file or directory names that include trailing spaces are treated as illegal characters on SMB namespaces.
- Native SMB shares cannot enable the NFS squash option.
- NFS users might not see ownership details on native SMB shares. For NFS users, default owner and group on native SMB shares appears as `root/root`. However, SMB users see the default owner and group as `BUILTIN administrators`.
- Template mapping ignores the domain of users and groups.
- Files does not support multi-protocol compatibility for legacy NFS exports.
- When SMB clients create share objects on non-native shares, the objects derive the mode information from their parent share.
- If SMB is the primary protocol, you can only apply a quota to SMB users.
- Files and folders with illegal characters display on the client, but you cannot open or browse them.

Modifying a Share or Export

Modify or delete a share or an export.

About this task

You can update or delete a share from the **Shares** tab in the Files Console. Note the following limitations for modifying a share or export:

- Clusters created using earlier versions of Files might not support some new features.
- When renaming a share or export, access to the old name remains if you maintain the existing connection. Close and reopen the browser or CLI to no longer see the old name.

> **Note:** See Explicit Paths for Shares and Exports for a list of modifiable features on shares and exports with explicit paths.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 486

Procedure

- In the Files Console, select the target entry in the share table of the **Shares** tab.
- In the row for the selected entry, click **three dots menu** following.
  - » Click **Delete**, to delete the share (you do not need to proceed to the next steps).
  - » Click **Update** to modify the settings of the share or export. Proceed to the next steps for directions.
  - » Click **Add Quota Policy** to add a user or group quota to the share, see Quotas on page 130.
- To update the share, follow the steps as indicated.
  a. In the **Basics** or **Settings** tab, update one or more values accordingly.

  > **Note:** When renaming a share or export, access to the old name remains as long as the existing connection is maintained. Close and reopen the browser or CLI to no longer see the old name.

  See the Creating an SMB Share on page 77, Creating an NFS Export on page 83, or Creating a Multi-Protocol Share or Export on page 90 for details about each field.

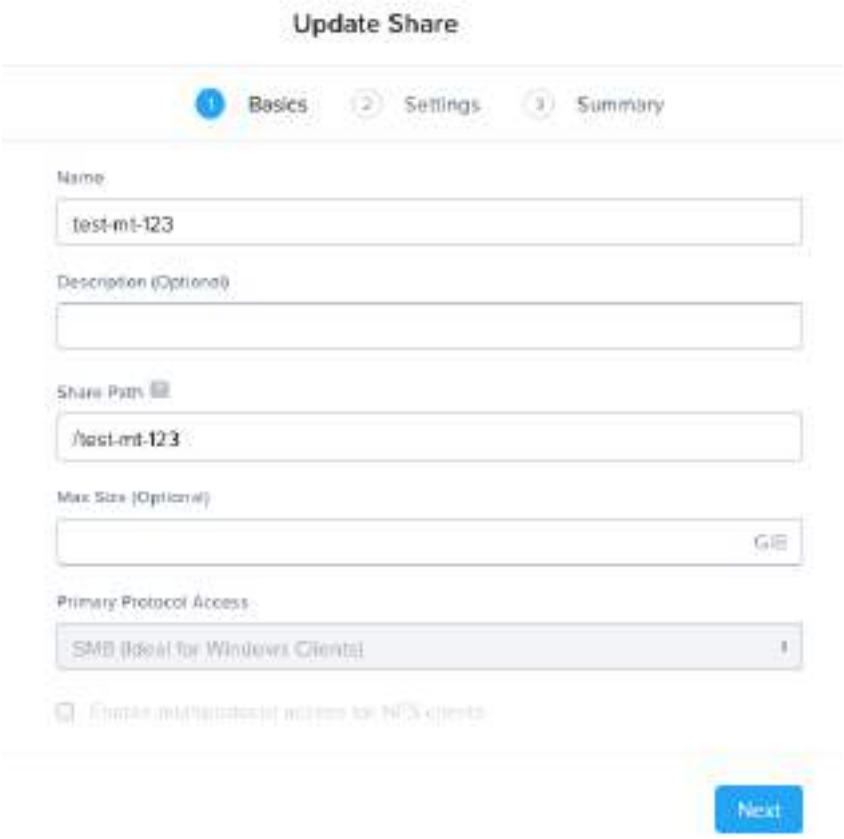


Figure 42: Update Share Window

  b. When all the values are correct, click **Update** (**Summary** tab).

Deleting a Share or Export

Delete a share or an export through the Files Console.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 487

About this task

> **Warning:** Deleting a share or export is permanent, and the deleted share or export cannot be recovered.

To delete a share or export, do the following:

Procedure

1. Remove the share or export contents and disconnect all clients. (All directories and files within the share/export should be deleted.)
2. In the Files Console, select the target entry in the share table of the **Share** tab.
3. In the row for the selected entry, click **three dots menu** > **Delete**.

> **Caution:** When deleting a share or export with an explicit path, the data and storage is not removed, see Nested Shares and Exports on page 105.

> **Note:** All shares and exports with explicit paths must be deleted before deleting the parent share.

Distributed Share Access

Access home directories without requiring the physical distributed share or export in the profile location.

Home directories are a type of distributed share. If the user profile exists in one of the distributed shares, access the distributed share directly using the universal naming convention (UNC) path.

If your username matches the directory name, you can reach it over the short UNC path: `\\Files_server\SamAccountName` (instead of `\\Files_server\home_share\SamAccountName`).

> **Note:** If your home directory exists in multiple distributed shares, Files matches to the first share created chronologically.

Distributed shares appear with other shares in Files when enumerating shares on the file server. Files enables distributed home share support by default. Learn more about distributed shares in the *Nutanix Files* Solutions Documentation.

Before modifying distributed share settings, confirm the following:

- Home directories are top-level directories in the distributed share.
- You have the required permissions. See the "Permissions" section in Share and Export Management on page 77.

Files supports using the following commands for FSVMs at the distributed share location

1. To enable or disable distributed home share support:

```
nutanix@fsvm$ afs smb.set_conf “enable user homes” yes|no section=global
```

2. To enable dollar user distributed share access.

```
nutanix@fsvm$ afs smb.set_conf “template user homeshare” “%U$” section=global
```

Accessing User Home Shares (Advanced)

Access home directories without the physical distributed share and the profile.

About this task

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 488

Before you begin

Ensure that you have met the requirements, see Distributed Share Access on page 99.

Procedure

To configure preferred home shares.

```
nutanix@fsvm$ afs smb.set_conf “preferred home shares” “home-share1, home-share2”
 section=global
```

Replace *home-share1* and *home-share2* with the names of the homes shares.

Continuously Available Shares (SMB Only)

Persistent file handles facilitate continuous availability (CA) for SMB shares.

During a disruption of service, SMB shares remain continuously available by using persistent file handles and high-availability. Persistent file handles reduce the period of data unavailability by automatically reconnecting users to the file service in use before the disruption.

Files stores open lock information on persistent volume groups, available on every FSVM in the cluster. During a fail-over, the fail-over FSVM can access the volume group. Persistent file handles let clients wait to reconnect without notifying you about the connection failure. As a result, disruptions are seamless to you and applications.

> **Note:** During a lock protection interval, Files does not prevent NFS clients from accessing the file. Files only prevents SMB clients from accessing files during the disconnected state.

> **Note:** The periodic handler cleans up stale locks for the disconnected persistent file handles every 24 hours.

Synchronous writes on CA shares may impact performance. Nutanix recommends continuous availability for shares with less metadata and more I/O intense workloads, such as VHD or VHDx based profile disks, where performance impact is minimal. As a result, CA is best suited for distributed shares.

Connected Shares

Connect standard or distributed shares in the namespace of another standard or distributed share.

Connecting shares creates a unique, continuous namespace. Use connected shares to distribute data across multiple FSVMs from a specified directory.

Distributed shares let you shard data only on the top-level directory (TLD) level. To shard data from a lower-level directory, connect shares by submounting a distributed share onto the path of another share or export. Files distributes that data from the mount point across multiple FSVMs. The distribution of data achieves load balancing.

The connected, continuous namespace lets you have different settings within the namespace, such as directory-level quotas. For more details on directory-level quotas, see Setting Directory-Level Quotas on page 106. Rather than connecting existing shares, you can also create a new share with an explicit path, see Nested Shares and Exports on page 105.

> **Note:** For multi-protocol enabled shares, a submount point can apply to multiple directories due to the case-sensitive NFS behavior and case-insensitive SMB behavior. As a result, Files uses all directories with the same name but different cases as submount points.

Connected Share Limitations

The following limitations apply to custom-level sharding:

- The submount path cannot point to the root of a parent share.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 489

- The submount path cannot contain snapshots.
- The submount path on a parent share must be empty before configuring submounts.
- Both parent and child shares must use the same type of NFS authentication.
- Nutanix does not allow nesting submounts. For example, if you have a child share child1 submounted on the submount path /parent/dir1/dir2/child1, you cannot submount child2 anywhere on the path.
- Nested shares and submounted child shares cannot have the same directory hierarchy.
- Stale locks for disconnected persistent file handles get cleaned up every 24 hours.

Connecting Shares

Shard a standard share or export.

About this task

Follow the steps as indicated.

Procedure

1. Sub-mount a distributed share onto a standard share to connect shares.

   ```
   nutanix@fsvm$ afs share.edit child-share-name submount_path=submount-path
   ```

   Replace `submount-path` with the file path to the mount point from the standard share. Replace `child-share-name` with the name of the child share.

2. List the connected shares.

   ```
   nutanix@fsvm$ afs share.list_all_submounted_shares parent_share_name=parent-share
   ```

   Replace `parent-share` with the parent share name.

Disconnecting Shares

Disconnect connected shares or exports.

About this task

To disconnect a child share from a parent share, update the mount point of the child share.

Procedure

1. Replace `child-share-name` with the name of the child share.

   ```
   nutanix@fsvm$ afs share.edit child-share-name submount_path=''
   ```

2. List all child shares connected to a parent share.

   ```
   nutanix@fsvm$ afs share.list_submounted_shares parent-share-name
   ```

   Note: Due to caching issues, child shares and exports can still appear as mounted.

What to do next

For NFS, remount the parent share on the client.

WORM Shares

Write-once, read-many (WORM) shares offer file retention to prevent inadvertent file deletion.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 490

WORM shares block file modification and deletion operations. As a result, only those applications that do not rely on file modification or deletion work on WORM shares.

> **Note:** WORM cannot be enabled on existing non-worm shares and exports. Also, you cannot apply worm on a newly (already) created share. You can only enable share-level retention (WORM) while creating a new share.

Share-level retention is also called *autocommit*. Configuring a cool-off interval for a share specifies the time for committing. When you do not change a file for the duration specified by the cool-off interval, the change time *ctime* remains unchanged. After the cool-off interval, the file transitions into the *locked* state and goes into retention, also called *commit*. The file remains in retention as specified by the `retention_time` parameter, or the default retention period specified for that share. After the retention time, the file transitions into the *expired* state where you can delete the file but not modify it.

You can edit the file during the cool-off interval. However, once the file is in the retention period, only privileged users can make edits to the file or delete it. If the retention period expires, Files does not support privileged delete operations.

WORM shares created with compliance mode block privileged users from deleting shares in the retention period. Compliance mode also includes the `legal_hold` variable, which, when toggled `on`, prevents the deletion of expired files. Once you create a WORM compliant share, you cannot disable WORM compliance mode.

The following applies to WORM enabled shares:

- If you set the DOS read-only bit, no one can delete the file. To perform the delete operations, you can turn the DOS read-only bit off.
- You cannot modify WORM cool-off interval and retention period parameters after share creation, but you can toggle the legal hold. You can modify share properties unrelated to WORM in the Files UI.
- To delete a file as a privileged user, use the following command:

```
nutanix@fsvm$ afs worm.priv_delete share_name path=file_path
```

To create and configure a WORM share, refer to Creating a WORM Share on page 103.

WORM Share Interoperability

This topic describes the interoperability of write-once, read-many (WORM) enabled shares with other features.

Consider the following interoperability, before using the WORM feature:

- You cannot enable tiering and WORM on the same share.
- Nested shares created within a WORM share have the same WORM configuration as the parent share.
- WORM shares do not retain their properties after SmartSync. You can configure the WORM policy on a remote site.
- Files supports Smart DR for WORM shares. After a Smart DR failover, the destination share has the same properties as the source share.
- Restoring a backed up WORM share converts it into regular share.
- A cloned WORM share has the same WORM configuration as the source.
- Files does not support retention for directories and symbolic links.
- Files share conversion retains the WORM properties.
- Nutanix does not recommend anti-virus (AV) scan on a WORM share or export.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 491

- Files does not support anti-virus policy configuration for WORM shares. Configured anti-virus policies skip WORM shares from scans.
- In the *locked* state, you cannot modify or delete alternate data streams (ADS), like regular files. The following applies In the *expired* state when the DOS read-only bit is off:
  - You can modify treams associated with the base file.
  - You cannot modify the base file and the associated attributes including modified time (mtime) and change time (ctime).

To create and configure a WORM share, see Creating a WORM Share on page 103.

Creating a WORM Share

You can create and configure a write-once, read-many (WORM) share using Files CLI commands on a File Server VM (FSVM).

About this task

You can do basic WORM share creation, deletion and querying of properties using the `afs` CLI commands.

> **Note:** You cannot enable WORM on existing non-WORM shares and exports.

Before you begin

Make sure you have read about WORM shares and their interoperability with other features. See WORM Shares on page 101and WORM Share Interoperability on page 102.

About this task

To create and configure a WORM share, do the following:

Procedure

1. Using SSH, log on to a Controller VM of the Nutanix cluster that deployed Files.
2. Start a file server.

   See Starting a Files Cluster on page 66.
3. Create a WORM share with default values.

   > **Note:** If no values are entered for the parameters, default values will be set.

   ```
   nutanix@fsvm$ afs share.add share_name worm_enabled=true
   ```
4. Create and configure a WORM share with non-default values.

   ```
   nutanix@fsvm$ afs share.add share_name worm_enabled=true worm_retention_period=time
    in seconds
   ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 492

```
worm_cooloff_interval=time in seconds worm_type=ShareLevel
```

(Optional) You can use one or more of the following parameters as needed while creating a share.

> **Note:** You cannot modify the cool-off interval or the retention period after creating the WORM share.

- worm_compliance=:Specify as true to block privileged users from deleting shares in the retention period (requires worm_enabled=true): Activates compliance mode. Compliance mode lets you set the legal_hold.
- legal_hold=: Prevents the deletion of expired files by all users.
- description=: Provide share description.
- hard_quota_size_gb=: Enter the hard quota size in GB.
- protocol=: Provide the value as NFS or SMB.
- share_type=: Provide the share type as general or distributed.
- size_gb=: Enter the size of the share in GB.
- timeout=: Enter the timeout in seconds.
- worm_cooloff_interval=: Specify the cool off interval for WORM in seconds. The default value for cooloff_interval is 600 seconds (10 minutes).
- worm_enabled= : Specify the value as true or false.
- worm_type= : Specify the type of WORM as ShareLevel.
- worm_retention_period= Specify the value of the retention period in seconds. The default value for retention period is 31449600 seconds (52 weeks).

5. (Optional) Check the attributes of the WORM share.

```
nutanix@fsvm$ afs worm.spec share_name=share_name
```

What to do next

To delete an expired WORM share, see Deleting a WORM Share on page 104.

Deleting a WORM Share

Admin can delete a write-once, read-many (WORM) share when desired using the AFS CLI or the Files Console.

About this task

> **Note:** The `share.delete` command can be used to delete non-WORM shares as well.

To delete a WORM share, do the following:

Procedure

1. Using SSH, log on to a Controller VM of the Nutanix cluster that deployed Files.
2. Start a file server.

   See Starting a Files Cluster on page 66.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 493

3. Delete a WORM share.

```
nutanix@fsvm$ afs share.delete share_name
```

For example,

```
nutanix@fsvm$ afs share.delete newshare
```

What to do next

For deleting shares from the Files Console, see Deleting a Share or Export on page 98.

Nested Shares and Exports

Use nested shares and exports to hide share paths or restrict access to parts of a tree.

Unless specified, Files creates shares and exports with an implicit path (the /share-name). To create a share or export with a different path, use the **Share Path** field to specify an explicit path for the share. Specifying an explicit path creates a nested share or export. The explicit path for the nested share must begin with the parent share or export (for example, to create an explicit path for share1 you can specify the explicit path / share1/dir1/dir2). Child shares and exports are nested under the parent shares.

To connect existing shares, see Connected Shares on page 100.

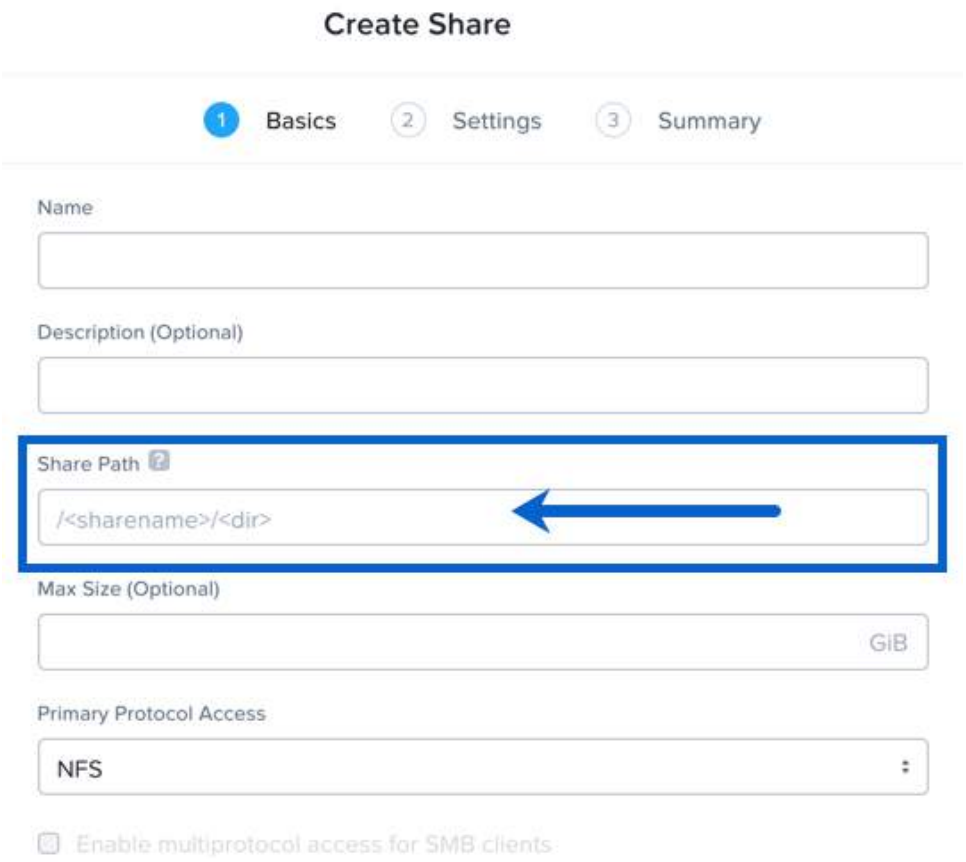


Figure 43: Shares and Exports with Explicit Paths

The following rules and limitations apply for creating, deleting, or modifying shares and exports with explicit paths:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 494

- New nested shares and exports cannot start with the name of another share or export created using an explicit path.
- Explicit paths must start with the forward-slash (/) character.
- When you create a share or export, an explicit path must contain a parent share or parent export name and the directory path (do not use the root directory).
- Files does not support changed file tracking (CFT) backup for nested shares and exports.
- When you enable or disable multi-protocol on a parent share, the action reflects for all nested shares or exports for that parent.
- Nested shares and exports inherit both the primary and secondary protocols, which you cannot modify at the nested-share level.
- The share path is case-sensitive for the NFS protocol.
- When you delete any of the directories in an explicit path, the path becomes inaccessible.
- Namespace changes under the root of the nested share do not appear immediately when accessed through the parent share path.

Consider the following recommendations:

- Delete all nested shares and exports before deleting the parent share.
- When a path becomes inaccessible after the deletion of a directory in an explicit path, you can recover the path by creating a directory with the same name.

Feature Modification

You can modify some of the properties of nested shares. Most of the time you cannot modify inherited properties. Refer to the following table for modification options.

Table 28: Nested Share Modification Options

Feature	Default State	Modification
SMB access based enumeration (ABE)	Disabled	Enabled
NFS advanced settings	Enabled	Enabled
Add quota policy	Disabled	Disabled
AV settings	Inherited from parent	Disabled

Setting Directory-Level Quotas

Set a directory-level quota by connecting shares.

About this task

Files supports size limits for shares and exports. Set a directory quota by sub-mounting a share or export onto the path of a standard share.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 495

Procedure

1. Create a share or export and specify the max size, see Creating an SMB Share on page 77.
   Alternatively, you can apply a share size limit to an existing share or export, see Modifying a Share or Export on page 97.
2. Connect the share or export to a directory of a standard share or export, see Connecting Shares on page 101.
   Files applies the quota (max size) for the connected share or export to the directory.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 496

DIRECTORY SERVICE AND DOMAIN MANAGEMENT

Administration of directory services and file server domains.

The domain and directory service configuration is an essential step of file server management. Join a domain and update domain name system (DNS) entries during or after file server creation. The this chapter describes domain and directory service management options and operations.

The directory services configuration specifies the primary and, if applicable, secondary protocol of a file server. If you intend to create multi-protocol shares and exports on file servers with secondary protocols, configure user mapping, see User Mapping on page 118 and Multi-Protocol Support for Files on page 95.

Permissions

The authorization setup on native shares and exports determines user and group access permissions to share data.

You can only make access permissions changes using the native protocol.

Native SMB Shares

You can set share permissions when creating or updating a primary SMB share in Files. See Creating an SMB Share on page 77.

You can add New Technology File System (NTFS) permissions for any valid user or group to the share root or to the sub-folders and files inside the share. Access to share objects is based on share permissions and NTFS permissions on the object. SMB share permissions, SMB share ACLs, and NTFS permissions on SMB shares only apply to SMB clients.

To access multi-protocol enabled shares using a non-native protocol, configure user mapping, see User Mapping on page 118.

You can also use the Windows native Microsoft Management Console (MMC) shared folders plug-in to manage share ACLs on SMB shares. Use the MMC Snap-In for Nutanix Files to manage NTFS permissions for distributed native SMB shares. On multi-protocol enabled shares, Files performs permission checks based on the native ACLs.

Default permissions for SMB shares are as follows:

- **Distributed shares:**
  - Domain administrator: Full access
  - Domain user: Read only
  - Creator owner: Full access (inherited only)
- **Standard shares:**
  - Domain administrator: Full access
  - Domain user: Full access
  - Creator owner: Full access (inherited only)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 497

Native NFS Exports

Unix mode bits, set from NFS clients, enforce permissions on NFS exports. By default, the NFS export root directory sets sticky bits, which are permission bits that allow only object owners and root users to remove objects. As an object owner, you can change the permissions on the files and directories that you own. By default, super users can only change export permissions after disabling root squashing.

Files does not support NFS ACLs.

Default permissions for NFS exports are as follows:

- **Distributed and standard exports:**
  - The initial permissions set on a NFS export (distributed and standard) is not configurable from Prism Element and defaults to mode 1777.
  - The choice of mode 1777 allows normal (non-root) users to create files and directories in any share (once a share has been created through Prism). The user owns the files and directories. In addition, the sticky bit (setting 1 in the 1777) ensures that only the owner (and root) can delete the created files.

    You can change the permissions from any client that has root privilege, but this requires disabling root squashing for the client.

Directory Services and Authentication

This topic provides an overview of directory services and authentication options for Files.

Depending on the primary and secondary protocols configured for your file server, directory service and authentication options vary. Configure directory services at the file-server level in the **Directory Services** tab during or after file server creation. Configure share-level authentication during share or export creation in the **Settings** tab.

File servers using the SMB protocol use Active Directory (AD) as the directory service. File servers using the NFS protocol can use Lightweight Directory Access Protocol (LDAP), AD, or unmanaged directory services. For NFS and multi-protocol shares, configure authentication during share creation in the **Settings** tab. For SMB shares, authentication is preconfigured once you set up the AD service for the file server.

The following describes each directory service and available authentication methods.

Active Directory

Files supports AD with NFS and SMB. To set up AD, specify the AD realm name, username, and password. If you have multiple domain controllers, you can configure a preferred domain controller (PDC). If you do not configure a PDC, Files uses any available domain controller.

Using the RFC 2307 standard is an optional setting in AD.

AD with SMB uses Kerberos and Windows NT LAN Manager (NTLM) authentication. SMB shares also support local user access.

For AD with NFS, you can use none, system, or user-based authentication with Kerberos. Each Kerberos type has varying levels of encryption, with Kerberos 5 being the lowest and Kerberos 5p the highest. The none authentication option does not have any security between users: each user can read and write to all other user's files. With the system authentication method, each user has a user ID that restricts other users from accessing their files.

LDAP

Files supports LDAP with NFS only. When you configure LDAP as the directory service, Files uses Netgroups to control client access. The Files LDAP setup is based on the RFC 2307 standard.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 498

To configure LDAP, assign an LDAP server and a base distinguished name (DN). The base DN specifies where the search for users begins. The file server binds to the LDAP server. For added security, set up a bind DN for the LDAP server. Without the bind DN, Files binds to the LDAP server as anonymous.

Unmanaged

Files supports the unmanaged directory service with NFS only. The unmanaged option lets you have none or system authentication, both of which rely on client-based rather than user-based authentication. To set up client-based authentication, specify default client access and exceptions during export creation.

Updating Directory Services

Update the authentication and user management configuration of a file server.

About this task

To update the directory services configuration, do the following:

Procedure

1. In the Files Console (see Files Console on page 21), go to **Configuration** > **Authentication**.
2. In the **Directory Services** window, select the protocols you want to use and complete the fields for the selected protocols.

   You can select SMB, NFS, or both. Each protocol contains more fields to complete. See the **Directory Services** tab step in Creating a File Server on page 37 for detailed instructions.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 499

3. When all the fields are correct, click the **Update** button.

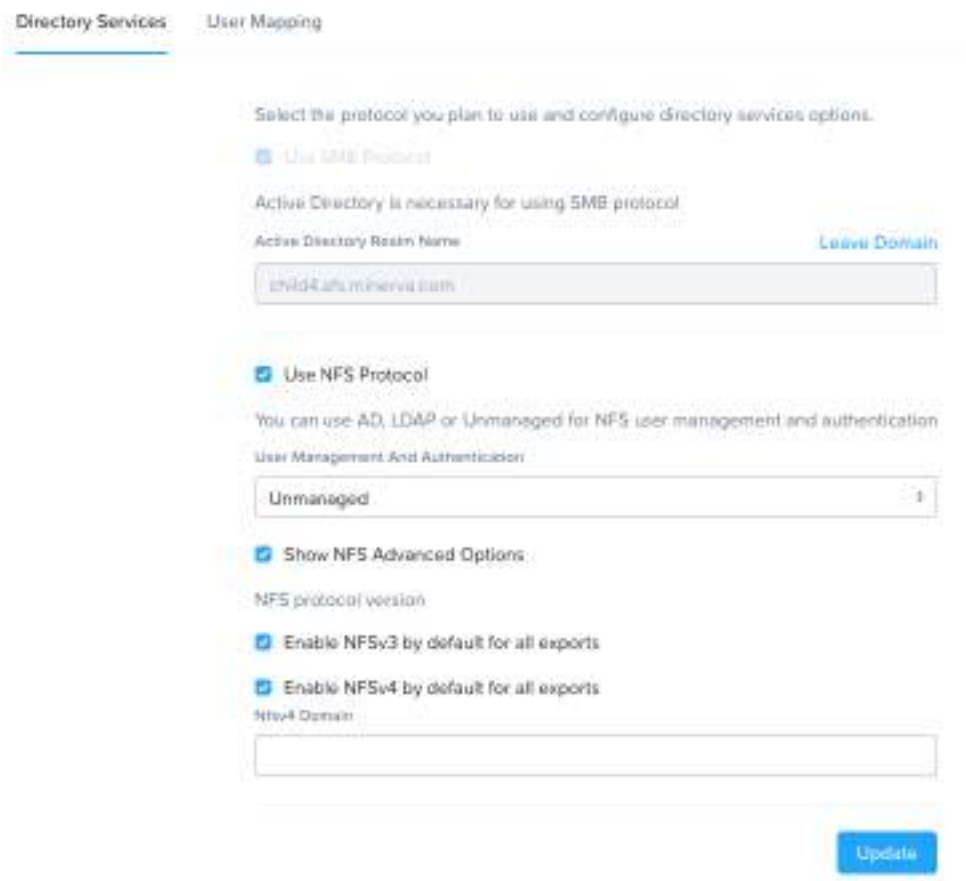


Figure 44: Directory Services Window

Setting AD Machine Account Password Expiry

Set an expiry period for the Active Directory (AD) machine account password.

About this task

The Files AD machine account password expiry value is zero by default, so, by default, the password remains unchanged.

For security reasons, if you want to keep the password renewed, follow the steps as indicated to change the password expiry to 30 days.

> **Note:** Renewing the password frequently (more often than once per week) can cause service issues due to possible AD synchronization issues in a multi-DC environment.

Procedure

1. Get the AD machine account password.

```
nutanix@FSVM:~$ afs smb.get_conf "machine password timeout"
[global]
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 500

2. Update the password expiry period to 30 days.

```
nutanix@FSVM:~$ afs smb.set_conf "machine password timeout" 2592000 section=global
```

The `machine password timeout` value is in seconds.

Joining a Domain

Join a file server to a domain.

Before you begin

Sync the file server time and Network Time Protocol (NTP) time before joining to a domain.

About this task

Join a domain either during or after file server creation. To join a domain during file server creation, see Creating a File Server on page 37.

When joining to an Active Directory (AD) domain, Files adds the following entries to AD.

- Machine account with the Files cluster name
- SPN entries

If the AD computer objects exist from previous unresponsive join attempts, the join domain process is unresponsive. Before attempting to join to the domain, remove the previous Files computer objects from AD. Otherwise, do not remove the file server computer object in AD, as that can cause disruptions to file server services.

To join to a domain after file server creation, follow the steps as indicated:

Procedure

1. In the Files Console, go to **Configuration** > **Authentication**.
2. In the **Directory Services** tab, select one or more protocols you want to use and complete the fields for the selected protocols. You can select SMB, NFS, or both. Each protocol contains more fields to complete, including fields about AD. See the **Directory Services** tab step in Creating a File Server on page 37 for detailed instructions.

   Enter an AD username in the *`domain|username`* format or in the UPN format *`username@ADrealm`*. You must have an administrator account or the following required permissions for the relevant AD organizational unit (OU) realm:

   - **Create computer objects**: Allows the delegated admin to create a machine account in the specified OU path, which is a requirement for Files to join the domain.
   - **Read service principal names**: Helps set the service principal names (SPNs) for the machine account. Kerberos access to Files requires SPNs.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 501

3. When all the fields are correct, click **Update**.

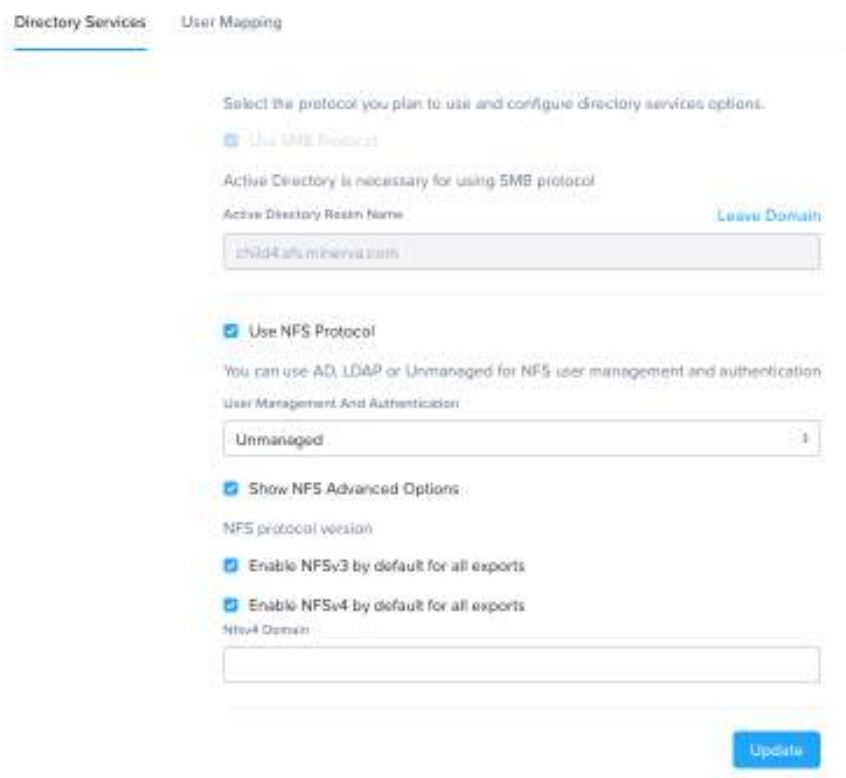


Figure 45: Directory Services Window

Leaving a Domain

Disconnect your file server from a domain.

About this task

The following tasks require that you first remove (leave) the connection between the file server and its current domain:

- Changing the file server name
- Joining the file server to a different domain
- Deleting the file server
- Changing the primary file server

Leaving a domain deletes the service principal name (SPN) entries and the Files computer accounts created on AD. To leave a domain, do the following:

> **Caution:** Leaving a domain causes Files to stop services until you join the file server to a domain. During this time, existing and future clients cannot use shares, exports, or permissions.

Procedure

1. In the Files Console, go to **Configuration** > **Authentication**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 502

2. In the **Directory Services** tab, click **Leave Domain**.

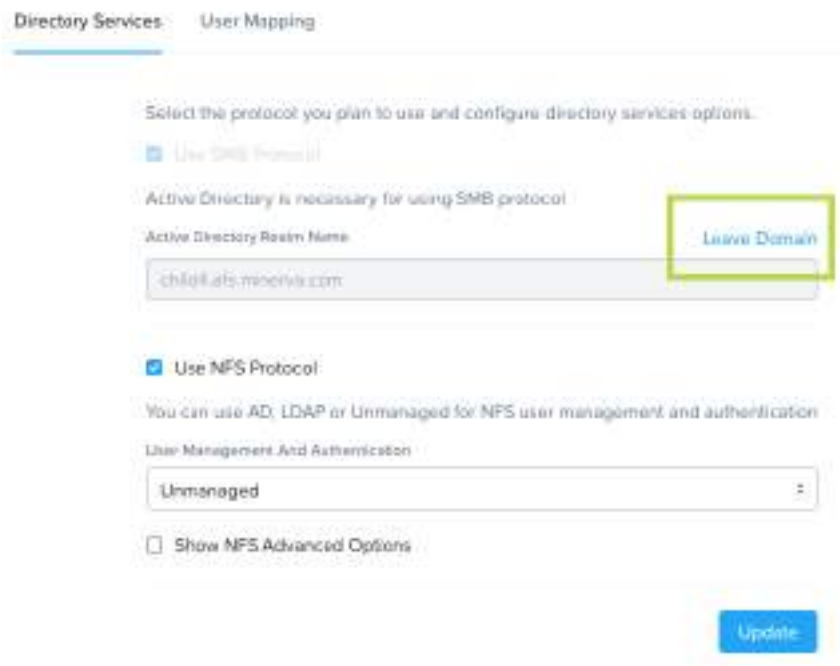


Figure 46: File Server Basics Window

What to do next

After changing the file server name or domain, do the following to re-establish the file server connection to a new domain:

- Remove any old DNS entries from one or more DNS servers.
- Add the new DNS entries, see Updating Domain Name System (DNS) Entries on page 114.
- Update the directory services, see Updating Directory Services on page 110.

Updating Domain Name System (DNS) Entries

Modify or add to existing domain name system (DNS) entries.

About this task

Administrators can choose to update or add more DNS entries for the following scenarios:

- Creating a file server
- Changing the filer server name or target domain
- Removing a node
- Adding a node

Files adds entries to the DNS server to ensure the availability of file services to clients using a Files namespace. Files uses DNS entries to resolve DFS referrals.

The total number of DNS entries added to the specified DNS server is three times the number of nodes in the Files cluster. Use the following format for DNS entries:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 503

- **File server name for each FSVM IP address**: *file_server_name.domain_fqdn*
- **FSVM name for its IP address** : *fsvm_name.domain_fqdn*.
- **Reverse external FSVM IP address**: *fsvm_external_ip_reversed*-in-addr.arpa

To update the DNS configuration, do the following:

Procedure

1. In the Files Console (see Files Console on page 21), go to **Configuration** > **Update DNS Entries**.
2. To automatically configure DNS entries, select the **Automatic (MS-DNS only)** option and do the following in the indicated fields:

   Note:

   - The automatic option is available only when using Microsoft DNS. If you use a different DNS server or you see a message that Files did not find the entries on the DNS server, use the manual method.
   - Files can only add PTR entries for the /24 zone. Check the subnet of the external network to confirm the zone. Files does not add PTR records automatically for external networks that are part of a large DNS zone. For these networks, follow the manual process instead.

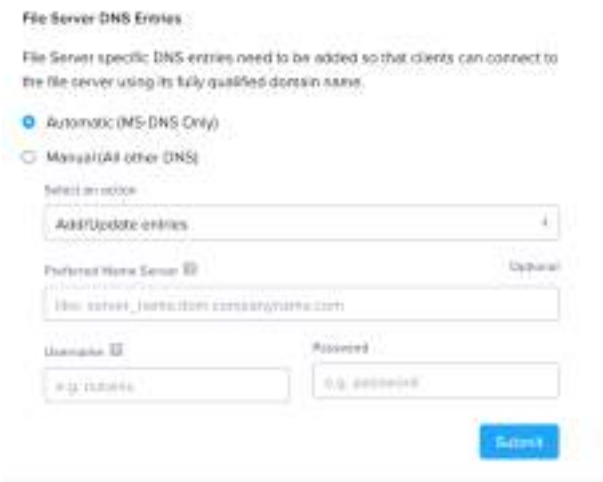


Figure 47: DNS Window (automatic view)

   a. **Select an action**: Select **Add/Update entries** or **Delete Entries** from the pull-down menu.

      Selecting **Add/Update entries** adds (or updates as needed) the required file server entries to the DNS server automatically. (You do not need to enter them yourself.) Selecting **Delete Entries** automatically deletes the current file server entries from the DNS server.

   b. **Preferred Name Server** (optional): Enter a preferred name server.

   c. **Username**: Enter the user name of the DNS server administrator.

   d. **Password**: Enter the administrator password.

   e. Click **Submit**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 504

3. To manually configure DNS entries, click the **Manual (All other DNS)** option and do the following:

   A table appears that lists entries consisting of a fully qualified host name and the corresponding IP address/PTR record.

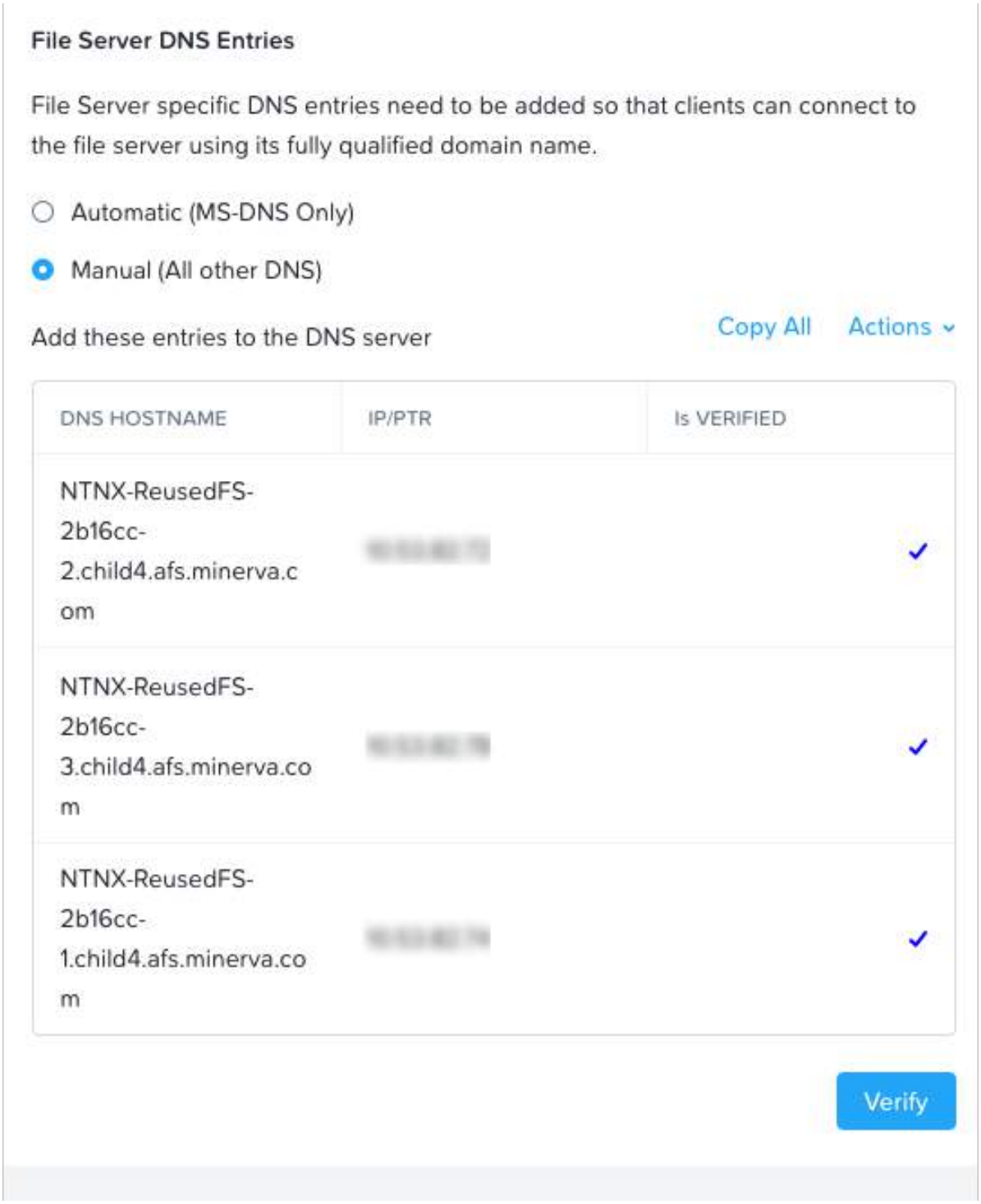


Figure 48: DNS Window (manual view)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 505

a. **Note:** For file server name, add A records only. For FSVM names, add both the A records and PTR records.

Copy the entries from the table and add them to the DNS server.

You can either copy the entries manually or click the **Copy All** link to copy the entire table. Click **Actions** to download that table in the CSV or JSON format. (To delete the current file servers entries on the DNS server, use this list to determine which entries to delete.)

b. Click the **Verify** button.

After copying the entries to the DNS server, verify that they are correct. Clicking the **Verify** button checks each entry in the table against the DNS server entries. A check mark in the **Is Verified** column indicates that entry is present on the DNS server. There should be a check mark for every entry.

c. Repeat step (a) for any entries that do not have a check mark in the **Is Verified** column.

The most likely reason (other than a network issue) for a missing check mark is a copy-and-paste error when transferring that entry to the DNS server. Check your work and repeat this process until Files verifies all entries.

Disjoint Domains

Configure different DNS domain and active directory (AD) realm values through the disjoint domains feature.

Your deployment must have the following requirements prior to configuring disjoint domains:

- A running AOS cluster
- A DNS domain name
- An AD realm name

Configuring Disjoint Domains

To have different DNS domain and AD realms, configure disjoint domains.

About this task

Follow the steps as indicated after creating a file server.

Procedure

1. After creating the file server configure the protocols and join the domain.

```
nutanix@fsvm$ afs fs.configure_name_services AD-realm-name username protocol
```

"SMB", "NFS", "NFS,SMB", "SMB,NFS" and "None" are valid arguments for `Protocol`.

(Optional) use one of following instead:

```
nutanix@fsvm$ afs fs.configure_name_services AD-realm-name username protocol
 organizational_unit=organizational unit
```

```
nutanix@fsvm$ afs fs.configure_name_services AD-realm-name username protocol
 overwrite=true/false
```

2. Configure the Microsoft DNS, see Updating Domain Name System Entries. If the DNS domain name and AD realm names are not the same, provide the full user principal name (UPN) of an administrator or user.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 506

USER MANAGEMENT

Configure user and group options.

This chapter describes options and steps for managing users and groups on the file server, including their roles, quotas, and mapping across protocols.

The directory services configuration specifies the primary and, if applicable, secondary protocol of a file server. If you intend to create multi-protocol shares and exports on file servers with secondary protocols, configure user mapping, see User Mapping on page 118 and Multi-Protocol Support for Files on page 95.

User Mapping

Configure user mapping on file servers that have multi-protocol shares or exports.

User mapping lets you access the same share or export using native and non-native protocols. You can retain your user-mapping configuration while configuring the directory services. User-mapping configurations are on a file-server level, which extend to all shares and exports on the file server.

When NFS is the primary protocol with unmanaged authentication, map the Active Directory (AD) username to the NFS client user ID, and map the AD primary group name to the NFS client group ID (GID).

The following restrictions apply to directory service use across protocols:

- NFS clients accessing SMB shares can use IDs from AD, LDAP, or client-generated unmanaged IDs .
- If the NFS security type is **not** Kerberos, configure user mapping for multi-protocol shares and exports
- LDAP usernames cannot be numeric.

> **Note:** Group identifiers (GID) and user identifiers (UID) can appear mismatched because of the access point. The first part of the UID/GID is a config-based range. The last part of the UID/GID is the relative ID (RID) of the user, which is based on the SID. Clients and file servers use different config ranges, so the first part of the GID/UID can appear mismatched.

Mapping Behavior

Files uses the following mapping behaviors:

- *UserGroup*: Default mapping for new shares and exports. Files maps a non-native user to a native user. Files ignores all groups of the non-native user and uses groups of the native user for authorization. Files does not use the groups of the non-native user in the access token.
- *MappedGroups*: Files maps the non-native user and the associated groups to a native user and the respective native groups. The native groups can also be groups of the native user. The access token has a set of user and group identities. Use MappedGroups for the following use cases:
  - Deny access to a specific group.
  - Give access to users based on groups in the ACLs of a file.
- *Legacy mapping*: Mapping for legacy multi-protocol shares and exports (shares and exports on file servers created with versions before Files 3.6.1). Legacy non-native SMB shares use the

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 507

MappedGroups mapping behavior, and legacy non-native NFS exports use the UserGroup mapping mechanism. You cannot modify the legacy-mapping behavior.

> **Note:** With legacy mapping, Files requires group mapping for the primary group of SMB users to access native NFS exports.

Mapping Configurations

User mapping includes the following mapping configurations:

- **Search**: Use the **Search** tab to search for mapping rules of a user or a group.
- **Rule-Based Mapping**: Use the **Rule-Based Mapping** tab to configure a mapping rule for AD and LDAP users. The following options apply:
  - SMB name matches NFS user name.
  - No template mapping.
- **Explicit Mapping**: Explicit mapping overrides rule-based mapping. The rule entered first takes precedence for users and groups that have multiple mappings configured. Explicit mapping consists of two mapping subcategories: a **one-to-one mapping** list and **wildcard based mapping**.

  You can use the one-to-one mapping list to manually enter or upload a csv file that maps users across protocols. Use wildcards for many-to-one mapping. Do not use wildcards on both ends of a user-mapping entry. You can also deny share and export access for a specific user or group.
- **Default Mapping**: Default mapping is the simplest mapping method to configure. You can map all non-native SMB users and groups to a specific native NFS user or group, and conversely. Default mapping also specifies how to handle users that have not had user mapping configured.

The **Summary** tab shows the configured mapping rules and the order in which the rules are prioritized. User-mapping rules take priority in the following order:

1. Deny access rules
2. One-to-one mapping
3. Wildcard mapping
4. Template mapping
5. Default mapping

Configuring User Mapping

Administer non-native user access for multi-protocol shares and exports.

About this task

For information on multi-protocol support, see Multi-Protocol Support for Files on page 95.

> **Note:** User mapping does not support the user name format (UPN).

Procedure

1. In the **Files Console**, go to **Configuration** > **Authentication** > **User Mapping**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 508

2. (optional) search for mapping rules for a specific user or group.
   a. Select from one of the following search options:
      » **SMB to NFS mapping**
      » **NFS to SMB mapping**
   b. From the dropdown, choose to search by **User** or **Group**.
   c. In the search bar, enter the search target.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 509

3. (optional) In the **Explicit Mapping** section, click **Configure** to set up explicit mapping rules.
   If you have already configured rules, click **Edit**.

   a. Configure explicit mapping by specifying one-to-one mapping, wildcard mapping, and deny access rules.

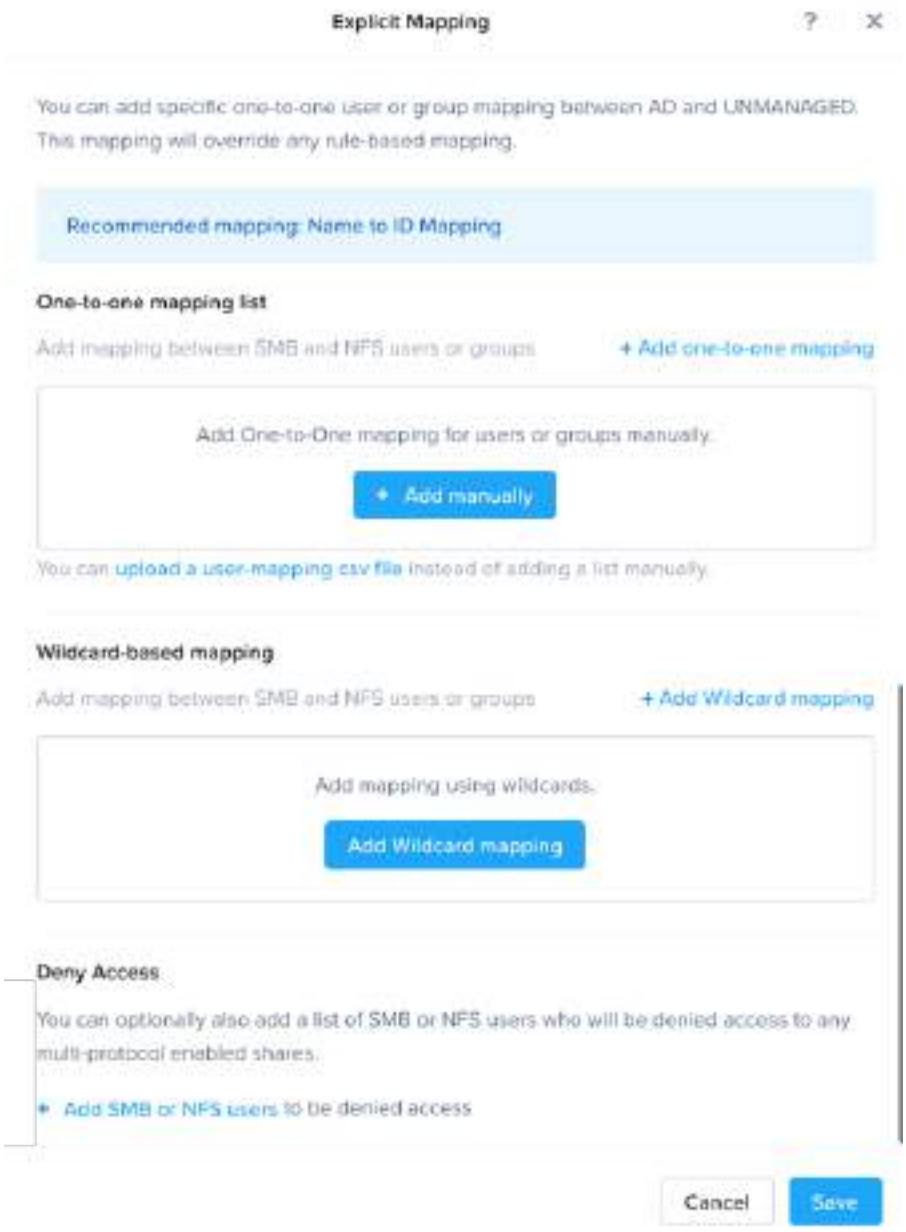


Figure 49: Explicit Mapping

   b. (optional) Configure one-to-one mapping to map single users or single groups by doing one of the following:

      - To map users or groups manually, click **Add one-to-one mapping**. Add the following information in the indicated fields:

        1. In the **SMB Name** field, enter the name of an SMB user or group.
        2. In the **NFS ID**, enter the name of an NFS user or group.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 510

3. In the **User/Group** field, indicate if the mapping is between users or groups.
4. To add the add one-to-one mapping rule, click the **check icon**.

- Click **upload a user-mapping csv file** to upload a file that specifies one-to-one mapping rules. Format the CSV file to consist of three columns with the indicated information, in the following order:

  - Name of an SMB user or group
  - Name of an NFS user or group
  - Indication of whether the mapping is for a user or group

Figure 50: One-to-One Mapping List

c. (optional) Add wildcard mapping to map multiple users or groups to one.

Note:

- Files does not support user mapping entries that have wildcards on both ends.
- Wildcards do not support the use of numeric NFS IDs.

- 1. Click **Add wildcard mapping**.
  2. In the **Priority** field, choose the priority for the rule. (The lower the number, the higher the piority).
  3. In the **SMB Name** field, enter the SMB user or group name.
  4. In the **NFS Name** field, enter the name of the NFS user or group.
  5. In the **User/Group**field, indicate if the mapping is between users or groups.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 511

6. To add the wildcard mapping rule, click the **check icon**.

Figure 51: Wildcard Mapping

d. (optional) Add a list of users or groups to be denied access.

- **1.** In the **Deny Access** section, click **+Add SMB or NFS users**.

  Note: Deny access rules take the highest priority.

  2. To deny access, add comma-separated users and groups in one or more of the following fields:

  - **SMB users to be denied access to NFS exports**
  - **SMB groups to be denied access to NFS exports**
  - **NFS users to be denied Access to SMB shares**
  - **NFS groups to be denied access to SMB shares**

Figure 52: Deny Access Rules

e. Click **Save**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 512

4. (optional) Configure rule-based mapping.

   a. To map SMB and NFS users and groups, choose one of the following default rules:

      » SMB name matches NFS name.

      » No template mapping.

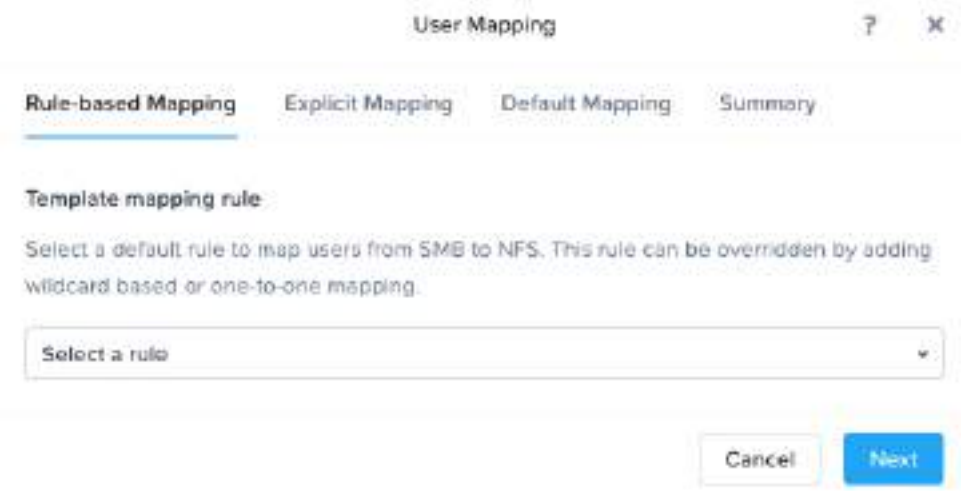


Figure 53: Rule-Based Mapping

   b. Click **Save**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 513

5. (optional) Set up default-mapping rules for Files to use when no applicable rule-based or explicit mapping rules exist for the user or group.

Figure 54: Default Mapping Rules

   a. Choose one of the following options from the **SMB Users With No NFS Mapping** dropdown:

      » Deny access to NFS export.

      » Map to specific Unix user and group.

   b. If you selected **Map to specific Unix user and group**, do the following (otherwise move on to the next step):

      - Enter a value in the **Unix UID** field.

        Note: If NFS has LDAP, use a user or group name. Otherwise, use a user or group ID.

      - Enter a value in the **Unix GID** field.

   c. In the **NFS Users With No SMB Mapping** field choose from one of the following options:

      » Deny access to SMB share.

      » Map to specific AD user and group.

   d. If you have selected **Map to specific AD user and group**, fill out the following fields (otherwise move on to the next step):

      - In the **SMB User** field, enter a default SMB user target for NFS users without mapping.
      - In the **SMB Group** field, enter a default SMB group target for NFS groups without mapping.

   e. Click **Save**.

6. (optional) To delete all mapping rules for all users and groups, click the **Purge All Mapping** button

   Caution: Clicking **Purge All Mapping** permanently removes all existing mapping rules.

Managing Roles

Manage roles by adding, removing, or modifying administrator privileges.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 514

About this task

You can create two types of Files administrators:

- *File server admin*: The file server admin can manage all file server operations, modify the access permissions for all users in all the shares/exports, and back up and restore data on the file server.
- *Backup admin*: The backup admin can back up and restore data on the file server (but does not have other administrative permissions).

> **Note:** Assign a backup service account (AD user or group) the backup admin role to prevent insufficient access issues.

To add or modify a Files administrator, do the following:

Procedure

Creating a New Role

1. In the Files Console (see Files Console on page 21), go to **Configuration** > **Manage Roles**.

   The **Manage roles** view displays.

Figure 55: Manage roles window

2. To add an administrator, click **+ New user** in the **Add Admins** section.
   A line for new credentials appears at the bottom of the list.
3. Do the following to configure a role for a user or group:
   a. In the **User** field, enter the Active Directory user or group name.

      Enter user or group names in the `samAcctName` or NETBIOS\`samAcctName` format. Replace `samAcctName` with the SAM-account-name.

   b. In the **Role** field, select **File Server Admin: Full access** or **Backup Admin: Backup access only** from the pull-down list.
   c. To add the user, click the **check mark** icon.
   d. To add more administrators, repeat these steps.

      The target users or groups must sign out for changes to take effect.

Modifying Roles

4. To modify an administrator, click the pencil icon in the **three dot menu** > **edit** for that user and update the name or role.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 515

5. To delete an administrator, click the **three dot menu** > **edit** for that user.

Managing REST API Roles

Manage REST API access for all users on a file server.

About this task

To add, modify, or remove REST API access, follow these steps.

Procedure

1. In the Files Console, go to **Configuration** > **Manage roles**.
2. To add a REST API user, click **+ New User** in the **REST API access users** section.
   A new line for the new user appears at the bottom of the list.

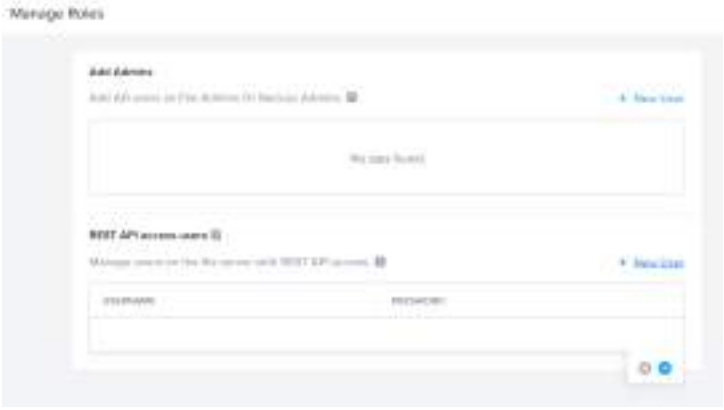


Figure 56: Manage roles window

3. To add a user, follow these steps:
   a. In the **Username** field, enter the username requiring REST API access.

      Note: You cannot add the "admin" username.

   b. In the **Password** field, type in a password for that user.
   c. In the same row, click the **check mark icon** to save the configuration.
   d. To add more users, repeat this step.
4. To modify a username or password, click **three dots menu** > **Edit** in the row for the target entry.
5. To delete a user, click **three dots menu** > **Delete** in the row for the target entry.

Authorizing a REST API User

To use the Files APIs, authorize a user in the REST API explorer.

About this task

Follow the steps as indicated from the Files Console.

Note: To create a REST API user, see Managing REST API Roles on page 127.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 516

Procedure

1. Go to **Admin** > **REST API explorer**.

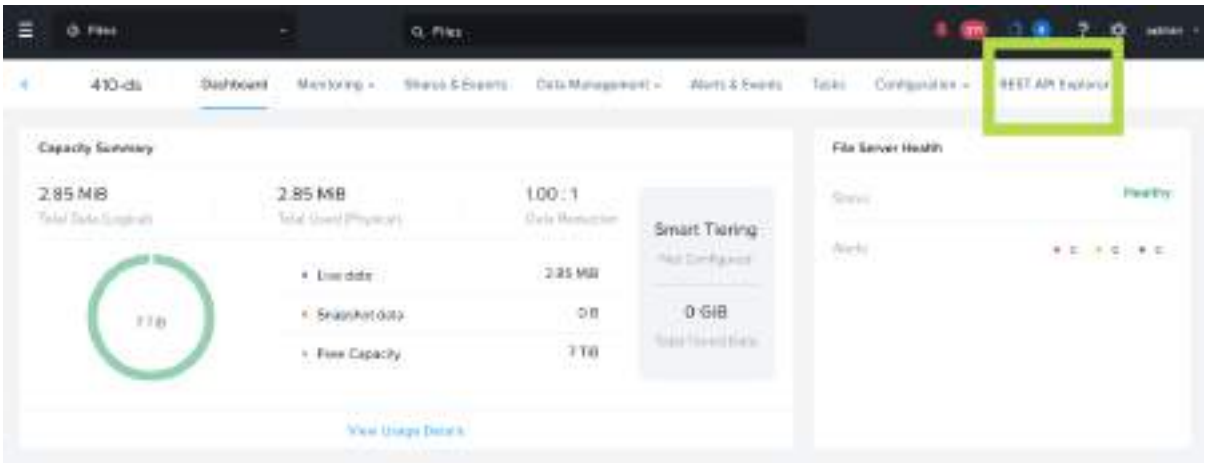


Figure 57: REST API explorer

2. Click **Authorize**.

Figure 58: REST API explorer

A dialog box for REST API user credentials appears.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 517

3. Enter the REST API user credentials in the **username** and **password** fields.

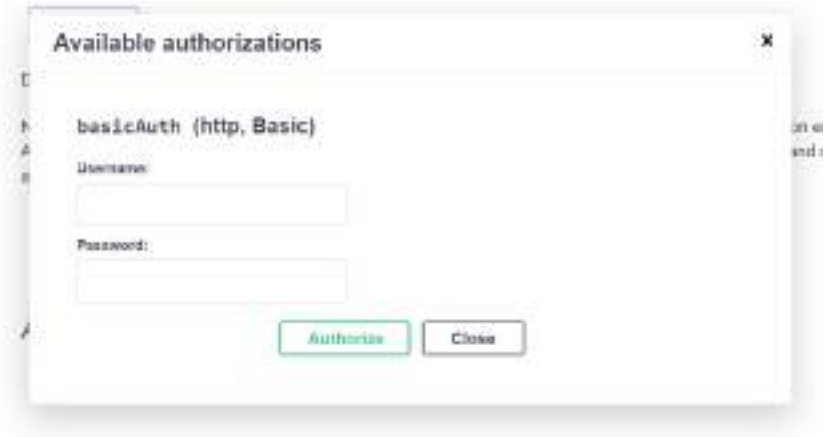


Figure 59: Authorize User Window

4. Click **Authorize**, and then click **Close**.

Managing Limited Local Users (SMB Only)

Manage limited local users and groups on your file server.

About this task

You can add limited local SMB users to a file server for SMB share access using the command line or using the Microsoft Management Console (MMC) Local Users and Groups snap-in.

If you add a limited local user using the MMC Local Users and Groups snap-in, MMC adds the user to the built-in Local Users group, user in this group inherit default permissions from the group. See Microsoft documentation for steps on adding local users using the MMC.

Manually add users to a group with specified permissions or browse and assign permissions using the MMC Local Users and Groups snap-in.

Limited local user management includes the following limitations:

- Files permits a maximum of 100 limited local users per file server.
- Limited local users cannot access non-native shares.
- Files does not support user-mapping for limited local users.
- Files does not support quota for limited local users.
- Files does not support renaming local users.
- Files does not support limited local users who are not joined to a domain or to standalone file servers. The file server must join an AD domain.

Use the commands as indicated to manage limited local users.

Procedure

- Add a limited local user.

```
nutanix@fsvm$ afs user.add limited-localuser-name
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 518

- Add a limited local user to a limited local group.

```
nutanix@fsvm$ sudo net sam addmem 'group-name' 'file-server-name\user-name'
```

> **Note:** You can add local users to local groups, which are in BUILTIN\Users and BUILTIN\Administrators.

- List limited local users.

```
nutanix@fsvm$ afs user.list
```

- Edit a limited local user.

```
nutanix@fsvm$ afs user.edit limited-localuser-name
```

- Delete a limited local user.

```
nutanix@fsvm$ afs user.delete limited-localuser-name
```

- Delete a limited local group.

```
nutanix@fsvm$ sudo net sam delmem 'group-name' 'file-server-name\user-name'
```

Quotas

This topic describes the Files quota types, notifications, and policies.

Set quotas to allot the storage space a user or group can use.

There are two quota levels:

- *User*: Sets a specific amount of storage for a single user. For example, if an administrator allots only 1 GB, then you cannot use more than 1 GB – the total storage capacity for you is limited to 1 GB.
- *Group*: Sets the amount of space for each user in that group. For example, a group with a policy of 10 GB and 10 users can potentially use 100 GB of data (10 x 10 = 100 GB) under that quota policy.

Alternatively, rather than configuring quotas for specifics users, groups, or directories, you can configure a maximum share size to restrict the amount of storage space used by a share. To limit the space in a directory, see Setting Directory-Level Quotas on page 106.

Notifications

You can configure email alert notifications that Files sends when user or group quotas are near the maximum threshold. Files can send the alerts to you and other recipients. Emails notifications alert the recipient when the quota is near maximum and when it is near full consumption. When the quota reaches 90 percent consumption, Files sends warning emails to the recipients. When the quota reaches 100 percent consumption, Files sends alert emails to the recipients. If the quota has a soft limit, you can continue to consume over 100 percent of the storage and Files will send an email notification to the recipients every 24 hours.

Policies

A quota policy specifies the consumption limit and enforcement type for all quota levels as configured by the administrator. Enforcement types determine if a user or group can continue to use the quota once they consume their share. See the enforcement types descriptions in the following table.

> **Caution:** Quota policy enforcement begins several minutes after policy creation. Therefore, if you reach the quota limit before the interval is complete, Files raises the alert but does not enforce the quota.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 519

Note: Beginning with AOS 5.15.1 and AOS 5.17.1 you can set decimal quota values, earlier AOS versions only permit integer quota values. During a disaster recovery (DR) event to a container with a version earlier than AOS 5.15.1 and AOS 5.17.1, Files rounds the decimal quota value down to an integer.

Quota Configurations	Description
User or Group	The designated name for a specific user or group.
Quota	The limit of quota space (in GB).
Enforcement Type	• **Hard Limit**: Prevents further writes once quota limit is reached. • **Soft Limit**: Does not prevent writes. Sends email notifications to email recipients. **Note:** You cannot set both a soft and hard limit for the same user or group.
Email Recipients	Enable the email recipients box and enter the email addresses for recipients Files should notify about hard and soft quota limits.

Applying Quota Policies

Files resolves quotas policies per the following:

- If you have defined a Files user-level quota, then recipients receive the quota from this user-level policy.
- If you have not defined a user level, but you have defined multiple group-level policies, then Files applies the policy with the most space.
- If you have not defined a user or group policy for any given user, Files chooses the quota default policy.
- For distributed shares and exports, each user has one home directory. Therefore, quota applies only to the first user directory at the root of a distributed share.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 520

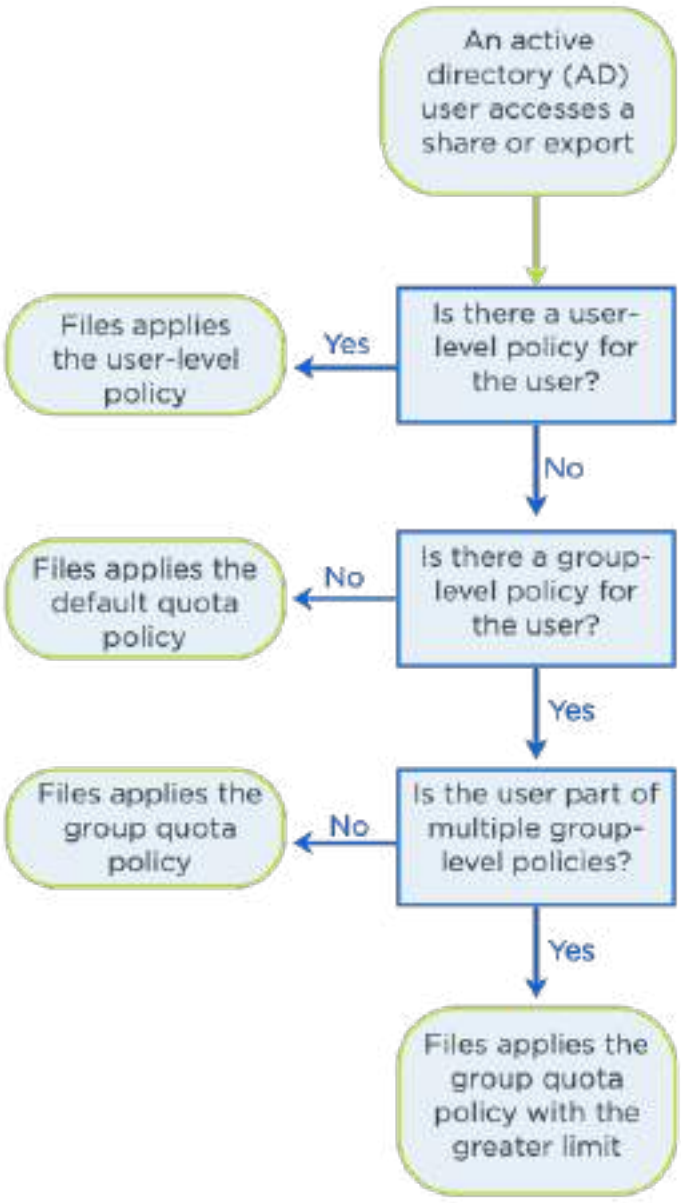


Figure 60: Quota Policy Hierarchy

> **Note:** If you add a new AD group and add a quota policy for that group, changes take 24 hours to reflect. For a faster update, contact Nutanix Support.

Multi-Protocol Limitations

The following limitations apply when you enable both SMB and NFS read-and-write access on a share or export.

- You can only apply a quota to users and groups of the primary protocol. For example, if SMB is the primary protocol, you can only apply a quota to SMB users.
- When you map multiple non-native users or groups to a single native user or group, Files only applies a quota to the first non-native user or group.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 521

- Quota applies to non-native users mapped to native users who belong to a group quota.

Managing Quotas

Add or edit user or group quotas in Files.

About this task

Files implements user and group quota types that balance storage per a user of a share or export. To configure the quota levels for user, group, or default levels, perform one of the following steps.

Procedure

Creating a new quota policy

1. In the Files Console (see Files Console on page 21), go to **Shares**.
2. Click the name of the target share.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 522

3. Click **Actions** > **Add Quota Policy**.

   a. Under **Add Users**, select to add the quota policy for a **Individual User** or **User Group**.

   b. In the **Username** field, enter the target user-name or group-name.

   c. In the **Quota Limit** field, enter the space for the quota limit (in GiB).

   d. Select the enforcement type.

      - **Hard limit**: Prevents further writes after reaching quota limit and puts the user or group into read-only mode.
      - **Soft limit**: Does not prevent writes. Sends email notifications to email recipients.

        Note: You cannot set both a soft and hard limit for the same user or group.

   e. Check the **Send email notification to the Files administrator** box to enable email notifications.

      - (optional) To customize the alert, click **Customize email template**.

        1. Under **Email Subject**, enter a subject for the alert emails.
        2. In the field under the email body, enter the custom message to appear following the quota alert details.
        3. Click **Save**.

        The **Add Quota Policy** window is displayed.

      - Add email recipients in the **Email Recipients** field.

   f. To add the quota policy, click **Update**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 523

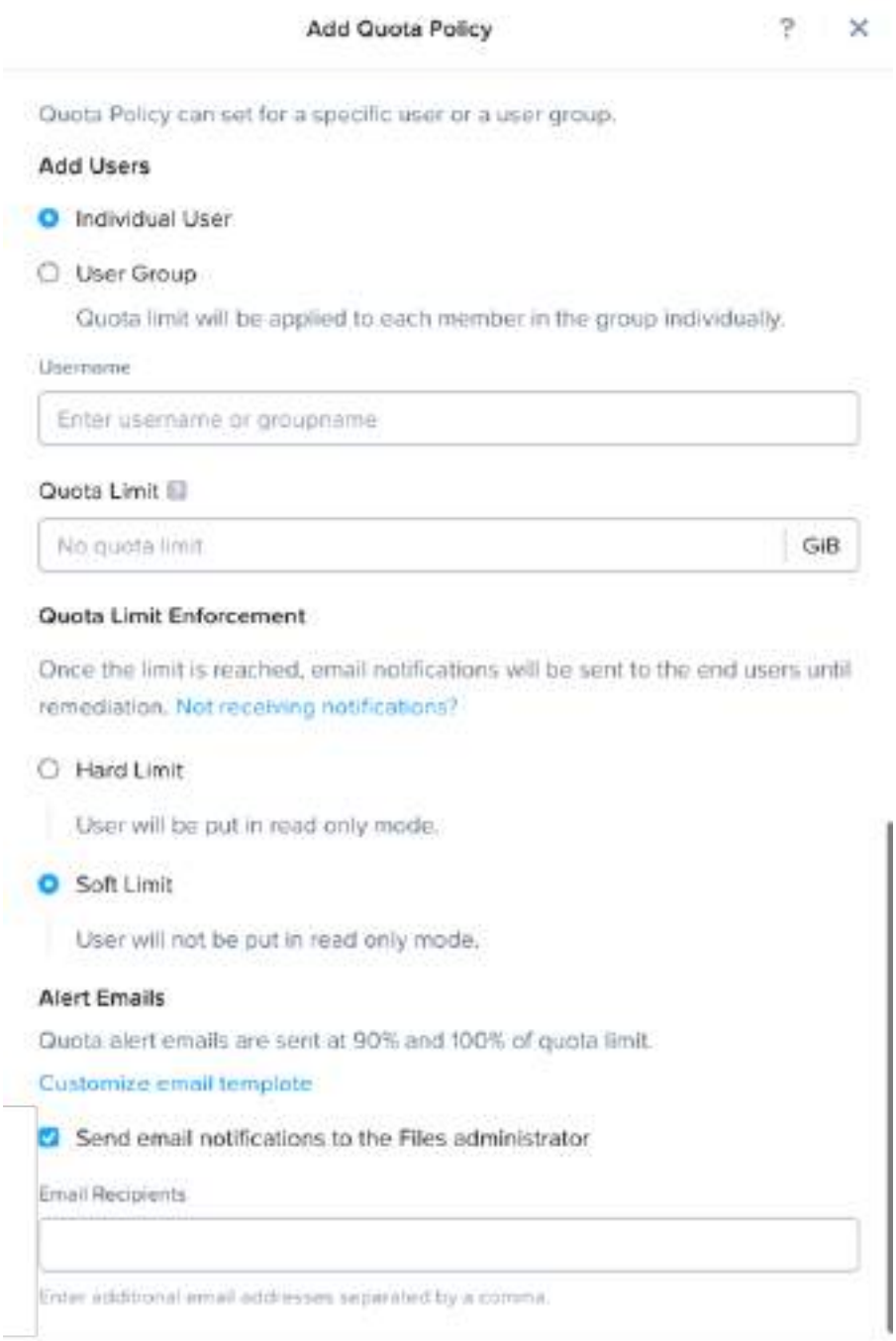


Figure 61: Add a Quota Policy

Editing a quota policy

4. Edit an existing quota policy.

   a. Click the share or export in the **Shares** tab.
   The **Quota Policies** tab displays all of the quota policies on the share.

   b. In the row for the target policy, click the **three dot menu** > **edit**.

Figure 62: Edit an Existing Quota

   The **Quotas** window displays.

   a. You can edit the existing policy by updating the amount of space (GiB), the enforcement type (hard or soft limit), and the email notifications and recipients. Click **Add**.

> **Note:** To remove a quota, change the share size to 0.

Remove a quota policy

5. In the row for the target policy, click the **three dot menu** > **delete**.

Role-Based Access Control (RBAC) for Files

You can configure RBAC with Files on Prism Central (PC) using the Files Manager. For more information on RBAC, see the following documentation:

- "Role-Based Access Control Workflows for Files" in the *Files Manager Guide*.
- "Controlling User Access (RBAC) " in the *Security Guide*.
- "Operations Entities" in the *Prism Central Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 525

FILES OPTIONS

Files provides a number of options to accommodate your file server implementation.

Cloning

Clone any file server protection domain snapshot at the local or remote site.

The file server clone is not protected by default. Be sure to enable the protection domain if you want the file server protected. Files cannot clone snapshots taken in earlier releases. Also, file server clones cannot be replicated or migrated to clusters that use earlier AOS and Files versions.

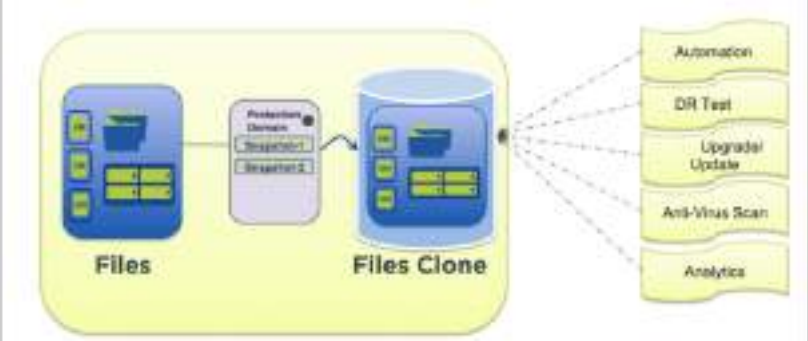


Figure 63: Cloning capability for Files

Cloning helps with the following without impacting the original Files cluster:

- Create backups at the primary and secondary sites
- Undertake DR test at secondary site
- Recover a file server from a specific point in time
- Spin-up a file server at the primary or remote site for testing or development purposes

Cloning a File Server

Follow this procedure to clone a file server from a specific snapshot.

About this task

The file-server clone is a thin copy that consumes minimal storage space. You cannot clone a file server to a storage container that is different from the original container.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 526

Procedure

1. In the **File Server** view in PE (see File Server View in Prism on page 19), select the target file server and then click the **Clone** button.

   The **Clone File Server** window displays.

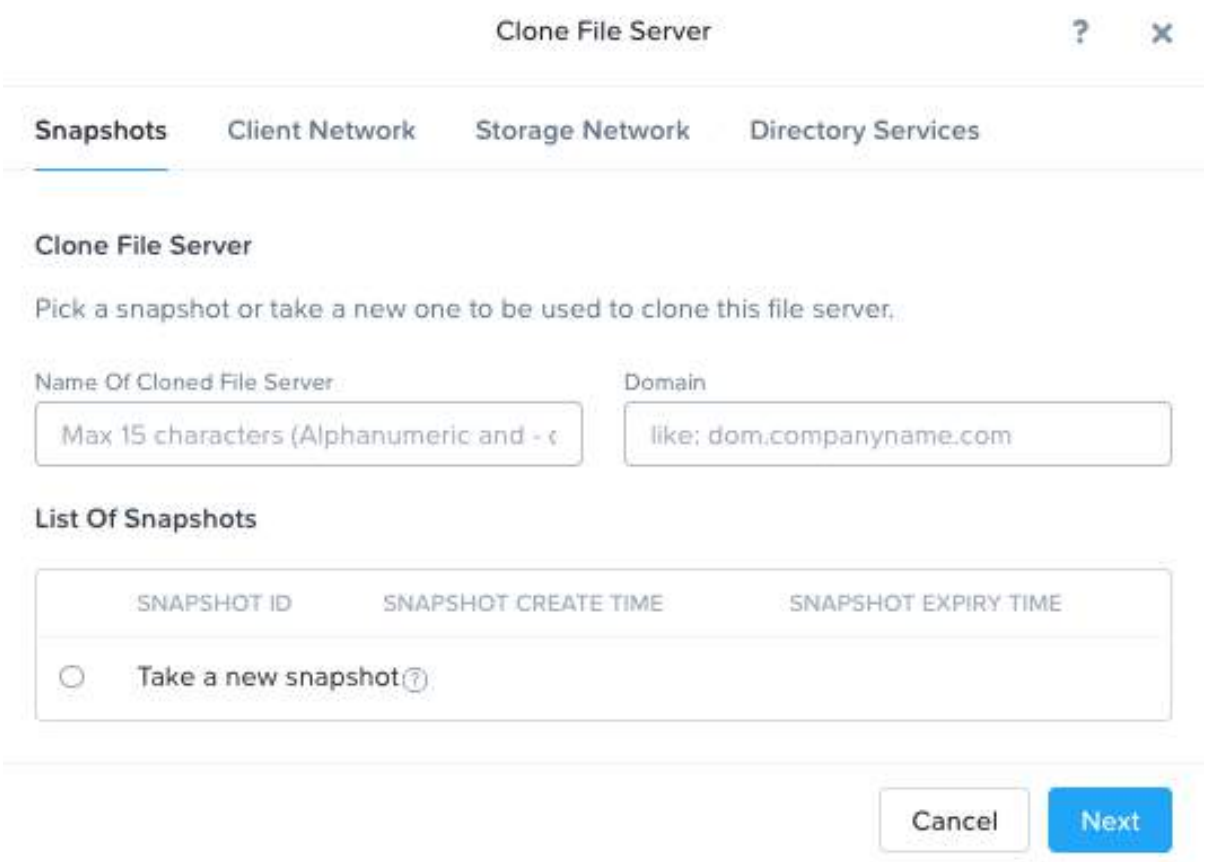


Figure 64: Clone File Server Window (Snapshots tab)

2. In the **Snapshots** tab, do the following in the indicated fields:

   a. **Name of Cloned File Server**: Enter a name for the new (cloned) file server.

      The clone name must be different that the original file server name.

   b. **Domain**: Enter a fully qualified domain.

   c. **List of Snapshots**: Click the option of the snapshot to use for the clone.

      A list of available snapshots (if any) appears in this field. Select one of the existing snapshots or select **Take a new snapshot**, which takes a new snapshot of the file server (after you complete this form) and then use that snapshot to create the clone.

   d. Click the **Next** button.

3. In the **Client Network** tab, enter the required information to configure the client network for the clone and then click the **Next** button.

   Note: See Creating a File Server on page 37 for details about configuring the client network, storage network, and user management.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 527

4. In the **Storage Network** tab, enter the required information to configure the storage network for the clone and then click the **Next** button.

5. In the **Directory Services** tab, select one or more protocols to use (SMB, NFS, or both) and enter the specified configuration information. When all the information is complete, click the **Create** button.

Encryption

Encryption options for Files.

Files supports AOS software encryption and in-flight message encryption for SMB3 shares.

You can apply AOS software encryption to Files by activating it through Prism, see "Configuring Data-At-Rest Encryption (Software Only)" in the *AOS Security Guide*. See the *Nutanix Files Release Notes* to ensure that you are running a compatible version of AOS.

SMB3 Message Encryption

To enable SMB3 message encryption, see Modifying a Share or Export on page 97. After enabling message encryption, Files encrypts messages on the file server side and decrypts them on the client side (only on new connections for the share). Clients that do not support encryption (Linux, Mac, Windows 7) cannot access a share with encryption enabled.

Files Data Collection

Files data collection with Pulse.

The feature known as Pulse collects Files diagnostic system data and sends it to Nutanix Support. After you enable Pulse, Files synchronizes Pulse configurations from the Controller VM to the file server VMs. Synchronized data includes the Pulse enablement status and the mechanism chosen for streaming data to Nutanix Support. If Pulse data cannot reach Nutanix Support, administrators receive alerts in Prism. To enable or disable Pulse, see "Configuring Pulse" in the *Prism Web Console Guide*.

Access-Based Enumeration (SMB only)

Access-based enumeration (ABE) restricts user-access by only letting you view the files and folders you have read-access to when browsing content on a file server.

About this task

ABE is a Microsoft Windows (SMB protocol) feature that filters the list of available files and folders on the file server to only include those you have read-access to. The filtering ensures that Files enforces read-and-write privileges for all users and that information can remain confidential. ABE controls the user visibility of shared folders on mounted file system shares based on the user permissions.

Enable ABE during or after share creation. To activate ABE after a group membership of a user changes, remove all previous share sessions, remount the share, and reconnect existing client connections.

Note:

- To activate ABE after a group membership of a user changes, remove all previous share sessions, remount the share, and reconnect existing client connections.
- Enabling ABE on a Nutanix Files SMB share will have a slight performance hit depending on the number of folders or files.
- For standard shares, ABE is applied to all folders and files in the share.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 528

- For a distributed share, by default ABE is applied only to the share and top-level directories (TLDs). To enforce ABE on the whole subtree, use the following command:

  ```
  nutanix@fsvm$ afs smb.set_conf "abe tld subtree" "yes" section=global
  ```

Procedure

1. To enable ABE during share creation, see Creating an SMB Share on page 77.
2. After creating a file share, you can modify ABE settings. To enable ABE after share creation, do the following:
   a. In the Files Console, go to the **Shares** tab.
   b. In the row for the target share, click the **three dots menu** > **Edit**.
   The **Update Share** window displays.
   c. In the **Settings** tab, check (enable) or clear (disable) the **Enable Access Based Enumeration (ABE)** box and click **Save**.

Enabling SMB Symlinks

Enable symlink support over the SMB protocol.

About this task

A symbolic link (also known as a symlink or a soft link) is a file type that contains a path to a target file or directory.

Although symlink support is enabled by default, Files requires enabling the following link configurations on Windows clients to use symlinks on SMB shares:

- Remote-to-remote
- Remote-to-local

Note: By default, remote to local and remote to remote symlinks are disabled on Windows clients. To enable, symlink access on Windows clients, use the following command.

```
> fsutil behavior set SymlinkEvaluation  R2R:1  R2L:1
```

SMB clients must have symlink access enabled to access symlinks and follow the targets.

Files does not support the following functionalities for symlinks:

- Directory symlinks at the root of distributed shares.
- Alternate data streams (ADS).
- Durable or persistent file handles.
- Opportunistic locks (oplocks) and leases.
- There is no interoperability support between SMB and NFS on Multi-protocol shares for symlinks with absolute targets.

Note: Hycu does not support symlinks. Commvault does not support cross-share symlinks.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 529

Procedure

1. Disable symlink support on the file server.

```
nutanix@fsvm$ afs smb.set_conf "enable smb symlinks" "False" section=global
```

   Disabling SMB links only prevents the creation of new symlinks. Existing symlinks remain accessible.

2. Enable symlink support on the file server.

```
nutanix@fsvm$ afs smb.set_conf "enable smb symlinks" "True" section=global
```

   Disabling SMB links only prevents the creation of new symlinks. Existing symlinks remain accessible.

File Blocking

Restrict specific files or file types from appearing on a file server or share.

Specify a character pattern of file names or extensions to block files. Use an asterisk (*) as a wildcard for multiple characters or a question mark (?) as a wildcard for a single character.

> **Note:** The question mark character (?) only matches UTF-8 single byte ASCII characters. The question mark character (?) does not apply to multibyte unicode characters.

Files applies the file blocking policy to all levels of a share or export, which disables the ability to create files with the specified character pattern in the name. An attempt to create blocked files results in an error. Share-level file blocking overrides the files blocked on the file-server level.

Files allows a maximum of 300 file blocking patterns on a file server.

After enabling file blocking, Files does not permit the following operations:

- Creating a file with the blocked character pattern.
- Renaming an existing file to one with the blocked character pattern.
- Duplicating a file with the blocked character pattern.
- Moving a file with a blocked character pattern.

You can still perform read-and-write operations on existing blocked files.

To enable file blocking on a file server, see File Server Updates on page 55. To enable file blocking on a share or export, see Modifying a Share or Export on page 97.

Files blocked on a share level appear in the **Summary** tab of the **Create share/export** and **Update share/export** windows. Files blocked on a file server level appear in the **Blocked File Types** tab.

Blocking Files on a File Server

Block the creation and modification of files on a share, export, of file server.

About this task

For information about the file blocking feature, see File Blocking on page 141. To block files on the share or export level, see Modifying a Share or Export on page 97.

To block files with specific character patterns in their names, do the following.

Procedure

1. In the **File Server** view, select the target file server.
2. Click **Update** > **Blocked File Types**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 530

3. In the **Blocked File Types** field, enter (or modify) a comma-separated list of file extensions for blocked file types.

Figure 65: Blocked File Types

4. Click **Save**.

Durable SMB File Handles

Durable handles facilitate seamless SMB client reconnection.

Files automatically enables durable handles for SMB shares. Durable handles let SMB clients survive a temporary client-side connection loss after opening a file, allowing transparent client reconnection within a timeout.

Durable handle reconnection times increase when a previous session, with multiple durable handles, must flush the data and metadata before re-establishing the connection.

Note:

- Files does not grant durable file handles for client negotiations with a dialect lower than SMB 3.0.
- Files does not support durable file handles for the directories or alternate data stream (ADS) files.
- Files does not support durable reconnects during server-side copy operations due to the client-side limitation of not attempting to restore the source handle first.

Non-Disruptive Upgrades (NDU) for SMB

NDU support for SMB provides a seamless reconnect experience for SMB connections to non-continuous available (CA) shares during a planned outage.

Note: NDU support is a best-effort solution without any guarantees for the SMB client reconnects.

Note: The non-disruptive upgrade feature does not support file copy over remote desktop protocol (RDP) onto an SMB share.

Files upgrades one node at a time (rolling upgrade). Services on one FSVM failover to another FSVM before an upgrade begins, and failback to the source FSVM after completing the node upgrade. If the failover or failback succeeds within a minute, client applications can seamlessly reconnect to the file services without any failure.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 531

Some applications may time out as they can only tolerate network disruptions for less than a minute. In such cases, the client application retries establishing the connection to the file service. Services do this action by saving the client connection state to the persistent store just before an FSVM upgrade begins, and restore the state after services are available on the taking-over FSVM. This functionality makes most SMB client applications stay connected during the upgrade process.

For applications that require strong guarantees of reconnects (for example, FSLogix and other container based user profile apps), use CA shares.

Antivirus (AV) Scanning (SMB Only)

Third-party antivirus software for SMB shares.

Files supports the Internet Content Adaptation Protocol (ICAP) to enable communication with external servers hosting third-party antivirus software. This software scans files stored on file shares to help provide protection against viruses. This software scans files in real time when you open, close, read from, or write to files.

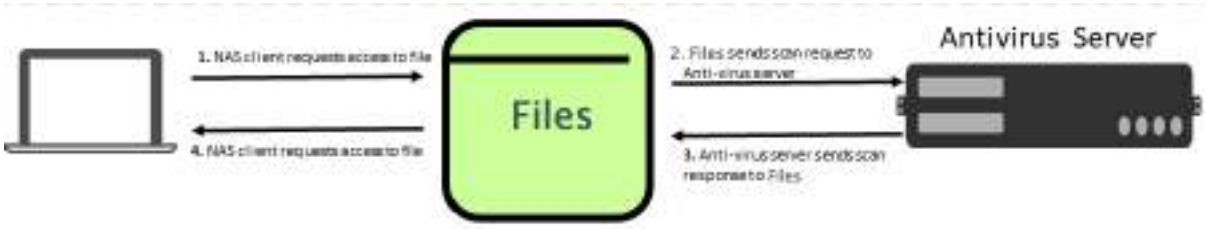


Figure 66: Files AV Concept

Note: For a list of compatible security software, see the Compatibility Matrix. Filter by **Solution Type** > **Security** and **Additional Component** > **Nutanix Files**. Files requires two or more ICAP servers. Nutanix recommends having a minimum number of scanning threads that is 11 times the number of FSVM nodes or (11 * number of FSVM nodes).

Overview

Files performs the following tasks with ICAP servers when a client requests to read, write, open, or close a file.

1. Files determines that the file requires scanning.
2. Files sends files that require scans to the ICAP server with a scan request.
3. The ICAP server scans the file and reports the scan results to Files.
4. Files quarantines and denies access to unsafe files.
5. If the file is clean or disinfected, then Files allows the client access to the file.

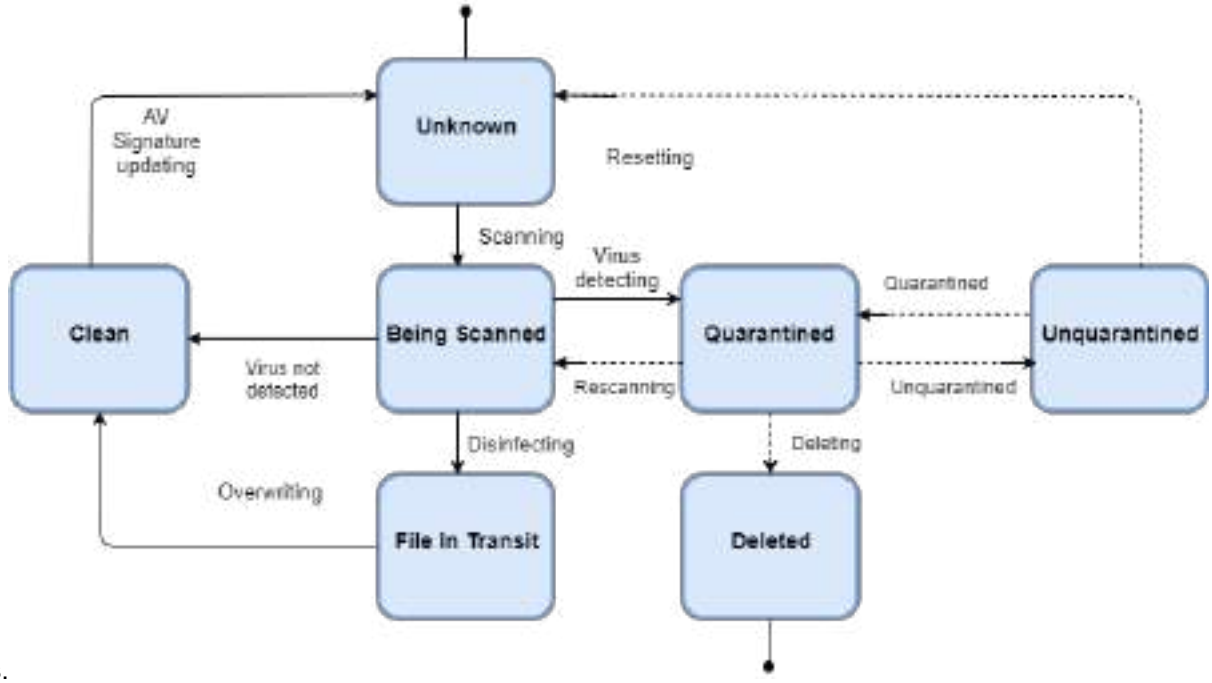
Note: By default, shares have antivirus scan disabled.

Antivirus File State

This diagram shows the process flow for file scans.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 532

Administrator actions are denoted with dotted



lines.

Figure 67: Antivirus File State Diagram

File States and Events

Files and Prism Element use the following terms to indicate the status antivirus scanning applies to files.

Table 29: State

State	Definition
Quarantined	A scanned file that the antivirus scan qualifies as unsafe. Files blocks access to the file until you manually change the file state.
Unquarantined	The administrator moves the file from the quarantined state to allow client access. Files does not rescan unquarantined files.

Table 30: Events

Event	Definition
Cleaned	The antivirus scanner has scanned and cleaned the file. This process overwrites the original file. Using this feature requires the disinfected virus file function on the ICAP server.
Quarantined	A scanned file qualified as unsafe. Files blocks all access to the file until the administrator manually changes the file state.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 533

Event	Definition
Unquarantined	The administrator manually moves the file from the quarantined state to allow client access. Files does not rescan unquarantined files.
Deleted	File removed from the file system.

Configuring Antivirus Scanning (SMB Only)

Configure and enable antivirus scanning for SMB shares.

About this task

> **Note:** To view the entire antivirus scanning configuration page, you need the following permissions: *View File Server Antivirus Server* and *View File Server Virus Scan Policy* .

After configuring the antivirus scan, enable the scan for each share that you want scanned.

Procedure

1. In the Files Console, go to **Configuration** > **Antivirus**.
2. Connect the ICAP server.
   a. Click **+ Connect ICAP Server**.
   A new row appears for new ICAP server details.
   b. Enter the following information in the corresponding fields:
      - IP address or hostname
      - Port (the default port number is 1344)
      - Service name

        > **Note:** Only use this field if you have changed the default service name of the ICAP server. The default service name for most ICAP servers is `avscan`.

      - Description
   c. To save the configuration, click the **check mark icon**.
   For a detected antivirus server, the software tests the validity of the configured server and updates the status to OK.
   d. Ensure the connection status automatically updates to **OK**.
   e. Click **Next**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 534

3. Complete the **Scan Settings**.
   You can override settings through the share-level antivirus settings.

   > **Note:** Nutanix recommends two or more ICAP servers.

   a. **Scan on Write**: Scans saved and updated files (a write operation).

   b. **Scan on Read**: Scans opened files (read operation).
      Nutanix recommends to always enable **Scan on Read**.

   c. **File extensions to be excluded**: Add one or more file extensions to exclude from the scan.

      > **Note:**
      >
      > - Ensure these settings match the file type configuration of your ICAP servers.
      > - Nutanix recommends adding the following file extensions for user profiles when using the Files antivirus scanning:
      >   - .dat
      >   - .ini
      >   - .pol
      > - When the ICAP server incorrectly quarantines files with specific extensions, adding this file type extension to the ignore list only prevents future file quarantines. To access the incorrectly quarantined files, remove them from quarantine.

   d. **File Size**: Limit the size of scanned files.

   e. **Advanced Settings**:

      - **Scan Timeout**: Set the maximum amount of time that a scan can take before timing out.
      - **Block access to files if scan cannot be completed (recommended)**: Block access if the ICAP servers are unavailable or cannot scan the file for any reason.

        > **Important:** If you do not choose the block access option, repeated scan requests might cause severe latency when accessing shares if the ICAP server is unreachable.

   f. Click **Save**.

4. Enable the antivirus scanning on each share.

   a. Go to the **Shares** tab and click on the target share.

   b. In the **Share Details**, go to **Actions** > **Configure Antivirus**.
      The **Configure Antivirus** setup window displays.

   c. > **Note:** To **Disable Antivirus scan**, uncheck the **Enable antivirus scan** and click save.

      Check the **Enable antivirus scan** box.

   d. Check the **Enable antivirus scan** box.

   e. (optional) Change the settings for the share (see Step 3 for details).

   f. Click **Save**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 535

Antivirus Tab

The layout and elements of the **Antivirus** tab in the Files Console.

The **Antivirus** tab displays dynamic information about scanned files. The tab includes the following sub-tabs:

- ICAP servers
- Reports
- Quarantined Files
- Unquarantined Files

To view this information, in the Files Console, go to **Monitoring** > **Antivirus**.

ICAP Servers

The ICAP servers tab displays the scanned files information for each ICAP server.

- **ICAP Server Statistics**: The table displays information such as port number, description, files scanned, disconnect count, average latency, connection status, and actions available.
- **Average Latency**: This graph displays the latency times for the scans (in milliseconds).
- **Files Processed** or **Data Processed**: Click the **Files Processed** drop-down arrow to select the files processed or data processed graph. The processed files graph displays the number of scanned files. The data processed graphs display the amount of processed data (in GiB).
- **Queue Length**: The number of files in the scan queue.

Reports

The **Reports** tab displays the information about the scanning period and share status.

- **Scan Period**: This information displays the files scanned, threats detected, number of files cleaned, and number of files quarantined during each scanning period.
- **Share Status**: Displays the state of the scanned share. The parameters includes: file path, threat description, ICAP server, time, action taken on share.

Quarantined Files

The **Quarantined Files** tab displays the files that contain a virus. The antivirus software places virus-infected files into quarantine where clients cannot read or write the files. An administrator can perform the following actions on the quarantined files.

- **Rescan**: Rescan the files that have been quarantined.
- **Unquarantine**: Move the files out of quarantine. The selected file is then available for use.
- **Delete**: Delete the quarantined file permanently.

Unquarantined Files

The **Unquarantined Files** tab displays files manually released from quarantine. You can use unquarantined files. Files does not rescan unquarantined files again until the administrator resets the unquarantine state. Perform the following actions on unquarantined files.

- **Reset**: Move the files to a normal state that is not quarantined or unquarantined. In this state, the next access to the file triggers the scan.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 536

- **Quarantine**: Move the files to quarantine to block read and write access.

> **Note:** Reaching the limit of the number of files in both the **Quarantined** and **Unquarantined** tables impacts scanning through the UI. The web consoles alerts you when the number of files has reached 80 percent of the number of files supported.

Files REST APIs

Access the Files REST APIs using the Files REST API explorer.

> **Caution:** Files v4 APIs are an early access (EA) feature. Do not use EA features in a production environment. Do not upgrade Nutanix software with EA features to general availability (GA) versions of the software. To participate in the EA program, contact your Nutanix product team. Your use of any EA technology is subject to the Nutanix License and Service Agreement.

The Files REST API Explorer offers developers tools to customize the Files experience using Files v4 REST APIs. You can access the Files REST API Explorer through the Files Console or through an FSVM. The Files service v4 APIs are independent from Prism Element (PE) and Prism Central (PC) APIs. However, the platform APIs, for operations such as create, clone, update or delete a file server, remain in Prism Element (PE).

To access the Files API Explorer in the Files Console (see Files Console on page 21), go to **Files Console** > **REST API Explorer**.

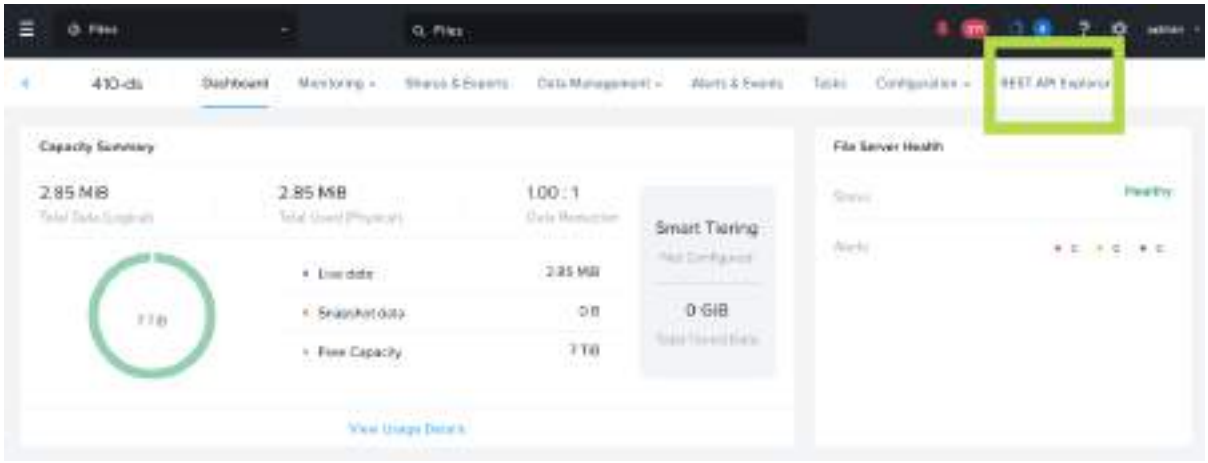


Figure 68: REST API Explorer

ETag and OData Queries Overview

The `ETag` (or entity tag) HTTP response header is an identifier for a specific version of a resource and used to cache unchanged resources. Every POST operation creates a resource, generates and sets a default `ETag` value which is changed in subsequent successful PUT requests used for updating that resource. In the subsequent API requests, this `ETag` value associated with the resource has to be used in the Headers section of the request.

ETag Usage

> **Note:** Use of `ETag` in headers is a must for PUT and DELETE requests, and optional for GET requests.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 537

- **Getting the current value of `ETag` associated with the resource.**

  In the **Headers** section of the GET request, you must have the Key-Value pair as `Accept-Encoding: gzip`

  If the response is successful, then the **Headers** section in the response will have a Key named **ETag** with its value in resource.

  > **Note:** Continue using `Accept-Encoding: gzip` in the **Headers** of GET/PUT/DELETE requests.

- **Using `ETag` in GET operations**: Specifying `ETag` in the **Headers** section of the request is optional and can be used by adding the following Key-Value pair.

  ```
  If-None-Match: ETag value
  ```

  If the *`ETag value`* specified in the header is the same as the current `ETag` value in the resource, then the response will be a 304 Not Modified status without a body. If the `ETag` value does not match, the server will send the full payload with the latest `ETag` value in the response headers.

- **Using `ETag` in PUT/DELETE operations**: Specifying `ETag` in the **Headers** section of the request is mandatory and can be specified by adding the following Key-Value pair:

  ```
  If-Match: ETag value
  ```

  If the *`ETag value`* specified is same as the current value in the resource, then edit or delete operations will be successful else the request will fail with the 412 Precondition Failed status.

OData Queries

While using OData (Open Data Protocol) queries in GET calls, you can use filter expressions in OData requests to filter and return only those results that match the expressions specified. You do this by adding the `$filter` system query option to the end of the OData request.

For example, sample request URLs would look like this:

```
 https://PC_IP_address:9440/api/files/v4.0.a2/config/file-servers/File Server UUID/
mount-targets?$filter=type eq Schema.Enums.MountTargetType'STANDARD'
```

```
https://PC_IP_address:9440/api/files/v4.0.a2/config/file-servers/
fe17badf-30b7-43b1-6b4f-99cfab250d48/mount-targets/File Server UUID/snapshots?
$filter=name eq 'std_1_snap_1'
```

For more information, refer to *Files API Explorer*.

Using the Files API Explorer

Steps to use the API Explorer for Files.

Before you begin

Make sure you have added a REST API user and authorized them, see Managing REST API Roles on page 127. Also, make sure you have read about using ETag and OData queries while making API requests, ETag and OData Queries Overview on page 148.

About this task

> **Caution:** Files v4 APIs are an early access (EA) feature. Do not use EA features in a production environment. Do not upgrade Nutanix software with EA features to general availability (GA) versions of the software. To participate in the EA program, contact your Nutanix product team. Your use of any EA technology is subject to the Nutanix License and Service Agreement.

Do the following, to use the API explorer:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 538

Procedure

1. Go to **Admin** > **REST API explorer**.

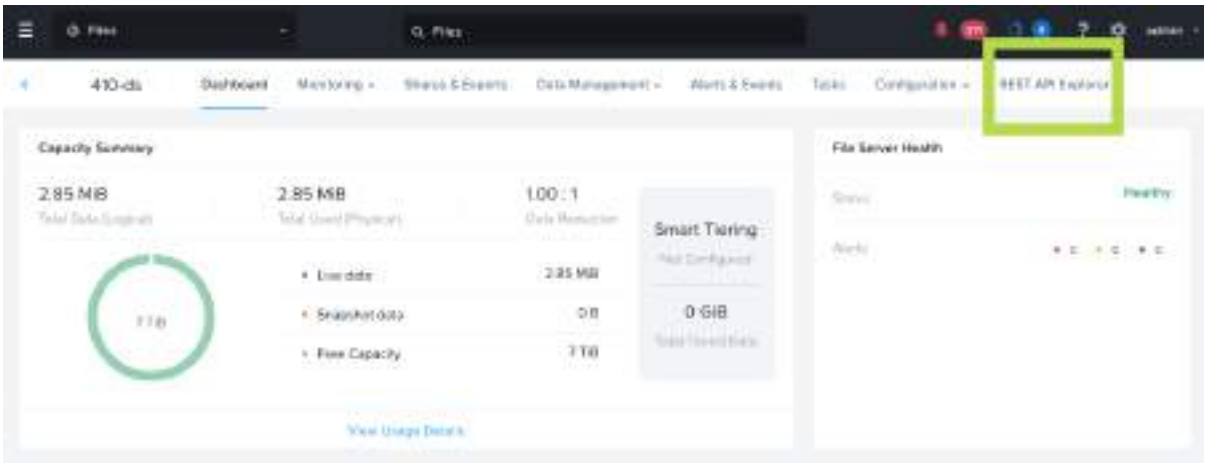


Figure 69: REST API explorer

2. Click the API from the left navigation page that you want to run.
   You can also search for the APIs in the search bar at the top left.
3. Click **Try**.

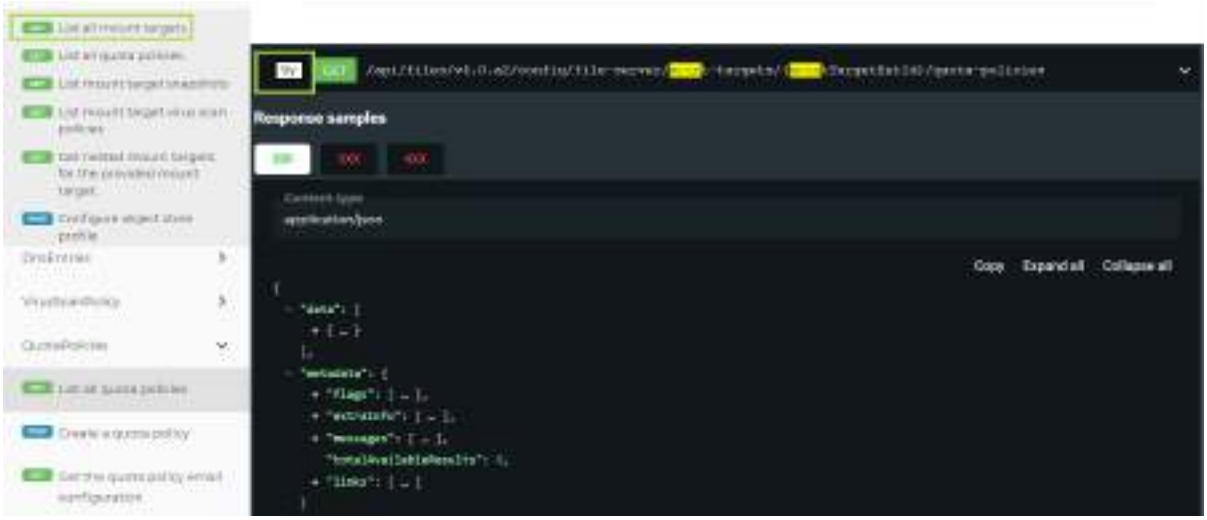


Figure 70: REST API Explorer

List of parameters with its descriptions and response types are listed.

> **Note:** All APIs does not have parameters.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 539

4. Click **Try it Out**.

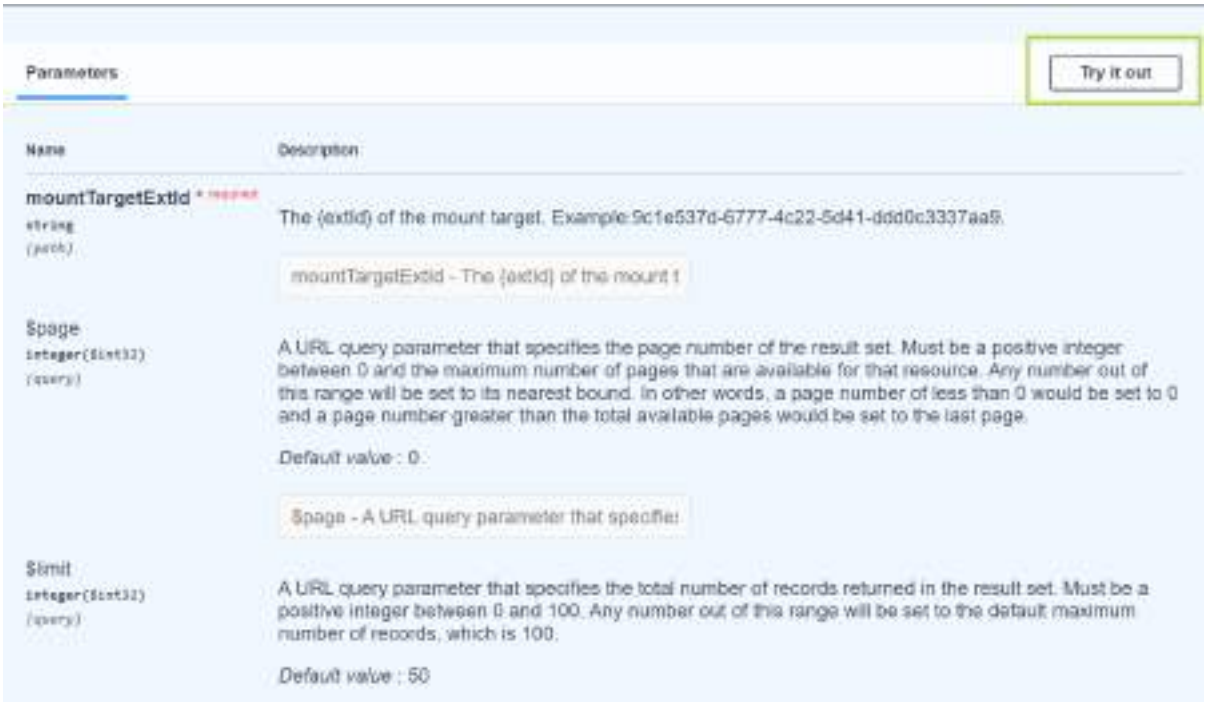


Figure 71: REST API Explorer

5. Enter the values as required for the parameters and response types.
6. Click **Execute**.

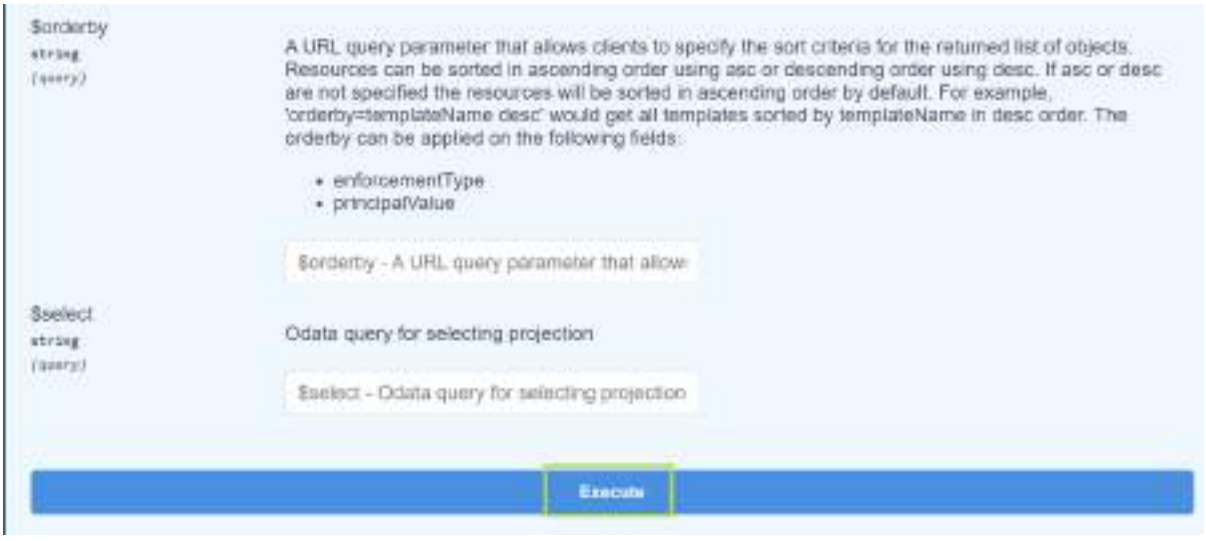


Figure 72: REST API Explorer

The responses are listed.

Note: You can also click **Download** to download the response.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 540

PERFORMANCE OPTIMIZATION

Files performance optimization notifies you when the file server is under load and needs a change to improve optimization.

Performance optimization includes scale up and scale out options. The **Dashboard** tab in the Files Console includes a **Recommendations** widget that indicates performance optimization options.

Scale-up recommendations occur when an FSVM reaches 95% client connection utilization over a two hour time window. If performance is slow due to storage group disruption, the recommendations for optimal performance options appear in the **Recommendations** widget. When possible, perform scale-out and rebalancing operations during maintenance windows, as scaleout and rebalancing disrupts existing connections.

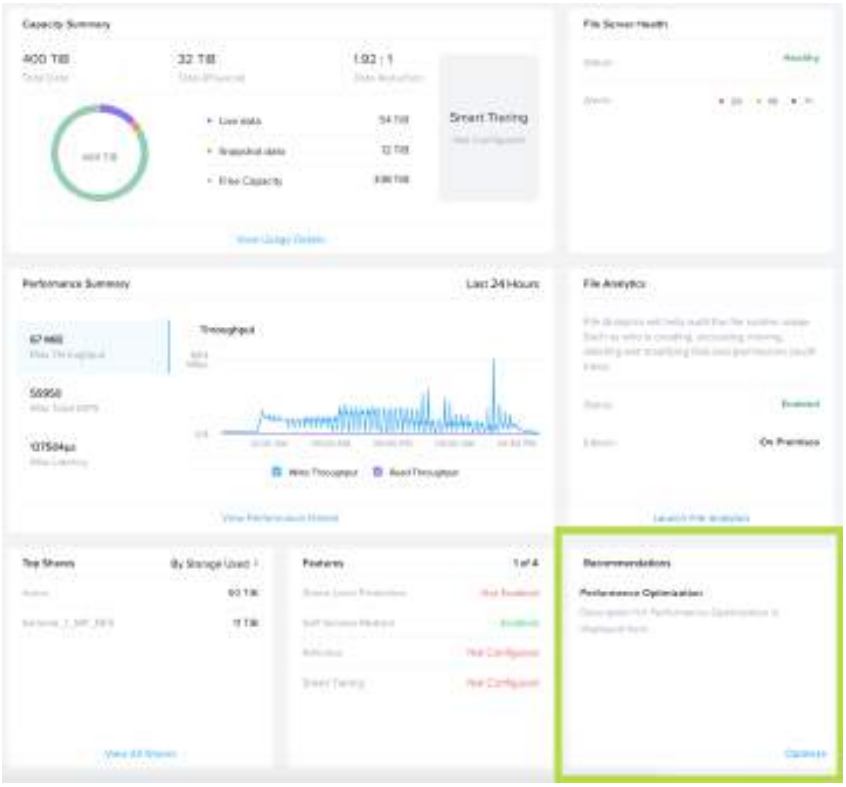


Figure 73: Performance Optimization Recommendations

Managing Performance Optimization

Performance optimization moves consistently used storage between available storage groups within the file server.

About this task

Caution: This operation can cause a momentary connection drop for end users accessing files on the file server. When possible, perform scale-out and rebalancing operations during maintenance windows, or off-peak hours.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 541

Procedure

1. In the Files Console, go to the **Dashboard** tab.
   The file server displays a warning to recommend performance optimization.

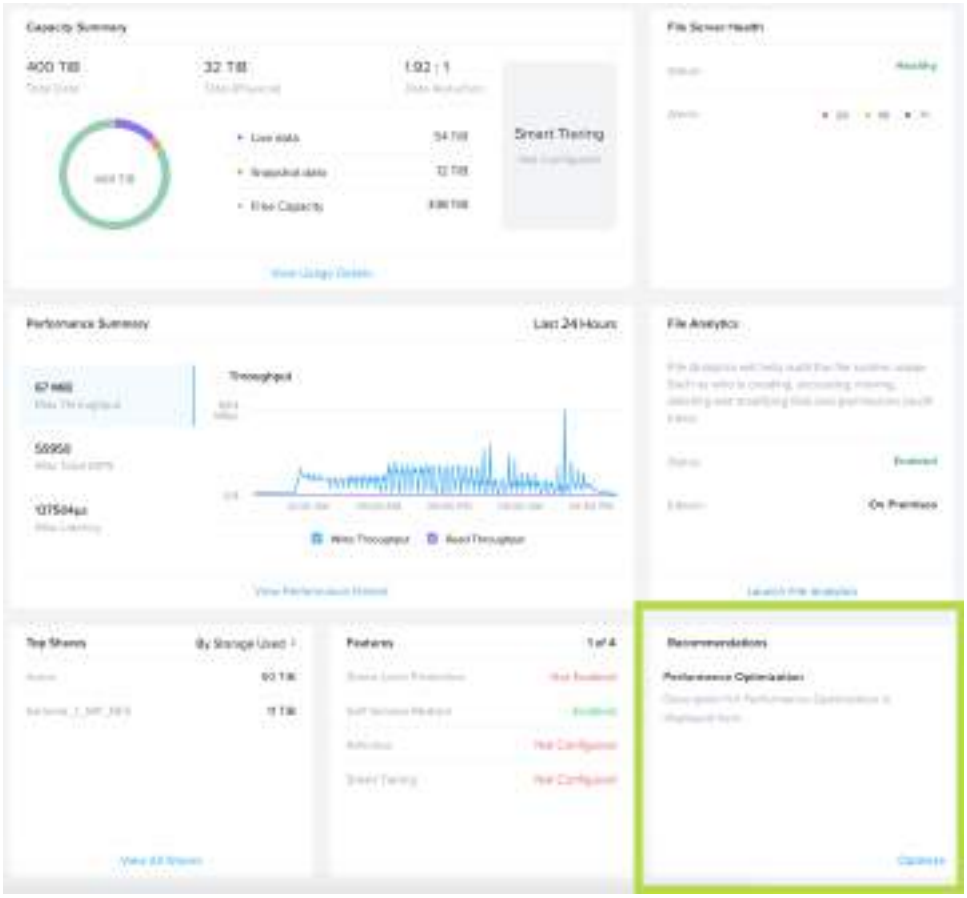


Figure 74: Performance Optimization Warning

2. Under **Recommendations**, click **Optimize**.
   The **Recommendations: Performance Optimization** window appears.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 542

3. Select one of the following options:

   » Scale up

   » Rebalance

   » Scale-out

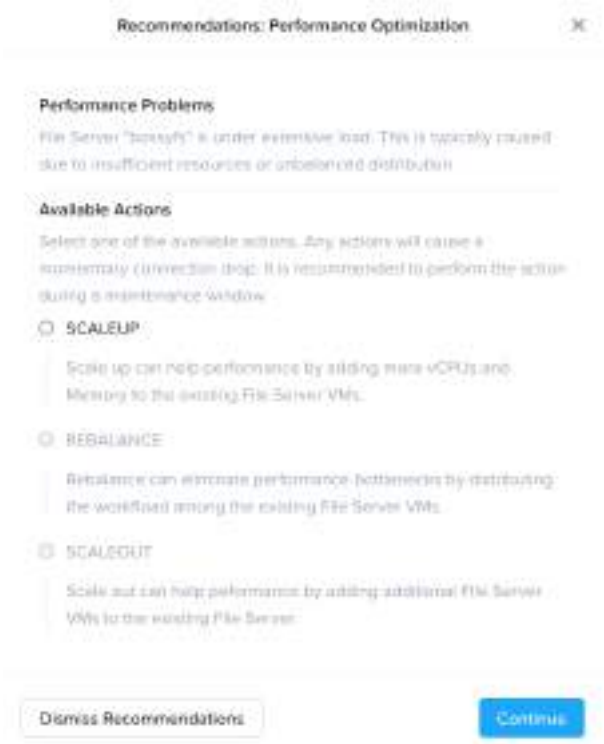


Figure 75: Performance Optimization Recommended Options

4. Click **Continue**.

   » For the rebalancing, confirm that you are performing the operation during off-peak hours.

   > **Note:** Perform rebalance operations during off-peak hours. For earlier AOS versions, you must manually unblock the rebalancing operation, see Unblocking Rebalancing on page 155.

   » For scale up or scale out, continue to the next step to update the file server capacity configuration.

5. (Scale up and scale out only) update the file server capacity configuration.

   a. Review or modify the recommended value for **Number of VCPUs Per File Server VM** as it appears in the drop-down menu.

   b. Review or modify the recommended value for **Memory Per File Server VM** as it appears in the drop-down menu.

   c. To complete the configuration, click **Save**.

Dismissing recommendations

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 543

6. In the **Recommendations: Performance Optimization** window, click **Dismiss Recommendations**.
   New recommendations appear in the **Recommendations** widget once the system identifies new instances of high performance load.

Unblocking Rebalancing

Unblock rebalancing guardrails.

About this task

Files guardrails prevent initiating rebalancing operations during high-volume periods.

Procedure

Unblock load-balancing guardrails on the file server.

```
nutanix@fsvm$ afs lb.unblock_rebalancing
```

Workload Optimization

This topic describes options for optimizing the performance of your Files cluster.

There are three types of share workload types: default, random, and sequential. Designating a workload type determines the file system characteristics (including block size) used for the share, which optimizes the resource usage and performance of certain workloads. For example, workloads with small I/O on large files perform more efficiently with small block sizes.

The different workload types have the following specifications.

- Default: Uses 64 KB per block. Does not provide specified optimization. The share can perform all workloads varying performance
- Random: Uses 16 KB per block. Optimized for small I/O workloads.
- Sequential: Uses 1 MB per block. Optimized for large I/O workloads. Requires a minimum of 24 GB memory per FSVM.

The **Shares** view in the Files Console includes a **Metrics** tab and a **Performance** subtab, which displays write, read, and metadata I/O per second in the **IOPS** graph. Use the data from the graph to configure the workload type for the share, see Modifying the Workload Type on page 155.

> **Caution:** If you modify the share type without following the workload optimization guidance as specified, share performance can degrade.

- If the I/O sizes for read and write operations are less than or equal to 16 KB and the file sizes equal to 10 MB or more, use the **Random** workload type.
- If the I/O sizes for read and write operations are less than or equal to 1 MB and the file sizes equal to 10 MB or more, use the **Sequential** workload type.
- If the I/O sizes for read and write operations do not match the criteria for **Random** or **Sequential** workload types, use the **Default** workload type.

Modifying the Workload Type

To optimize performance, modify the workload type of a share or export.

About this task

Perform the following steps to modify the workload size of a share or export, see Workload Optimization on page 155 for optimization guidelines.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 544

Note: Changing the workload type of a share changes the performance characteristics only for the files created after the change.

Procedure

Modify the workload size.

```
nutanix@fsvm$ afs share.edit share-name share_workload_type=workload
```

Replace *share-name* with the name of the share or export. Replace *workload* with one of the following workload types: `default` , `sequential`, or `random`.

File System Compression

File system compression reduces the input and output (I/O) load, iSCSI traffic, space usage, and the amount of data on a share or export.

You can enable file system compression at the share or export level. Earlier versions of Files included compression at the container level. Files applies share-level compression during ingest operations, compressing incoming data in-line prior to writing it to storage. As a result, share-level compression reduces storage traffic between Files and AOS.

Note: Only clusters created with later versions of Files and AOS support file system compression. The option to enable file system compression does not appear on clusters created with earlier versions of Files and AOS.

To enable or disable compression on the share-level, see the following:

- Creating an NFS Export on page 83
- Creating an SMB Share on page 77
- Creating a Multi-Protocol Share or Export on page 90
- Modifying a Share or Export on page 97

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 545

DATA MANAGEMENT

File server data recovery and management options.

Files provides several features for managing the data on your file server. Manage data availability using data recovery features, which include self-service restore (SSR) and several types of disaster recovery (DR). Consolidate and organize your data using data management features.

Files provides the following DR features:

- **Async and NearSync DR:** Async and NearSync DR are Prism Element (PE) based DR solutions that replicate data to a protection domain on a set schedule. The *Data Protection and Recovery with Prism Element* guide provide information on both solutions.
- **Metro Availability (Metro) for ESXi:** Metro is also a PE-based DR solution. Unlike Async and NearSync DR, Metro provides synchronous data replication to the protection domain and is only available for ESXi hypervisors. See Metro Availability for Nutanix Files on page 164.
- **Smart DR:** Smart DR replicates data with share-level granularity to a recovery file server (see "Smart DR" in the *Files Manager User Guide* for information on Smart DR).

Files provides the following data management features:

- **Smart Tiering:** Smart Tiering maximizes space on the file server by moving stale data to an object store. Use the Files Console to configure standard Smart Tiering policies and Data Lens for advanced Smart Tiering. See the Smart Tiering on page 166 and the Data Lens User Guide for more information.
- **Data Synchronization:** Data synchronization is a Prism Central (PC-based) feature that lets you consolidate data from one or more source paths on a file server to another file server. Manage synchronization policies and locations using the Files Manager (Files on PC). For information on data synchronization, see "Data Synchronization" in the *Files Manager User Guide*.

  Important: You cannot upgrade file servers with technical preview data synchronization policies to general availability (GA) versions. Delete policies created during the technical preview.

- **Self-Service Restore:** SSR takes read-only snapshots at the share level. Based on your snapshot retention configuration, you can recover a share, data from a deleted file, or an earlier file version. File-level SSR for SMB lets you restore and manage previous versions of Files at the system level, while file-level SSR for NFS lets you restore files by manually copying read-only snapshot versions. Both DR and SSR let you configure a snapshot interval, but with SSR, you cannot set a specific time to take the snapshot. See Self-Service Restore on page 176 for more information.

Data Protection and Recovery

Files provides disaster recovery (DR) through customizable protection domains and protection policies.

Tip: For information on disaster recovery with share-level replication, see "Smart DR" in the *Files Manager User Guide*.

As part of DR, Files creates a protection domain for a file server and the entities within the file server (such as VMs and volume groups) during file server creation. By default, Files adds all entities on the file server to the protection domain. You can provide custom names for the file server protection domains at the time of setting up the file server (see Creating a File Server on page 37). If a file server does not have a specified protection domain name, the default protection domain name is NTNX-`file_server_name`. If you clear the checkbox for the protection option during file server creation, Files does not create the protection domain.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 546

For more information on managing protection domains, see *Data Protection and Recovery with Prism Element*.

To activate Async or NearSync DR, enable and set up the schedule for snapshots and replication for the protection domain. Files Async and NearSync DR take snapshots when the preceding snapshot is complete. Async has a 60-minute recovery point objective (RPO), and NearSync has a 1-minute RPO. To activate Metro Availability for ESXi, see Metro Availability for Nutanix Files on page 164.

Files creates a dedicated container for each file server instance, which cannot be used by another file server, VM, or for any other purpose. This requirement also applies to remote containers used for replication. If you want to replicate a file server container to a remote site, make sure that the remote container, like the local container, is not used for any other purpose. The remote site must have at least the same number of nodes as the number of FSVMs in the Files instance. To ensure feature parity after activating the file server on the remote site, both sites must have the same AOS version.

Files supports cross-hypervisor NearSync and Async DR.

Note:

- You can restore all self-service restore (SSR) and Windows Previous Version (WPV) snapshots that exist at the time of the protection domain (PD) snapshot locally or remotely.
- Files does not support DR with one-hour RPO on high-density nodes. To check the supported frequency for the snapshots across various hardware configurations, refer to the "Snapshot Frequency" table in the *Resource Requirements Supporting Snapshot Frequency (Asynchronous, NearSync)* section of the *PD-Based DR* guide .
- Files does not perform frequent suspend and resume operations of the protection domain. Files performs protection domain suspend and resume operations during meta-data pinning on flash drives.

Configuring Disaster Recovery

Set up file server disaster recovery for planned or unplanned (disaster) migration.

About this task

To protect the VGs associated with a file server, Nutanix recommends using this Files workflow and not the Prism Element workflow. You need vStore mapping to initiate the full replication of protected entities to the specified target container. You can only define the vStore mapping for the file server using Files workflow for DR.

To set up file server Async disaster recovery (protection domain based), follow the steps in this procedure.

Note: Refer to "Smart DR" in the *Files Manager Guide*, for steps on configuring Smart DR.

Procedure

1. If you have not done so already, configure a remote backup site to the local cluster.

   See the "Configuring a Remote Site (Physical Cluster)" topic in the *Data Protection and Recovery with Prism Element* guide.

   Note: The remote site must have at least the same number of nodes as the number of FSVMs in the Files instance.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 547

2. In the **Files Console** (see Files Console on page 21), go to **Data Management** > **Protection**.

   The **Disaster Recovery** and **Self Service Restore** tabs appear. In the **Disaster Recovery** tab, the **Protection Domain (PD) Based** and **Smart DR** sections specify if the indicated DR type is enabled.

   After creating a file server, Files automatically adds the file server to a newly created protection domain. However, when the file server does not have a protection domain, the **Configure** action link displays in the **Protection Domain (PD) Based** section with the **not enabled** status.

3. To add the file server to a protection domain, do the following:

   a. Click **Configure**.
      Files redirects to the **File Server** view in Prism Element.

4. In the file server table, select the file server by clicking the row it appears in.

5. Under the file server table, click the **Protect** action link.
   The **Protection configuration: [file-server-name]** window appears.

6. In the **Disaster Recovery** section do the following:

   a. (Optional) in the **Protection Domain Name** field, update the name of the protection domain.

   b. Click **Protect File Server**.

7. (Optional) configure a schedule for disaster recovery.

   > **Note:** Prism creates a default schedule for every protection domain.

   a. In the Files Console, go to **Data Management** > **Protection**.

   b. Click **Manage on Prism Element**.
      Files redirects you to Prism Element.

   c. See Creating a Protection Domain Schedule on page 159 to add or modify the protections schedule.

8. Configure the local and remote container mapping.

   a.

   > **Note:** In Metro Availability enabled environments, avoid using identical container names. Ensure that the name of the remote container is unique, then map the containers to each other.

   If you did not map the local and remote containers when configuring a remote site (vStore name mapping), create a new remote container.

   > **Tip:** See the "Creating a Storage Container" section in the *Prism Web Console Guide* for this procedure.

   Changing a vStore mapping causes associated protection domains to initiate full replication of protected entities to the newly specified target container as if it were initial replication. A mapping change therefore results in the overconsumption of storage resources at the remote site. Contact Nutanix Support for help with cleaning up snapshots in the previously specified container.

   b. Ensure that the remote and the local containers have symmetric configurations and that both containers map to each other. On the remote vStore site, configure explicit mapping between the source and the destination container.

Creating a Protection Domain Schedule

Create a snapshot schedule for Files protection domains.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 548

About this task

Files disaster recovery uses snapshot schedules for protection domains.

> **Note:** Ensure to also save the snapshot schedule on the remote site.

Procedure

1. In Prism Element, go to the **Data Protection** tab in the pull-down menu.
2. In the **Table** view and **Async DR** tab, select the protection domain from the table.
3. Click **Update**.
   The "Update Protection Domain" window appears.
4. In the **Schedule** tab, click **New Schedule** (or, to update an existing schedule, click the **pencil icon**).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 549

5. Complete the indicated fields:

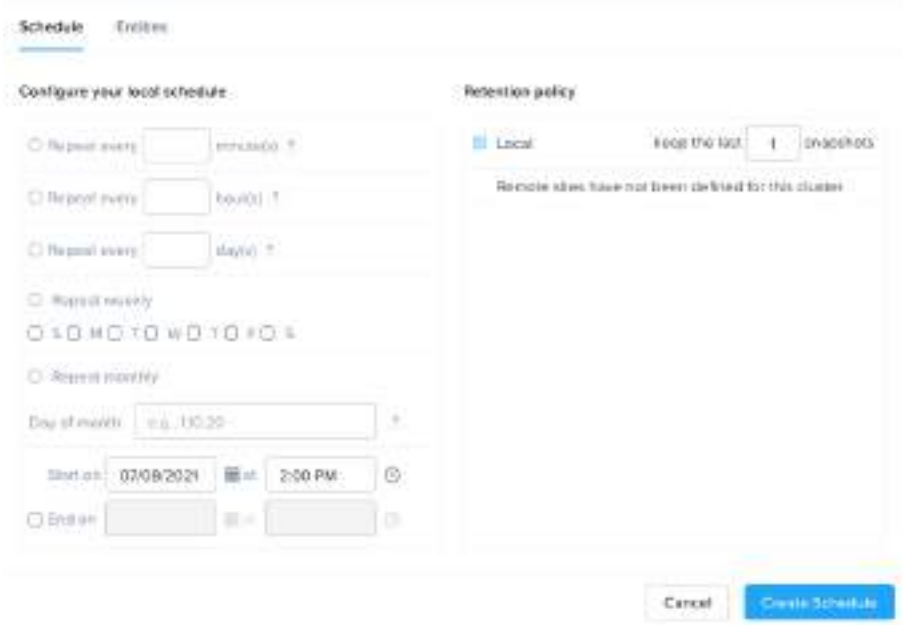


Figure 76: Create the File Server Protection Domain Schedule

a. **Repeat every [minutes|hours|days]**: Click the appropriate circle for minutes, hours, or days and then enter the desired number in the box for the scheduled time interval.

   The interval cannot be less than 1 minute.

   > **Note:** Intervals of less than 60 minutes use NearSync disaster recovery. NearSync schedules inherit requirements and limitations of AOS NearSync, see "Requirements of Data Protection with NearSync Replication" in the *Data Protection and Recovery with Prism Element* guide.

b. **Repeat [weekly|monthly]**: Select which days to run the schedule.

   - If you select weekly, select the boxes for the days of the week the schedule should run.
   - If you select monthly, enter one or more integers (in a comma-separated list) to indicate which days in the month to run the schedule. For example, to run the schedule on the 1st, 10th, and 20th days, enter "1,10, 20".

c. **Start on**: Enter the start date and time in the indicated fields.

   The default value is the current date and time. Enter a new date if you want to delay the schedule from starting immediately.

d. **End on**: To specify an end date, check the box and then enter the end date and time in the indicated fields.

   The schedule does not have an end date by default, and the schedule runs indefinitely unless you enter an end date.

e. **Retention Policy**: Enter the number of snapshots to save locally and at the remote sites.

   - Enter a number in the **Local** line "**keep the last ## snapshots**" field. The default is 1.
   - Enter the number of snapshots to save on the **Remote Site** in the "**keep the last ## snapshots**" field. This number can be different from the number that you have entered in the **Local** line. This

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 550

replication is an async replication. After the replication completes, the protection domain is going to be available in the **Async DR** tab of the remote site.

- The saved snapshots equal to the value entered in the **keep the last ## snapshots** field + 1. For example, if you entered 20 as the value for **keep the last ## snapshots** field, Files saves 21 snapshots. When Files takes the next (22nd) snapshot, Files deletes the oldest snapshot and replaces it with the new snapshot.

  Note: If too many schedules have the same start time, replications can fall behind. To avoid this issue, stagger start times across schedules.

Activating Disaster Recovery

How to recover a file server after a planned or unplanned migration.

About this task

Fail over and fail back a protection domain.

Note: The name for the automatically created protection domain contains NTNX as a prefix followed by the file server name.

Procedure

1. Fail over the protection domain.

   Unactivated protection domains display shaded indicators next to the protection domain name. Activated protection domains display green indicators next to the name. For AOS 5.15 in later, see "Failover and Failback Operations for Asynchronous and NearSync DR" in the *Data Protection and Recovery with Prism Element* guide. For earlier AOS versions, see the "Failing Over a Protection Domain" topic in the *Data Protection and Recovery with Prism Element* guide for either a planned (migration) or unplanned (disaster recovery) activation procedure.

2. Fail back a protection domain.

   See the "Failing Back a Protection Domain" topic in the *Data Protection and Recovery with Prism Element* guide for steps.

What to do next

Activate the file server for planned or unplanned migration. See Activating a File Server on page 162.

Activating a File Server

Activate an inactive file server.

About this task

Follow the steps as indicated to activate a file server after disaster recovery.

Procedure

1. In the Prism Element **File Server** view, select the target file server.

   When a file server is inactive, (Needs activation) appears next to the file server name and an **Activate** button appears in the action button list (just below the file server table).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 551

2. Click **Activate**.

   The **Activate File Server** window appears.

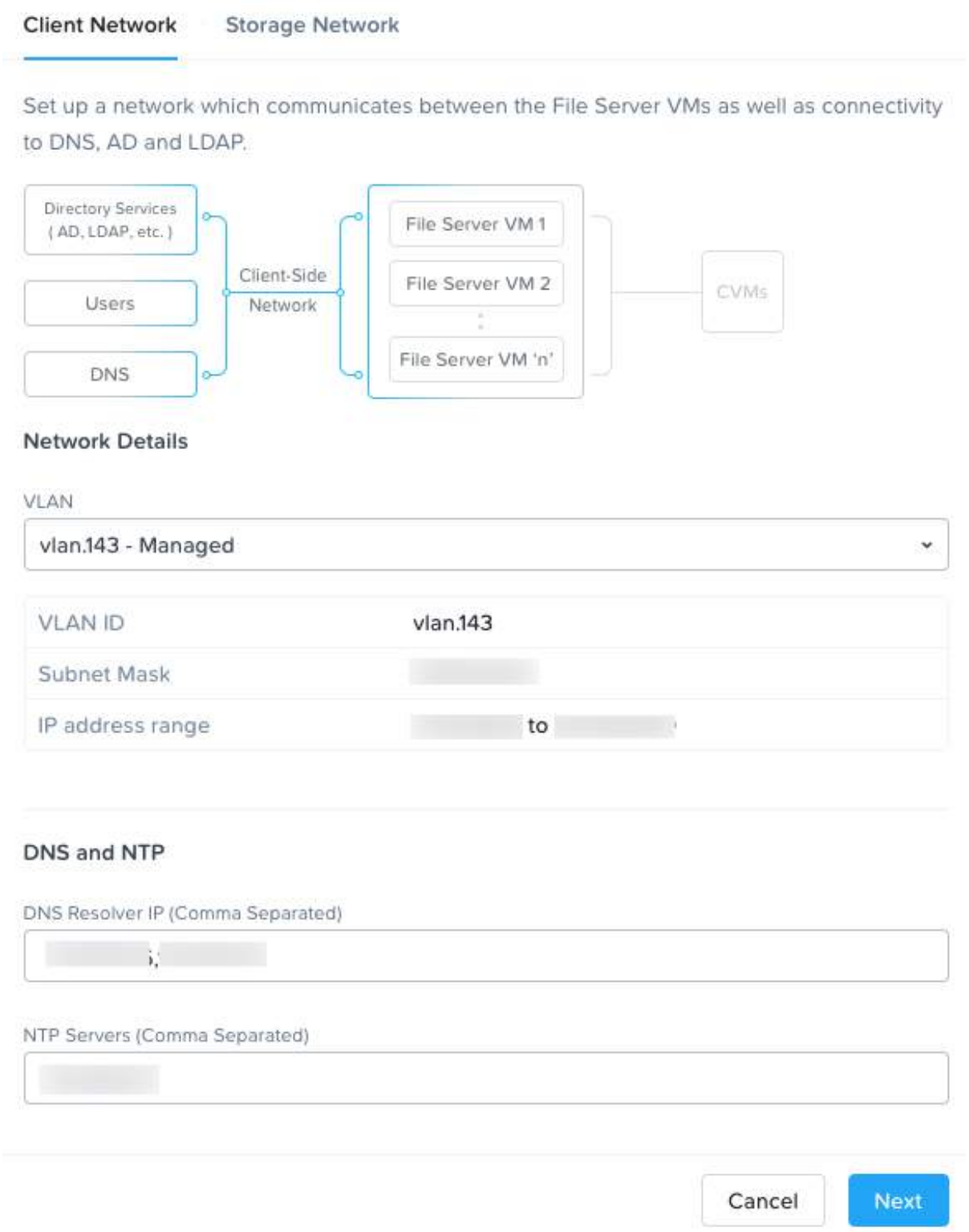


Figure 77: Activate File Server

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 552

3. Complete the indicated fields in the **Client Network** and **Storage Network** tabs.

   Some fields populate from the information provided during file server creation. See Creating a File Server on page 37 for more information about the fields.

4. When all of the information is complete, click **Save**.

   The file server configuration updates, and the (Needs activation) message disappears indicating the file server is now active.

Metro Availability for Nutanix Files

Use Metro Availability (Metro) as a synchronous DR solution for ESXi Files clusters.

Metro is a disaster recovery solution that provides synchronous replication of data to a remote site. To configure Metro for Files, create a Metro protection domain (PD) for the file server. After configuring the PD, you can monitor and manage the configuration from the **Data Protection** tab in Prism.

Learn more about Metro in the Data Protection and Recovery with Prism Element Guide.

Do the following to configure Metro for Files:

- Check the File Server Table in Prism Element to ensure the target file server is not part of a protection domain. See File Server View in Prism on page 19.
- Configure remote sites. See "Configuring a Remote Site (Physical Cluster)" in the *Data Protection and Recovery with Prism Element* guide.
- Configure the vSphere cluster in vCenter:

  Note: For information on vCenter, see VMware documentation.

  - Configure AOS hosts to vSphere. For information on configuring vSphere. See "vSphere Metro Storage Cluster for Nutanix Metro Availability" and "VMware vSphere Settings".
  - Configure port groups to hosts.
  - Ensure that the vCLS VMs are in the proper container. See vSphere Cluster Services on Nutanix Clusters.
- Configure the witness VM. (Once configured, the witness VM appears on both sites). See "Installing a Witness VM" in the *Data Protection and Recovery with Prism Element* guide.
- Create a remote site container with the same name as the source site container. See "Creating a Storage Container" in the *Prism Web Console Guide*.
- Enable Metro for the File Server. See Enabling Metro Availability on page 165.
- Manage your Metro for Files deployment in the **Protection** view of Prism Element.

Metro for Files supports witness and automatic resume failure handling. For unplanned failovers with the witness mode, FSVM migration and promotion of the protection domain (PD) occurs automatically. During planned failovers in the witness mode, manually migrate the FSVMs to the remote site. In the automatic resume mode, for planned failovers, migrate the FSVMs manually, and for unplanned failover manually promote the PD. For failbacks, irrespective of the failure handling mode, manually migrate the FSVMs to the original site in vSphere and manually trigger promote. For more information, see Metro Availability on ESXi in the Data Protection and Recovery with Prism Element guide.

Note: After a Metro failover, if the primary site is in a healthy state, manually re-enable Metro.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 553

Requirements

Meet the following requirements before deploying Metro Availability with Nutanix Files.

- Each file server must have its own protection domain.
- The minimum number of nodes on the remote site must be equal to or greater than the maximum number of FSVMs per file server on the source.
- Reference existing ESXi Metro requirements. See Conditions for Implementing Data Protection (Metro Availability) in the *Data Protection and Recovery with Prism Element Guide*.
- Refer to the *Nutanix Files Release Notes* for compatibility requirements.

Limitations

Data Protection and Recovery with Prism Element Guide lists general limitations for using Metro, which apply to Files. The following limitations also apply:

- Each file server must have its own protection domain.
- You cannot configure Metro on a cloned file server or clone file servers in Metro protection domains.
- Metro uses the same set of IP addresses and networks for file server VMs on the target and the primary site.
- Upgrade operations, adding and removing FSVMs, and renaming the file server temporarily suspends Metro.
- Metro only supports automatic failures and witness failure scenarios
- If an ESXi host reboots while the protection domain is in a decouple state, the host may be in a permanent all-paths-down (APD) state, which requires manually unmounting and remounting the datastore.

Enabling Metro Availability

Enable Metro Availability for Files on ESXi.

About this task

Do the following.

Procedure

Enable Metro for the source file server.

```
nutanix@CVM$ ncli fs protect uuid=fs_uuid pd-name=pd_name
remote-site-name=remote_site_name enable-witness=true|false metro-avail=true
```

Replace *fs_uuid* with the universally unique identifier of the source file server.

Replace *pd_name* with the name of the protection domain of the source file server.

Replace *remote_site_ip* with the name of the remote site.

Once enabled, the **Metro Availability** tab in **Protection Domain** view displays the Metro status initially as **Synchronizing** and then as **Enabled (in sync)**.

What to do next

Before failback ensure that Metro is in standby-active mode, with the primary site in standby.

Metro for Files supports witness and automatic resume failure handling. For unplanned failovers with the witness mode, FSVM migration and promotion of the protection domain (PD) occurs automatically. During planned failovers in the witness mode, manually migrate the FSVMs to the remote site. In the automatic resume mode, for planned failovers, migrate the FSVMs manually, and for unplanned failover manually

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 554

promote the PD. For failbacks, irrespective of the failure handling mode, manually migrate the FSVMs to the original site in vSphere and manually trigger promote. For more information, see Metro Availability on ESXi in the Data Protection and Recovery with Prism Element guide.

Smart Tiering

Tier data to an object store using Smart Tiering.

You can free up space on your file server by tiering data to an object store. There are two ways to perform tiering: manage and define policies through the Files Console using **standard tiering** or through Nutanix Data Lens using **advanced tiering**.

To configure standard tiering, go to **Data Management** > **Smart Tiering** > **Enable and Configure Tiering**. Update all of the required fields as described in Smart Tiering Dashboard on page 169.

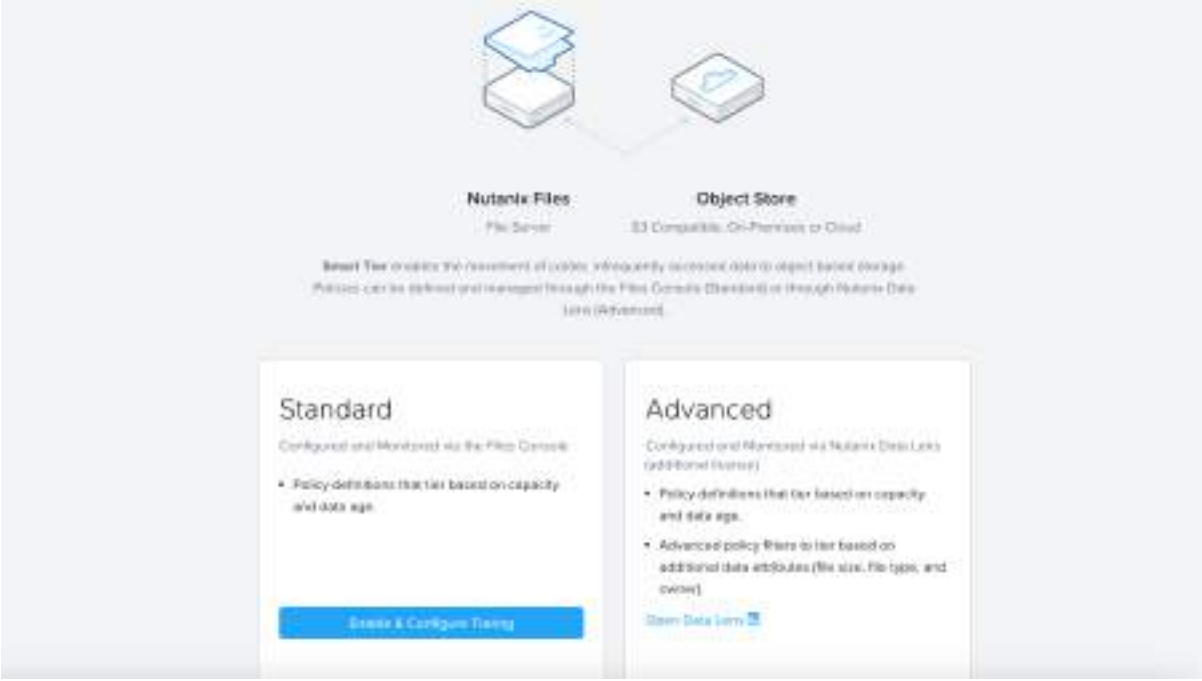


Figure 78: Set Up Tiering

Standard Tiering Overview

Standard Smart Tiering manages hot, warm, and cold file server data.

Use Smart Tiering to maximize the available file server space by moving cold data from the file server to an object store. Nutanix supports using Nutanix Objects, Microsoft Azure, AWS Standard, AWS IA, or Wasabi (S3 compatible storage) as the object storage, which you must configure before setting up a tiering profile, for details on setting up Nutanix Objects, see the *Objects User Guide*.

Tiered storage does not contain the full data set. The full metadata and pointers to tiered data remain on the primary storage.

> **Note:** You can create a tiering profile with AWS Glacier instant retrieval storage class in addition to Object Store, AWS, and S3 compliant storage classes.

Do the following to enable tiering on the file server:

- Review the "Limitations" section.
- Review the Smart Tiering Requirements and Recommendations on page 167 section.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 555

- Configure the tiering location and profile, see Configuring a Tiering Location on page 170.
- Configure the tiering capacity threshold, see Setting a Capacity Threshold on page 172.
- Configure a tiering policy, see Creating a Tiering Policy on page 174.

Limitations

- You can only add a migration target share to a tiering profile once the migration plan completes.
- You can only have one tiering profile and tiering location for each file server.
- You cannot evict tiered file data from the primary storage until all snapshots containing the file expire.
- You cannot tier files that are smaller than 64 KiB or larger than 5 TiB.
- You cannot write to tiered (offline) files.
- You can only configure tiering at the file-server level.
- After re-enabling versioning, tiering operations need a minimum of 10 minutes to resume.
- Files cannot compress data while tiering data to the object store.
- Files does not tier sparse files.
- None of the object stores support WORM-enabled buckets.
- As part of Wasabi, garbage collection of the objects does not work.

Terminology

- *Capacity threshold* – The percentage of file server capacity you must reach to trigger tiering operations.
- *Object store* – Secondary storage service.
- *Tiering* – Migrating cold data from primary to secondary storage.
- *Tiering profile* – The secondary storage location configuration, which includes the object store, security keys, and the storage bucket.
- *Tiering Policy* – Defines shares to be included or excluded from tiering by file size, and cool off period.
- *Tiering Schedule* – Specifies a window on when to tier and then schedule tiering accordingly.
- *Tiered data in Snapshot* – A tiered file can still have data in snapshot. This data can remain on-prem until the snapshot gets deleted.
- *Data Retention* – Acts on files after Data is deleted from the file server. Once the file is deleted from the file server, the corresponding object gets deleted only after the specified retention period.

Smart Tiering Requirements and Recommendations

Meet the indicated requirements to configure and administer Smart Tiering.

General Requirements

Meet the following general requirements.

- Enable versioning on the object store bucket.
- Disable object lock on the object store bucket.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 556

Note: For Advanced Smart Tiering with Data Lens, refer to the Data Lens User Guide for requirements and administrative guidance.

AWS Simple Storage Service (S3) Requirements

Have the following AWS IAM user permissions.

- s3:GetBucketObjectLockConfiguration
- s3:PutObject
- s3:GetObject
- s3:GetLifecycleConfiguration
- s3:AbortMultipartUpload
- s3:PutLifecycleConfiguration
- s3:CreateBucket
- s3:GetObjectTagging
- s3:ListBucket
- s3:PutObjectTagging
- s3:GetBucketVersioning
- s3:GetObjectVersion
- s3:DeleteObject

Ensure that the security keys have the following permissions on the S3 bucket:

- Set LifeCycle policy
- Read and write
- Set tags on object
- List and write on object

Nutanix Objects Object Store Requirements

- Use the bucket owner secret and access for tiering.
- Ensure that the owner has read and write permissions.

Security Recommendations

Nutanix recommends using the following security best practices:

- Implement security best practices for AWS S3 as described on the AWS documentation portal.
- Do not use the same bucket for storing non-Nutanix Files data.
- Do not manually delete or overwrite any object in the bucket, as this action results in data loss.
- Enable encryption on the bucket.
- Have the permissions to query the bucket location.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 557

- Do the following when changing security keys:
  - Ensure that both keys are valid when changing from key1 to key2.
  - Retire key1 from s3 only after updating key2 on the file server.
- On AWS, Files sets the life-cycle rule on the bucket to garbage collect deleted objects. Do not overwrite or remove the rule from S3. Do not apply another life-cycle rule to the bucket.
- For Nutanix Objects, provide security keys of the owner of the bucket.

Smart Tiering Dashboard

The **Smart Tiering** dashboard includes tools for managing the tiering configuration of a file server.

The **Smart Tiering** dashboard consists of the following primary elements:

- The **Tiering Configuration** pane includes options to configure the tiering location, configure the capacity threshold, and configure tiering policies.
- The **Capacity Summary** pane provides an overview of data distribution on the file server.
- The **Tiering Summary** pane provides an activity monitor of tiering operations.

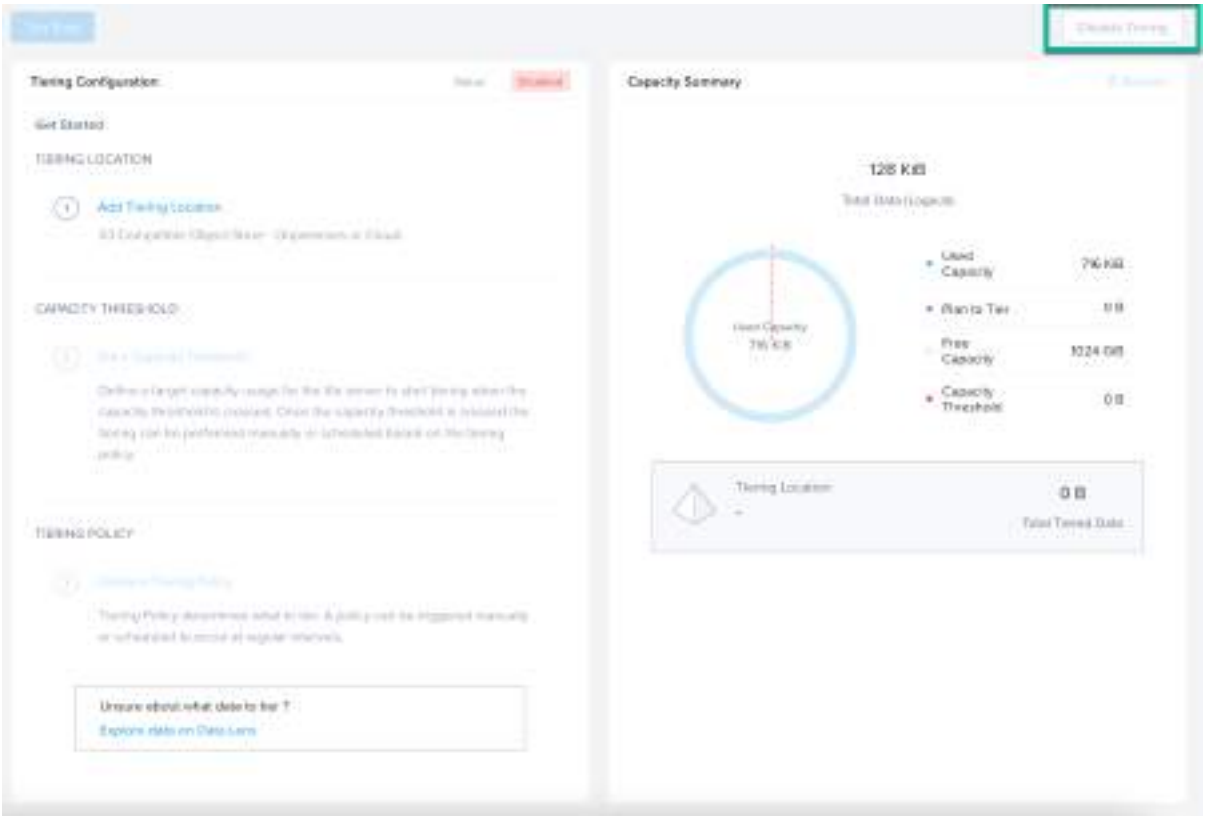


Figure 79: Smart Tiering Dashboard

The following table provides a detailed description of the features of each pane in the dashboard.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 558

Table 31: Smart Tiering Dashboard

Pane	Feature	Description
Tiering configuration	Tiering location section	Indicates the name of the tiering profile and the object store type. Provides an option to configure or edit the tiering location.
	Capacity threshold section	Indicates the configured capacity threshold and whether tiering is manual or scheduled. Provides an option to configure the capacity threshold, edit the capacity threshold, and to set up a tiering schedule.
	Tiering policy section	Indicates the configured tiering policy. Provides option to define files for tiering.
Capacity summary	File server and capacity	Indicates the name of the file server, the capacity used, and the total capacity configured for the file server.
	Used Capacity	Indicates the distribution of data on the file server by the space used, the space planned for tiering, and the free space.
	Plan to tier	Indicates the amount of data on the file server by the space planned for tiering. **Note:** There is no automatic update of values. Click **refresh** to show the current space planned for tiering.
	Free Capacity	Indicates the amount of free space available.
Tier Data	Tier data option	See Tiering Data Manually on page 174.
Disable Tiering	Disable Tiering option	Disable standard tiering.

Configuring a Tiering Location

To tier data, configure a secondary storage object store.

About this task

A tiering profile includes the tiering location and defines the secondary storage target, which is the object store.

Follow the steps as indicated to configure a tiering profile:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 559

Procedure

1. In the Files Console, go to **Data Management** > **Smart Tiering** > **Standard** and click **Enable and Configure Tiering**.
2. In the **Tiering Configuration** pane, under **Tiering Location**, click **Add Tiering Location**.
3. Update the fields as indicated:
   - **Name**: Enter a name for the tiering profile.
   - **Store type**: Select an object store type.
   - **Service host**: Enter a URL of the tiering service host.

     Supported URL formats for S3:

     - `https://s3.<region>.amazonaws.com, for example: s3.us-east-1.amazonaws.com`
     - https://s3.amazonaws.com, here Files tries to get the location constraint by querying the server.

     > **Note:** Do not specify the virtually hosted-style bucket URL. For **service host**, only specify the service host name or s3 endpoint (for example, s3.<region>.amazonaws.com or s3.amazonaws.com). Specify the bucket name in the **bucket name** field.

   - **Access key**: Enter the S3 access key ID for the object store.
   - **Secret key**: Enter the secret access key for accessing the object store.
   - **Bucket configuration**
     - **Bucket name**: Enter a name of the bucket in the object store.

       > **Note:** You cannot change the bucket name.

     - **Retention period**: Enter a period for data retention after deletion from the file server.

       > **Note:** The default retention period is 5 years and the minimum is 6 months.

   - **Certificate**
     - **Certificate**: Upload a secure sockets layer (SSL) certificate file.
     - **Validate certificate**: Check this box to enforce SSL certificate verification during tiering operations after profile creation.

Configuring a Tiering Location (Azure)

To tier data, configure a secondary storage object store.

About this task

A tiering profile includes the tiering location and defines the secondary storage target, which is the object store.

Follow the steps as indicated to configure a tiering profile:

Procedure

1. In the Files Console, go to **Data Management** > **Tiering** > **Standard** and click **Enable and Configure Tiering**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 560

2. In the **Tiering Configuration** pane, under **Tiering Location**, click **Add Tiering Location**.
3. Update the fields as indicated:
   - **Name**: Enter a name for the tiering profile.
   - **Store type**: Select **Azure** or **Azure Cool**.

     Note: Once configured, you cannot modify the store type.
   - **Service host**: Enter a URL of the tiering service host.
     - `For example: blob.core.windows.net`

       Note: Once configured, you cannot modify the service host.
   - **Storage account name**: Enter the name of the Azure storage account associated with the account key.
   - **Account key**: Enter the account access key for accessing your Azure Blob Storage account.
   - **Container configuration**
     - **Container name**: Enter a name of the Azure Blob Storage container.

       Note: You cannot change the container name.
     - **Retention period**: Enter a period for data retention after deletion from the file server.

       Note: The default retention period is 5 years and the minimum is 6 months.
     - **Generate JSON**: Use this option to manually configure the life-cycle policy in the Azure web console.
   - **Certificate**
     - **Certificate**: Upload a secure sockets layer (SSL) certificate file.
     - **Validate certificate**: Check this box to enforce SSL certificate verification during tiering operations after profile creation.

Setting a Capacity Threshold

The capacity threshold specifies when to tier data.

About this task

Follow the steps as indicated.

Procedure

1. In the Files Console, go to **Data Management** > **Smart Tiering**.
2. In the **Tiering Configuration** pane, click **Set a Capacity Threshold**.
3. To tier data based on a threshold of occupied capacity, check the **Set a Capacity Threshold** box.
   a. In the **% of Primary Storage** field, enter an integer that indicates the capacity percentage to trigger tiering (minimum 1%).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 561

4. Under **When to tier**, select an option.

   » To trigger tiering manually after crossing the capacity threshold, select the **Manual** option.

   » To configure a schedule for tiering data, select **Every Day** option.

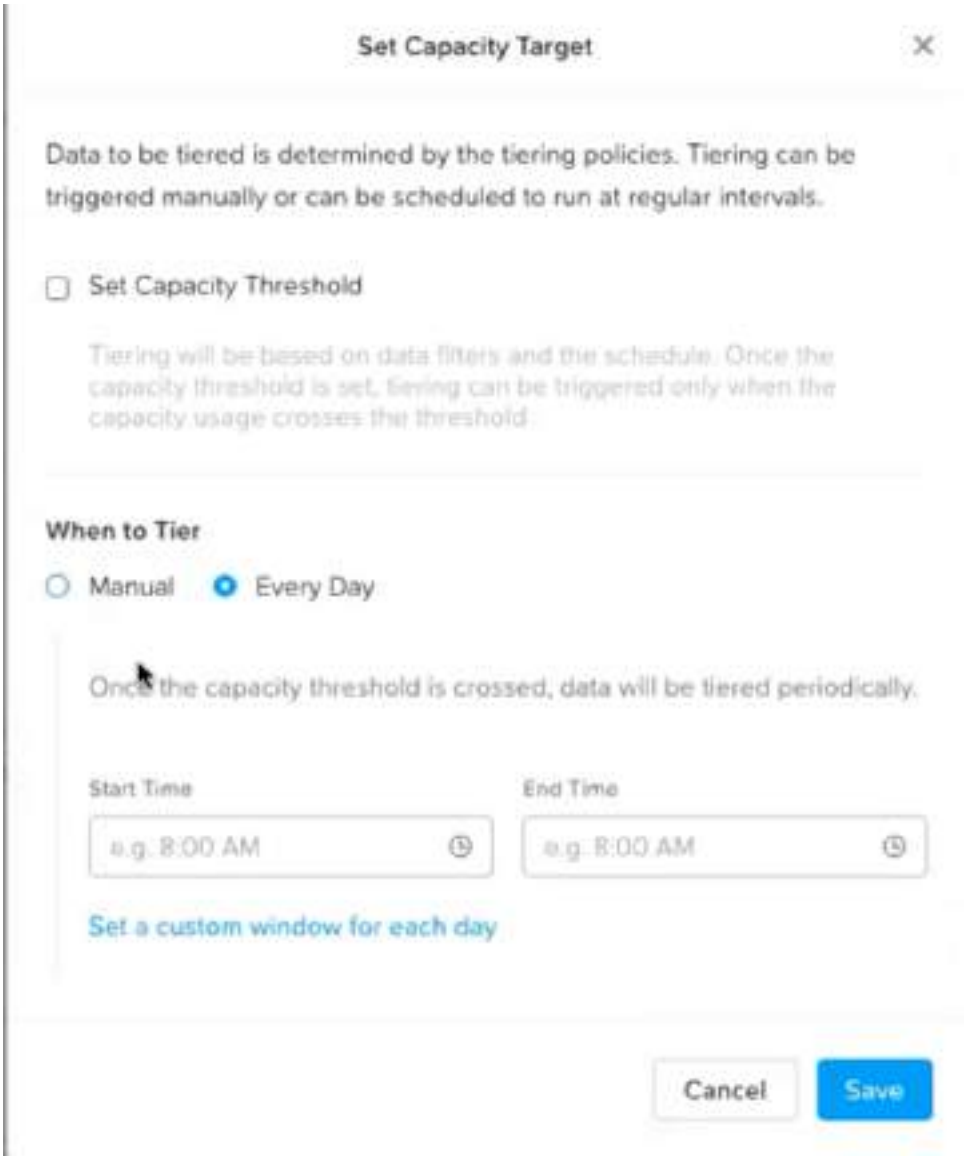


Figure 80: Set Capacity Target

Note: If you choose the **Manual** option, follow the steps in Tiering Data Manually on page 174 to initiate tiering after you observe that the file server reaches the configured capacity threshold.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 562

5. If you chose the **Every Day** option, do the following in the indicated fields (otherwise, continue to the next step).

   Note: The actual tiering operation on the file server can begin and end shortly after the scheduled time.

   - **Frequency**: Use the **Every Day** option and do the following (or click **set a custom window for each day**):
     - **Start time**: Specify when to start tiering operations.
     - **End time**: Specify when to end tiering operations.
   - (Optional) to customize the tiering schedule, click **set a custom window for each day**, and do the following:
     - Select the desired tiering days.
     - For each day, specify the schedule for tiering operations in the **start time** and **end time** fields.
6. Click **Save**.

Creating a Tiering Policy

Add a policy that defines when to tier cold data to object storage.

About this task

To create a tiering policy, do the following:

Procedure

1. In the Files Console, go to **Data Management** > **Smart Tiering**.
2. In the **Tiering Configuration** pane, under **Tiering Policy**, click **Create a Tiering Policy**.
3. Under **Filters for Data to be Tiered**, do the following:
   - **Access Time**:
     - Enter an integer to specify the data age.
     - In the dropdown, select the unit of measurement (days, weeks, months, years).
   - **File Size (greater than)**:
     - Enter an integer for the minimum tiering file size (minimum 64 KB).
     - In the dropdown, select the unit of measurement (KB, MB, GB).
4. (Optional) under **Shares**, to specify shares excluded from tiering, check the **Exclude Shares** box.
5. Click **Save**.
   If you set a schedule for the capacity threshold, file server automatically triggers the tiering operation in Nutanix Files according to the policy and threshold configuration. If you chose to manually trigger tiering, you must trigger the operation after the file server meets the criteria in the threshold and policy configuration.

Tiering Data Manually

If you have not selected to tier data on a schedule, initiate tiering manually.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 563

About this task

See Setting a Capacity Threshold on page 172 for details on configuring a manual tiering policy. Follow the steps as indicated to tier data manually.

Procedure

1. In the Files Console, go to **Data Management** > **Smart Tiering**.
2. Cick **Tier Data**.
   An unavailable **Tier Data** button indicates that file server has not found enough tiering candidates on the file server or that the file server has not reached the capacity threshold.
   A dialogue window asks you to confirm the action.

Updating a Tiering Configuration

Edit an existing tiering configuration.

About this task

Follow the steps as indicated.

Procedure

1. In the **Dashboard** for the file server, click **Smart Tiering** in the **Data Management** pane.
2. In the **Tiering Configuration** section, do one or more of the following.
   - To update the tiering profile configuration, click **Edit** under **Tiering Location**. Update one or more fields as described in Configuring a Tiering Location on page 170. You can only update the access key, secret key, profile name, or the certificate.
   - To update the capacity threshold, click **Edit** under **Capacity Threshold**. Update one or more fields as described in Setting a Capacity Threshold on page 172.
   - To update the tiering policy, click **Edit** under **Tiering Policy**. Update one or more fields as described in Creating a Tiering Policy on page 174

Recalling Tiered Data

Recall tiered data from an object store.

About this task

Follow the steps as indicated to recall tiered data.

Procedure

Use the corresponding command for the data type you wish to recall.

» Recall a tiered file.

```
nutanix@fsvm$ afs tiering.recall share_name file_paths=file_path
```

Replace `file_path` with a comma separated list of target file paths starting from the share root, and replace `share_name` with the name of the share.

> **Note:** You can use a maximum of 32 file paths a time.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 564

» Recall files using inodes.

```
nutanix@fsvm$ afs tiering.recall share_name inodes=inodes
```

Replace *inodes* with a comma separated list of target inodes, and replace *share_name* with the name of the share.

» Recall all files on a share.

```
nutanix@fsvm$ afs mscan.create_scan share_list=share_name receiver_type=RecallFiles
```

Replace *share_name* with a comma separated list of share names.

Self-Service Restore

Self-service restore (SSR) lets you restore a previous version of a file or share.

With SSR, Files takes snapshots of share data in intervals defined by a snapshot schedule. You can enable SSR during or after share creation as the feature is disabled by default.

Files takes snapshots of the stored cluster data at the share and file levels. Files allows client-side restoration at the file-level granularity and server-side restoration at the share-level granularity. Server side restoration is faster and takes approximately the same time irregardless of the share size or number of files.

Use the client to view and manage file-level snapshot data. You don't need administrator level permissions for file-level snapshot data retrieval.

Nutanix recommends scheduling snapshots in regular or frequent intervals to provide same-day protection against accidental deletions or corruption.

You can configure 24 hour (every hour), daily, weekly, and monthly snapshots schedules. By default, SSR takes a snapshot every hour, retains the most recent 24 snapshots, and deletes the oldest SSR snapshot after exceeding the retention count for the snapshot type.

The snapshot retention count corresponds to the retention period. For example, for daily snapshots, Files deletes the oldest snapshot and creates a new one every day.

Files supports share updates for both standard and distributed shares. To enable SSR during share creation, see Creating an SMB Share on page 77 or Creating an NFS Export on page 83. To enable SSR after share creation, see Enabling Self-Service Restore on page 177.

Share-Level Restore

You can restore share-level snapshots using the Files Console, see Restoring a Share on page 180.

Restoring a share takes the same amount of time irrespective of the amount of data. The share restore feature only restores the share data and not the complete metadata, like the state of share features and share permissions. For NFS shares, existing client mounts will see stale mount error and need to remount. After restoring a share, Files automatically re-enables snapshots

See information on share-level limitations below.

Table 32: Feature Parity

Share migration	You cannot restore shares on an incomplete or active migration plan.
Smart Sync	You cannot restore shares that are part of a Smart Sync policy.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 565

Smart DR	You cannot restore shares that are part of a Smart DR policy.
Tiering	In the event of unresponsive non-critical tiering operations, you will get an alert.

File-Level Restore

You can view removed or overwritten files and choose a snapshot from the history of the target file. For file-level snapshots, the primary protocol determines the method for restoring the data. For SMB, you can restore files through the system. For NFS, Files only provides read-access and you must manually restore the files by copying and pasting the file data. For more information, see Retrieving Files with Self-Service Restore (SSR) on page 180.

Limitations

Consider the following limitations before enabling SSR:

- SSR for SMB does not restore streams or attributes in directories.
- Files does not support SSR at the root of distributed shares or exports.
- Share-level restore limitations:
  - Restoring a share cancels metadata scan jobs.
  - Restoring a share is unsuccessful when a snapshot is in the database but not in the file system, which can occur during service disruptions or deletion of snapshots.
  - Share restore rollback doesn't re-enable paused features, for example Smart Tiering.
  - An alert might not appear for surpassing the maximum number of TLDs after share-restore SSR.
  - You can have a maximum of 2,000 sub-mounted shares under the restored share.

Enabling Self-Service Restore

Enable self-service restore on a share or export.

About this task

Follow the steps as indicated.

Procedure

1. In the Files Console, go to the **Shares & Exports** tab.
2. In the row for the target share, click **three dot menu** > **edit**.
3. In the **Update Share** window, click **Next** to go to the **General Settings** tab.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 566

4. For the **Enable Self Service Restore** box, do one of the following:

   » To enable self-service restore, check the box.

   » To disable self-service restore, clear the box.

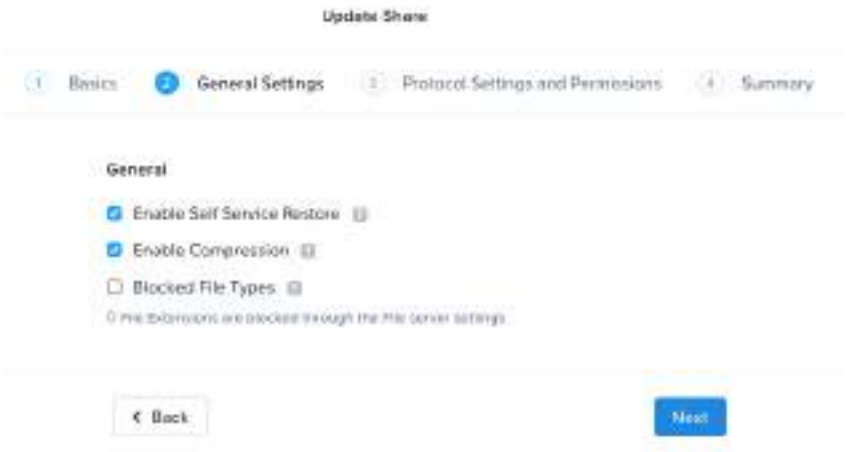


Figure 81: Enabled Self-Service Restore

5. Click **Next** > **Save**

What to do next

Add a snapshot schedule for SSR. See Adding Snapshot Schedules on page 178.

Adding Snapshot Schedules

Add file server protection by adding a snapshot schedule.

About this task

Use self-service restore (SSR) to create snapshot schedules to protect the file server. You can change the snapshot intervals but cannot change the specific time when Files takes the snapshot, except for hourly snapshots. Files takes snapshots at 00:00 UTC (midnight) for daily snapshots and at 0 minutes for hourly snapshots.

Before you begin

Ensure that the file server shares have SSR enabled.

> **Note:** The limit for configured snapshots is 50 or all schedule types.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 567

Procedure

1. In the **Files Console**, go to **Data Management** > **Protection** > **Self Service Restore**.
   The **Self Service Restore** window displays.

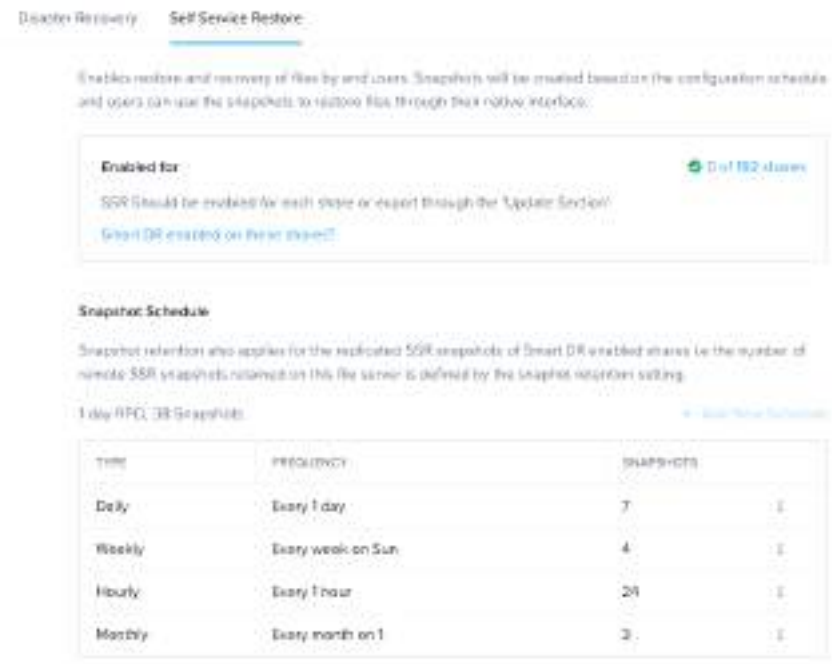


Figure 82: Self Service Restore Window

2. Click **+ Add New Schedule** and enter schedule details in the indicated fields.

   a. **Type**: Set the schedule interval. The snapshot types include hourly, daily, weekly, and monthly.

   > **Note:** You can only have one schedule type per file server. For example, a single file server cannot have two hourly schedules.

   The schedule does not have an end date by default and runs indefinitely unless you enter an end date.

   - If you select weekly, select boxes for the days of the week to run the schedule. Select the boxes in **Pick days of week**.
   - If you select monthly, enter one or more integers (in a comma-separated list) to indicate which days in the month to run the schedule. For example, to run the schedule on the 1st, 10th, and 20th days, enter "1,10,20".

   b. **Frequency**: Enter the number of snapshots within that type of schedule in the box. Enter the value in numerical format for minutes, hours, or days.
   The interval cannot be less than an hour, so the minutes' value must be at least 60.

   > **Note:** The frequency field only supports hourly and daily schedules.

   c. **Snapshots**: Enter the number of snapshots to retain for this schedule. Enter the value in numerical format.

3. Click the **blue checkmark icon** to add the schedule.
   The new schedule appears in the **Snapshot Schedule** table.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 568

4. To edit an existing snapshot schedule, click the **three dots menu** > **edit** icon.

   a. To delete an existing schedule, click the **three dots menu** > **delete**. Deleting schedules clears the snapshots based on the schedule type. For example, Files deletes hourly schedules every hour until complete. Delete a schedule only if you also want to delete existing snapshots from that schedule.

Retrieving Files with Self-Service Restore (SSR)

Retrieve SMB file snapshots using SSR.

About this task

Accessing file snapshots requires browsing the target directory on the client.

Do the following to retrieve SMB files.

Procedure

1. On the client, go to the target directory and look for **Previous Versions** as described in Microsoft documentation.

   Previous versions of files typically display in order of the date modified. Therefore, unmodified files do not appear. Previous versions of folders display every available snapshot.

   To see deleted files or directories, access a previous version of the parent folder and restore the file or directory.

2. Open and manage the previous versions according to the Microsoft documentation.

Retrieving NFS Files with SSR

About this task

Enabling SSR on NFS exports lets you access snapshot versions of a directory using a hidden .snapshot sub-directory. Browse the directory for the intended snapshot and restore it by manually copying the file or its content.

> **Note:** When the absolute path to the snapshot's directory is longer than 3922 characters, the attempt to browse into the snapshot can fail with a file name too long error message.

Procedure

Retrieve an NFS file with SSR.

1. Go to the snapshots of the target directory.

   ```
   $ cd /dir1/dir2/.snapshot
   ```

   Replace `/dir1/dir2` with the directory path

   > **Note:** You can only access the .snapshot directory using the cd command. The .snapshot directory is not visible otherwise. Using the `ls -a` command does not show the .snapshot directory.

2. List the snapshots for the target directory.

   ```
   $ ls
   ```

3. Browse the snapshots and copy the desired data.

Restoring a Share

Restore a share or an export from a snapshot.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 569

About this task

When you restore a share from a snapshot, Files deletes snapshots taken after the target snapshot. Disable the following features before you attempt to restore a share: Smart-DR, Smart Sync, share conversion, share migration. Follow the steps as indicated to restore a share from a snapshot.

Procedure

1. In the Files Console, go to the **Shares & Exports** tab.
2. In the row for the target share, click **three dot menu** > **Restore Share**.
   The **Select a Snapshot** window appears.
3. Select the target snapshot from the table.

   Note: This step is irreversible and deletes all newer snapshots.

4. Click **Restore**.
   The restore tasks begins and Files pauses new snapshots on the target until the operation ends. If the restore task completes but the post-restore task fails, use the following command `afs share.restore_commit share-name`.

What to do next

If you disabled any of the following features, re-enable them: Smart-DR, Smart Sync, share conversion, share migration.

Manually Restoring a Share

How to restore a share from a Nutanix Files or third-party snapshot.

Procedure

Restore a share from a snapshot on the client or using CLI.

```
$ afs share.restore_from_snapshot share-name snapshot-name
```

Replace *share-name* with the name of the share and replace *snapshot-name* with the name of the snapshot.

Deleting SSR Snapshots

Manually delete SSR snapshots to reclaim disk space.

About this task

By default, Files deletes the oldest SSR snapshot after exceeding the retention count for that snapshot type. To manually delete SSR snapshots, follow the steps as indicated.

Procedure

1. List the snapshots by creation time.

   ```
   nutanix@fsvm$ afs snapshot.list share_name=share_name
   ```

2. List the space occupied by a single snapshot or range.

   ```
   nutanix@fsvm$ afs snapshot.reclaimable_space uuid_start:uuid_end
   ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 570

3. Remove snapshots.

   » Remove a single snapshot using the universally unique identifier (UUID).

   > **Note:** You can delete multiple snapshots by specifying a comma-separated list of UUIDs.

   ```
   nutanix@fsvm$ afs snapshot.remove share_name=share_name
    snapshot_uuid_list=snapshot_uuid
   ```

   » Remove multiple snapshots using labels by defining the label. Labels define if the snapshot schedule is hourly, daily, weekly, or monthly. Deleting snapshots using labels deletes all snapshots for the specified label on the share.

   ```
   nutanix@fsvm$ afs snapshot.remove share_name=share_name label=label
   ```

Setting Custom Hourly Snapshot Times

Set a custom hour for self-service restore (SSR) snapshots.

About this task

To take hourly snapshots at a custom time, indicate the time by specifying the number of hours offset from midnight UTC.

Procedure

Set snapshot times.

```
nutanix@fsvm$ afs snapshot.set_ssr_hourly_offset 1 - 23
```

Replace `1 - 23` with an integer to specify the time offset from UTC. For example, if the offset is 9 and the frequency is 12 hours, Files takes hourly snapshots at 9 AM and 9 PM UTC, compared to the default of 12 AM and 12 PM UTC.

Share Migration

Share migration lets you copy data from a specified path on one share to another, including from third-party sources to Nutanix Files.

> **Note:** Files fully supports the migration of live shares. Nutanix recommends running the final or cut-over iteration on a static share.

Each time you initiate share migration, Files starts an iteration of the migration copy process. If some files fail to migrate, you can copy the failed files to the target using the migration retry procedure, see Re-attempt Share Migration on page 186. Files trims the forward slash (/) from the beginning and the end of the source path and migrates the content inside the path.

> **Note:** Once the number of failed files exceeds a threshold, the migration retry procedure cannot succeed, and you must run another iteration of the migration.

If the source share is not static and the data changes either during or after the migration, run another iteration to copy the changed data from the source to the target. If you run an iteration when the source and target shares are in sync, then Files shows zero copied entities (files, folders, streams). To ensure the migration of all data, run multiple iterations.

For more information about restoring target share access upon cancellation of a migration plan, see Troubleshooting on page 193.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 571

Note: You can also migrate shares using Move. Move provides a user interface for file migration. For more information, see Files Migration in the *Move User Guide*.

Supported Features

Share migration supports the following.

- Migrating and retaining symlinks to the target shares.
- Source shares with SMB encryption enabled.
- A mirroring option for the data between the source and the target. Files replicates any renames and deletes on the source to the target.

NFSv3 Export Migration

Meet the following requirements:

- Configure AUTH_SYS security on the source. On Linux-based servers, you can do this using the `sec=sys` export option.
- Disable root squashing on the server to allow the Files migrator to read and transfer all files. On Linux-based servers, use the `no_root_squash` export option.

Limitations

Files does not do the following for share migration:

- Migrate system access control lists (SACLs).
- Migrate directory junctions.
- Support multi-protocol on shares that already have long-name enabled.
- Support custom extended attributes (EA) on SMB shares. Therefore, all custom extended attributes present on the source files are ignored during migration.
- Support deduplication. You must disable deduplication during share migration.

Migrating Shares

Migrate share data from another share.

About this task

Follow the steps as indicated to migrate shares.

Procedure

1. Provide source file server details.

```
nutanix@fsvm$ afs migration.source_add source_alias=source_server_alias /
 source_fs_fqdn="source_server_IP_address_or_FQDN" source_user='domain\\user_name'
```

For NFS migration, source_user is not required.

For example:

```
nutanix@fsvm$ afs migration.source_add source_fs_fqdn="filer1.child4.afs.minerva.com"
 source_alias=filer1 source_user='CHILD4\\backup_user'
Password for user:
Registering source (filer1: filer1.child4.afs.minerva.com).
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 572

```
Source created.
```

> **Note:** The file server must be able to access the source user domain.

> **Note:** Do not add a destination file size.

Files asks you to provide the source user password.

2. If you have not already, create a target share using the Files user interface.
3. Check that Files registered the source.

```
nutanix@fsvm$ afs migration.source_list
```

For example:

```
nutanix@fsvm$ afs migration.source_list
+--------------+------------------------------+--------------------+------------
+----------+
| SOURCE ALIAS | SOURCE FQDN                  | SOURCE USER        | START TIME |
 END TIME |
+--------------+------------------------------+--------------------+------------
+----------+
| filer1       | filer1.child4.afs.minerva.com | CHILD4\backup_user | 0          | 0
       |
+--------------+------------------------------+--------------------+------------
+----------+
```

4. Create the migration plan.

```
nutanix@fsvm$ afs
 migration.plan_create name=plan_name source_alias=source_server_alias /
source_share=share/path target_share=target_share target_share_path=path/within/share
 /
plan_type=NFS|SMB
migrate=true|false
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 573

```
mirror=true|false
```

Setting the mirror option to `true` honors rename and delete operations. For consolidation to the same target share, set the mirror option to `false`.

Setting migrate option to `true` initiates the migration as soon as you create the plan.

Example 1: Migrate the source share to the target share.

```
nutanix@fsvm$ afs migration.plan_create name=plan1 source_alias=filer1
 source_share=share1 target_share=home plan_type=NFS migrate=false mirror=true
```

Example 2: Migrate a path on the source share to a target share.

```
nutanix@fsvm$ afs migration.plan_create name=plan1 source_alias=filer1
 source_share=share1/users target_share=home plan_type=NFS migrate=false mirror=true
```

Example 3: Migrate a path on the source share to a path on the target share.

```
nutanix@fsvm$ afs migration.plan_create name=plan1 source_alias=filer1
 source_share=share1/users/user1 target_share=home target_share_path=user1
 plan_type=SMB migrate=true mirror=true
```

> **Note:**
>
> - Share migration requires `target_share_path` when the target is a directory within the target share.

(optional) add more arguments.

```
json_output=         Render output in json format


total_bytes=         The total number of Bytes to be migrated.

total_files=         The total number of files to be migrated.
```

> **Tip:** Setting the total_bytes or total_files arguments lets Files display the progress of the migration.

5. Start the migration.

```
nutanix@fsvm$ afs migration.plan_migrate name=plan_name
```

For example:

```
nutanix@fsvm$ afs migration.plan_migrate name=plan1
```

> **Note:** Use the allow_unknown_sids= parameter if you have files or directories with local security identifiers (SIDs) on the source.

```

allow_unknown_sids=          Copy entities with an unknown owner or group SID.
                                When set to false, Files does not copy entities with
 an
                                unknown user or group SID.


                                false, Files fails the migration when the root of
 the
                                source share path has files.(For distributed shares
                                only.

ignore_long_tld_names=        Ignore TLD names with more than 255 bytes on source.
 If
                                set to false, Files fails migration when the name of
 a
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 574

```
                                TLD at the root of the source share is longer than
255
                                bytes long. (For distributed shares only.)
```

Note: You can rerun the migration multiple times after completion.

6. Check the status of the migration.
   Setting verbose to true provides extra migration status details for every FSVM on the file server.

```
nutanix@fsvm$ afs migration.plan_status name=plan_name verbose=true|false
```

Note: Checking the status of a migration plan returns a granular status view of all nodes on the file server. For any node excluded from the migration plan, Files reports a succeeded status.

7. (optional) Use one or more of the following commands as needed.

```
migration.plan_summary                  Display a summary of each iteration of the
 plan.
migration.plan_pause                    Pause the migration.
migration.plan_resume                   Resume the migration.
migration.plan_cancel                   Cancel the migration.
migration.source_update                 Update the source.
migration.source_delete                 Delete the source.
migration.source_list                   List configured sources.
migration.plan_update                             Update the migration plan.
```

Re-attempt Share Migration

Retry share migration for files that failed to migrate.

About this task

Before retrying share migration for failed files, Nutanix recommends running the share migration operation multiple times to ensure the migration of all source data.

Follow the steps as indicated.

Procedure

1. (optional) Get a list of files that failed to migrate in the last iteration of the plan.

```
nutanix@fsvm$ afs migration.plan_get_failed_files_list name=plan_name /
out_file=output_directory_path [iter_index=-1]
```

2. Retry the migration for the files that failed to migrate in the last iteration of the plan.

```
nutanix@fsvm$ afs migration.plan_retry_failed_files name=plan_name
```

Configuring Backup for Distributed Shares

Specify a backup server for distributed shares and exports.

About this task

Third-party solutions do not automatically back up distributed shares. Follow the steps as indicated to update the backup configuration syntax and allow the backup of distributed shares and exports.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 575

Procedure

1. Check the global backup configuration.

   ```
   nutanix@fsvm$ afs smb.get_conf "backup hosts"
   ```

2. Update the backup configuration.

   » Add a backup server by replacing *backup-server-ip* with the IP address for the backup server. For multiple backup servers, enter a comma separated list of the *backup-server-ip*.

   ```
   nutanix@fsvm$ afs smb.set_conf "backup hosts" backup-server-ip section=global
   ```

   » Remove a backup server.

   ```
   nutanix@fsvm$ afs smb.del_conf "backup hosts" section=global
   ```

3. Validate changes to the backup configuration.

   ```
   nutanix@fsvm$ afs smb.get_conf "backup hosts"
   ```

High Availability

Fail over for file server VMs (FSVMs).

High Availability (HA) for Files ensures that, during a service disruption, a file server VM (FSVM) on clusters of two or more FSVMs can fail over to another FSVM. All clusters of two or more FSVMs have a HA enabled by default.

When an FSVM experiences an issue, Files reassigns the IP address of the FSVM to another FSVM in the cluster. The IP address of the out-of-service FSVM remains available. However, the shares and exports on the impacted FSVM are unavailable for several minutes during a failover. For NFS, it takes 30 seconds to be able to read files again but around 2 minutes to gain write access due to the NFS grace period.

Affinity rules do not affect HA; multiple FSVMs can share a single host during a HA event.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 576

SECURITY HARDENING

Use the Nutanix command-line interface (nCLI) or Files CLI to customize your Files security configuration.

Table 33: General Files Hardening Configuration

Description	Command or settings
Support file server configuration of the SCMA policy.	`ncli file-server get-security-config fs-name=`*`file-server-name`*
Schedule weekly execution of advanced intrusion detection environment (AIDE)	`ncli file-server edit-security-params fs-name=`*`file-server-name`* `enable-aide=true`
Enable the strong password policy.	`cli file-server edit-security-params fs-name=`*`file-server-name`* `enable-high-strength-password=true`
Enable the Department of Defense knowledge consent banner of the US department.	`ncli file-server edit-security-params fs-name=`*`file-server-name`* `enable-banner=true`
Change the default schedule of running the SCMA. The schedule can be hourly, daily, weekly, and monthly.	`ncli file-server edit-security-params fs-name=`*`file-server-name`* `schedule=hourly`
Disable the core-dump settings to let the file server VM generate stack traces for any cluster issue. **Note:** On a file server, this parameter turns both the `core` and the `kerneldump` salt status on or off.	`ncli file-server edit-security-params fs-name=`*`file-server-name`* `enable-core=false`

When a high governance official must run the hardened configuration.	Have the following settings.
	`Enable Aide : true`
	`Enable Core : false`
	`Enable High Strength Password : true`
	`Enable Banner : false`
	`Schedule : HOURLY`

When a federal official must run the hardened configuration.	Have the following settings.
	`Enable Aide : true`
	`Enable Core : false`
	`Enable High Strength Password : true`
	`Enable Banner : true`
	`Schedule : HOURLY`

Back up the DoD banner file.	Run the following command, and repeat on all FSVMs. `nutanix@FSVM$ sudo cp -a /srv/salt/security/AFS/sshd/DODbanner /srv/salt/security/AFS/sshd/DODbannerbak`

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 577

Description	Command or settings
Modify DoD banner file.	Run the following command, and repeat on all FSVMs. `nutanix@FSVM$ sudo vi /srv/salt/security/AFS/sshd/DODbanner`

Create a separate mount for audit logs on new file servers.	`nutanix@cvm$ allssh 'echo "--audit_logs_separate_fs=true" >> ~/config/minerva_cvm.gflags'`
	`nutanix@cvm$ allssh 'genesis stop minerva_cvm'`
	`nutanix@cvm$ cluster start`

Manage sudo authentication settings.	**Note:** Running the commands from a single FSVM applies the changes to all FSVMs on the cluster.
	Enable sudo authentication settings.
	`nutanix@fsvm$ afs infra.set_sudo_auth state=on`
	Disable sudo authentication settings before performing Files upgrades, expanding a files cluster, and before using the following commands: genesis restart, genesis stop, cluster stop, and cluster restart_genesis.
	Disable sudo authentication settings.
	`nutanix@fsvm$ afs infra.set_sudo_auth state=off`
	After performing file server activate, clone, or migrate operations, re-enable sudo authentication.
	`nutanix@fsvm$ afs infra.set_sudo_auth state=on`

Enable SMB signing.	Run the following command on any FSVM in the cluster. `nutanix@fsvm$ afs smb.set_conf "server signing" "mandatory" section=global`

Secure Sockets Layer (SSL) Certificate Settings

Files supports installing a self-signed or custom SSL certificate for certificate-based authentication. For file servers, these operations are only available through the nCLI and afs-CLI commands.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 578

Table 34: SSL Certificate Settings on a File Servers

Description	Command or Settings
Generate a new self-signed SSL certificate.	Run the following command. **Note:** Replace *fs_uuid* with the universally unique identifier of the file server. `nutanix@CVM$ ncli file-server ssl-certificate-generate uuid=fs_uuid`
Replace the existing self-signed SSL certificate with a new one.	Run the following command. `nutanix@CVM$ ncli file-server ssl-certificate-change-pfx-file-password uuid=fs_uuid`
Get the current SSL certificate.	Run the following command. `nutanix@CVM$ file-server get-ssl-certificate`
Apply a custom SSL certificate on an FSVM.	Run the following command. • Replace *ca-path* with the CA certificate or chain file path. • Replace *cert-path* with the SSL certificate file path. • Replace *key-path* with the private key path. • Replace *value* with the type of private key (ECDSA_256, ECDSA_384, ECDSA_521, RSA_2048). `nutanix@FSVM$ afs misc.import_ssl ca_chain_file=ca_path cert_file=cert-path key_file=key-path key_type=value`

Quality of Service (QoS) Setup

The table following details QoS setup on a file server using differentiate services code point (DSCP) values.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 579

Table 35: QoS Settings

Description	Command or settings
Enable QoS. **Note:** The default management traffic value is 16, and the default data traffic value is 10.	`nutanix@FSVM$ afs net.enable_qos [management_dscp_value=value] [data_dscp_value=value]`
Get the currently configured DSCP values.	`nutanix@FSVM$ afs net.get_qos`
Modify the DSCP value of one or more traffic types.	`nutanix@FSVM$ afs net.edit_qos [management_dscp_value=value] [data_dscp_value=value]`
Disable QoS on all traffic types and delete the existing configuration.	`nutanix@FSVM$ afs net.disable_qos`

Rsyslog

The table following provides details on rsyslog daemon configuration for log forwarding.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 580

Table 36: Rsyslog

Description	Command or settings
Add a rsyslog server.	`nutanix@FSVM$ afs rsyslog.add_server server_name=server_name ip_address=server_ip port=server_port network_protocol=TCP/UDP relp_enabled=true/false`
Modify the properties of the rsyslog server.	`nutanix@FSVM$ afs rsyslog.update_server server_name=configured_server_name ip_address=server_ip port=server_port network_protocol=TCP/UDP relp_enabled=true/false`
Remove the configured rsyslog server.	`nutanix@FSVM$ afs rsyslog.remove_server server_name=configured_server_name`
Add forwarded modules and their debug-level to the rsyslog server. **Note:** Files only supports the syslog module.	`nutanix@FSVM$ afs rsyslog.add_server_module server_name=configured_server_name module_name=SYSLOG_MODULE level=ALERT/ CRITICAL/ DEBUG/ EMERGENCY/ ERROR/ INFO/ NOTICE/ WARNING`
Remove the module and forwarding level form the rsyslog server.	`nutanix@FSVM$ afs rsyslog.remove_server_module server_name=configured_server_name module_name=SYSLOG_MODULE`
Set the status for rsyslog forwarding. (You can disable rsyslog forwarding completely without removing the configured server details.) **Note:** Setting the `false` status ends forwarding and removes the configuration.	`nutanix@FSVM$ afs rsyslog.set_status enable=true/false`
Get the status of rsyslog forwarding.	`nutanix@FSVM$ afs rsyslog.get_status`
Get the current rsyslog configuration.	`nutanix@FSVM$ afs rsyslog.list`
Get the configured modules and their forwarding level for a configured rsyslog server.	`nutanix@FSVM$ afs rsyslog.list_modules server_name=server_name`
Set up transport layer security (TLS) parameters of the rsyslog server. **Note:** Not setting the auth-mode to *anon*, requires specifying permitted peers in a comma-separated list.	`nutanix@FSVM$ afs rsyslog.set_tls auth_mode=anon, x509/certvalid, x509/ fingerprint, x509/name ca_chain_path=PEM_encoded_CA_certificate_file_absolut permitted_peers=permitted_peers`
Get the configured TLS parameters.	`nutanix@FSVM$ afs rsyslog.get_tls`
Disable all configured TLS parameters, and disable TLS on forwarded packets.	`nutanix@FSVM$ afs rsyslog.disable_tls`

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 581

TROUBLESHOOTING

Disable distributed file system (DFS) support on a witness share

You are unable to use a Nutanix Files witness share with Windows 2019 Failover Cluster Services.

DFS is enabled by default on the witness share.

Procedure

1. **Note:** This is remedy is only possible for standard shares.

   Disable DFS on the witness share.

   ```
   nutanix@fsvm$ afs share.dfs share-name disable
   ```

2. Get the fully-qualified domain name (FQDN) of the FSVM hosting the share.

   ```
   nutanix@fsvm$ afs share.owner_fsvm share-name
   ```

3. Use the FQDN of the specific FSVM hosting the share (not the file server) for the witness share.

Invalid Mounts After Authentication Change

Clients cannot mount share.

Changes to the authentication method.

Procedure

Remount the authentication type as a value for parameter sec.

```
host$ -o sec=authentication-type
```

For example, use `-o sec=krb5` for Kerberos 5.

Client Access Denial (NFS Protocol)

Linux client experiences a "permission denied" error while accessing NFS shares.

A user management (authentication) change on an existing file server.

Procedure

This problem might be fixed by restarting the RPC-GSSAPI service on the clients. For example, enter the following command on a Linux CentOS 6 client:

```
nutanix@fsvm$ sudo service rpcgssd restart
```

The command syntax to restart the RPC-GSSAPI service varies among different Linux versions.

Clients Cannot Mount Shares

Clients in the same subnet as the Controller VM or in the storage network of the file server cannot mount the shares of the file server.

The file server was configured with two separate networks for the client-side and storage-side networks.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 582

Procedure

To allow clients in the same subnet as the Controller VM or storage network to mount shares, configure the file server with the same network for both the client-side and storage-side networks.

Client Side Network Mapping

The file server client network does not map to a site on the AD and does not specify the client side.

The file server's client network does not map to any site on the AD. Files cannot find the local domain controllers in a multi-site AD environment and uses a geographically remote DC, which, can result in delayed domain operations.

Procedure

1. In a multi-site environment, map the Files client network to a local site in the AD.
2. In a single-site environment or with only a single geographic location, ignore the warning.

Connecting to Authentication Services

The file server cannot connect with the AD server or it cannot contact the LDAP server for the given domain.

The file server cannot reach the given domain name with the specified DNS server list. Possible reasons include spelling mistakes in the domain name, incorrect DNS name servers, or connectivity issues with the domain controller servers.

Procedure

1. Check the DNS server addresses, domain name, and status of the domain controllers.
2. Verify the DNS entries for the given domain name.

Constraint Violation

Domain controller reused an operation due to a possible constraint violation.

- Incorrect SPN configuration.
- An SPN is not unique in the forest and the conflict results in failure.

Procedure

1. Ensure that Files related SPN entries are not present in the forest.
2. Ensure that the domain controllers do not have any replication issues.

Disable Directory Leasing on Snapshot

Open file and directory handles caused by directory leasing prevent snapshot deletion.

Procedure

1. Display the directory leasing configuration for a share.

```
nutanix@fsvm$ afs smb.get_conf "directory leasing disabled on snapshot"
 section=share_name
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 583

2. Disable directory leasing and reset the default configuration.

```
nutanix@fsvm$ afs smb.del_conf "directory leasing disabled on snapshot" section=share_name
```

Note: Use the following command to re-enable directory leasing when needed.

```
nutanix@fsvm$ afs smb.set_conf "directory leasing disabled on snapshot" "yes"
 section=share_name
```

DNS Missing SRV Records

SRV records not found on the specified DNS servers.

The specified DNS servers do not resolve the SRV records with the appropriate domain controller names.

Procedure

Add the domain controller SRV records for the required protocols and services.

Domain Controller Issues

Cannot find a writable and reachable domain controller.

Files cannot discover an active non-RODC (writable) LDAP domain controller (at the site or domain level).

Procedure

Ensure that one writeable domain controller is working in the given domain.

Finding IP Addresses

Fetch the IP addresses for all FSVMs.

Various causes.

Procedure

Enter the following command from any FSVM: nutanix@fsvm$ afs misc.fsvmips
Output lists the IP addresses for the FSVMs in the node.

Identifying the Share Owner

Identify the owner of a share or export.

The Files UI does not list the name of share and export owners.

Procedure

Perform one of the following commands to identify the share owner.

» List the share owners of a standard share or export.

```
nutanix@fsvm$ afs share.owner_fsvm share-name
```

» List the share owners of a distributed share or export by specifying the *share-name* and the *share-path*(including the name of the top-level directory TLD).

```
nutanix@fsvm$ afs share.owner_fsvm share-name path=share-path
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 584

Invalid Credential

Invalid user name or password.

Files cannot authenticate on the AD using the given user name and password combinations.

Procedure

1. Ensure that the user name and password are correct.
2. Verify that the user is not expired, locked, or disabled.

NLM Locks

Unable to get Network Lock Manager (NLM) locks from Mac client.

NLM recovery does not work over the User Datagram Protocol (UDP). Use the transmission Control Protocol (TCP) instead.

Procedure

1. Add the following lines to the /etc/nfs.conf file:

```
nfs.lockd.send_using_tcp = 1
nfs.statd.send_using_tcp = 1
```

2. Restart services.

```
user@host$ launchctl stop com.apple.lockd ; launchctl start com.apple.lockd
```

```
 user@host$ launchctl stop com.apple.statd ; launchctl start com.apple.statd
```

Network Cannot Expand

You changed the network ID and the file server cannot expand.

Update the UUIDs.

Procedure

1. Log into the CVM.
2. To update the file server network, enter the following:

```
nutanix@cvm$ afs infra.update_file_server_network
```

3. To update a specific file server within the network, enter the following:

```
nutanix@cvm$ afs infra.update_file_server_network fs_name
```

NFS Cache Expiry During Share Migration

You get the following job error while migrating a primary or secondary NFS share: LeaderJobWorkFlow: NFS cache expiry time was reduced during migration. Unable to reset that to default value. Please refer migration doc for same.

Running the command to reset NFS cache expiry time.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 585

Procedure

Update the NFS cache configuration.

```
nutanix@fsvm$ afs nfs.remove_config_param block=EXPORT export_name=target_export_name \
 param=Attr_Expiration_Time restart=False
```

Replace *target_export_name* with the name of the target export.

Restore Target Share Access Upon Canceling Migration Plan

Target share is in *Read Only* state.

Migration Plans which were cancelled leave the target share in Read Only state.

Procedure

1. Trigger another iteration of migration on a cancelled plan to restore the write access on the target share once the iteration is completed.
2. Or you can restore *Write* access on the share without having to run another iteration of migration.

   ```
   nutanix@fsvm$ afs share.client_blocking_filter share name delete Read-only ip_list=*
    vendor_name=kMigration
   ```

   For example, if the target share name is `share1`.

   ```
   nutanix@fsvm$ afs share.client_blocking_filter share1 delete Read-only ip_list=*
    vendor_name=kMigration
   ```

NTLM Authentication Issues

Authentication might be unsuccessful for NTLM when contacting read-only domain controllers (RODC).

The list of allowed password replication must include the machine account name or file server name. To resolve, follow troubleshooting steps on a domain controller.

Procedure

1. Add the host name.

   ```
   C:\>repadmin /prp add RODC_host_name allow machine_account_DN
   ```

2. View the list of added names.

   ```
   C:\>repadmin /prp view RODC_host_name allow
   ```

   For example, viewing the list of added names would appear similar to the following:

   ```
   C:\>repadmin /prp view MINDC03 allow
   ```

   Output looks similar to the following:

   ```
   Allow list (msDS-RevealOnDemandGroup):
   RODC "CN=MINDC03,OU=Domain Controllers,DC=automation,DC=nutanix,DC=com":
   CN=MNRVATST124803,CN=Computers,DC=automation,DC=nutanix,DC=com
   CN=Allowed RODC Password Replication Group,CN=Users,DC=automation,DC=nutanix,DC=
   com
   ```

Share Copying

Copy operation interrupted while using Microsoft robocopy to copy large files to Files shares.

Various causes (for example network bandwidth issues).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 586

Procedure

Use robocopy with the `/z` option. This option resumes any interrupted copy operation.

Stale Statistics

Windows client experiences stale statistics.

Default cache entry time is approximately 5 minutes.

Procedure

To change the default cache entry time of 5 minutes, log into the FSVM and run the following :

```
nutanix@fsvm$ afs smb.set_conf “stats cache ttl” “value” section=global
```

Time Difference

A time difference exists between Files and the domain controller.

Files uses Kerberos protocol for authentication on the AD. Kerberos is a time sensitive protocol and cannot sync the correct time when the client and servers are out of sync for several minutes.

Procedure

Use the same NTP server for the domain controller and Files.

Unsuccessful Authentication

Authentication might be unsuccessful for the NT LAN manager (NTL when contacting read-only domain controllers (RODC).

The list of allowed password replication must include the machine account name or file server name. To resolve, follow troubleshooting steps on a domain controller.

Procedure

1. Add the host name.

   ```
   C:\>repadmin /prp add RODC_host_name allow machine_account_DN
   ```

2. View the list of added names.

   ```
   C:\>repadmin /prp view RODC_host_name allow
   ```

   For example, viewing the list of added names would appear similar to the following:

   ```
   C:\>repadmin /prp view MINDC03 allow
   ```

   Output looks similar to the following:

   ```
   Allow list (msDS-RevealOnDemandGroup):
   RODC "CN=MINDC03,OU=Domain Controllers,DC=automation,DC=nutanix,DC=com":
   CN=MNRVATST124803,CN=Computers,DC=automation,DC=nutanix,DC=com
   CN=Allowed RODC Password Replication Group,CN=Users,DC=automation,DC=nutanix,DC=
   com
   ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 587

COPYRIGHT

Copyright 2024 Nutanix, Inc.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Nutanix and the Nutanix logo are registered trademarks of Nutanix, Inc. in the United States and/or other jurisdictions. All other brand and product names mentioned herein are for identification purposes only and may be trademarks of their respective holders.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 588

v9.2 | October 2024 | TN-2041

SOLUTIONS DOCUMENT

Nutanix Files

NUTANIX

Legal

© 2024 Nutanix, Inc. All rights reserved. Nutanix, the Enterprise Cloud Platform, the Nutanix logo and the other Nutanix products, features, and/or programs mentioned herein are registered trademarks or trademarks of Nutanix, Inc. in the United States and other countries. All other brand and product names mentioned herein are for identification purposes only and are the property of their respective holder(s), and Nutanix may not be associated with, or sponsored or endorsed by such holder(s). This document is provided for informational purposes only and is presented "as is" with no warranties of any kind, whether implied, statutory or otherwise.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

Contents

1. Executive Summary..... 5

2. Nutanix Files Architecture..... 8

File Server Virtual Machines..... 8
Exports and Shares..... 15
Load Balancing and Scaling..... 24
High Availability..... 26
Active Directory and SMB Operations..... 30
Active Directory, LDAP, and NFS Operations..... 36
Multiprotocol..... 38
Quotas..... 41
Selective File Blocking..... 42
Files Manager..... 42
Role-Based Access Control..... 43
File Analytics..... 43
Nutanix Data Lens..... 47
Smart Tier..... 47
Data Lens Advanced Ransomware Protection..... 50
Hypervisor-Specific Support..... 51

3. Backup and Disaster Recovery..... 52

Self-Service Restore..... 52
Asynchronous Protection Domains and Consistency Groups..... 53
Cluster Migration, Failure, and Restoration..... 53
Cloning..... 54
Metro Availability..... 55
Files Smart Disaster Recovery..... 56
Data Synchronization..... 59

4. Third-Party Integration..... 61

Antivirus..... 61
File Operations Monitoring..... 63
Intelligent Backup..... 64

5. Conclusion..... 67

About Nutanix.....68

List of Figures.....69

1. Executive Summary

Nutanix Files is a software-defined, scale-out file storage solution that provides a repository for unstructured data, such as home directories, user profiles, departmental shares, application logs, backups, and archives. Flexible and responsive to workload requirements, Files is a fully integrated, core component of Nutanix.

You can deploy Nutanix Files on an existing or standalone cluster. Unlike standalone NAS appliances, Files consolidates VM and file storage, eliminating the need to create an infrastructure silo. Administrators can manage Files with Nutanix Prism, just like VM services, which unifies and simplifies management. Integration with Active Directory enables support for quotas and access-based enumeration (ABE), as well as self-service restores with the Windows previous version feature. Nutanix Files also supports native remote replication and file server cloning, which lets you back up Files off-site and run antivirus scans and machine learning without affecting production.

Nutanix Files can run on a dedicated cluster or be collocated on a cluster running user VMs. You can deploy Nutanix Files in the public cloud with Nutanix Cloud Clusters (NC2) in Microsoft Azure or Amazon Web Services (AWS). Through a tech preview with the Files 5.0 release, you can run Files in AWS using native services and decoupled from NC2.

Nutanix Files is hypervisor agnostic and supports both ESXi and AHV. It includes native high availability and uses Nutanix storage for intracluster data resilience. Nutanix storage also provides data efficiency techniques such as erasure coding (EC-X).

Nutanix Files includes File Analytics, which gives you a variety of useful insights into your data, including full audit trails, anomaly detection, file blocking–based ransomware protection, data age analytics, and custom reporting. You can also use Nutanix Data Lens to provide deeper insights and more robust ransomware protection for your Nutanix Files environment. Data Lens provides analytics, permissions monitoring, and ransomware defense at scale for Nutanix Unified Storage.

This tech note is part of the Nutanix Solutions Library. We wrote it for architects and systems engineers who want to use Nutanix Files to deliver user and group file

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 593

management. This document describes how to implement and operate Files in your datacenter.

We cover the following subject areas:

- Overview of the Nutanix architecture with Files
- Load balancing of standard and distributed shares (SMB) and exports (NFS)
- High availability
- Backup and recovery
- Quotas and permission management
- Antivirus

Table: Document Version History

Version Number	Published	Notes
1.0	December 2016	Original publication.
1.1	May 2017	Updated Backup and Disaster Recovery section.
1.2	September 2017	Updated for version 2.2 features.
2.0	February 2018	Updated for version 3.0.
2.1	April 2018	Solution overview update.
2.2	August 2018	SMB share and NFS export updates.
3.0	October 2018	Updated for version 3.1 and updated product naming.
4.0	January 2019	Updated for version 3.2 and AOS 5.9 and later.
5.0	April 2019	Updated for version 3.5 and AOS 5.10 and later.
5.1	August 2019	Updated for version 3.5.1.
5.2	October 2019	Updated for version 3.6.
5.3	October 2020	Updated for version 3.7.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 594

Version Number	Published	Notes
6.0	April 2021	Updated for Files 3.8, File Analytics 3.0, and Files Manager 2.0.
7.0	October 2021	Updated for Files 4.0 and Data Lens. Added Smart Tier and SSR Interoperability sections. Updated Shares and Exports, Notifications, Selective File Block, and Files Operations Monitoring sections. Updated Files Smart DR figure.
7.1	June 2022	Updated for Files 4.1 and Data Lens.
7.2	January 2023	Updated for Files 4.2 and Data Lens.
8.0	November 2023	Updated for Files 4.3, 4.4, and Data Lens.
8.1	December 2023	Updated the Volume Group and Storage Container Architecture section.
9.0	August 2024	Updated for Files 5.0.
9.1	September 2024	Updated erasure coding guidance in the Volume Group and Storage Container Architecture section.
9.2	October 2024	Updated the SMB Signing section.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 595

2. Nutanix Files Architecture

Nutanix Files is a scale-out approach that provides Server Message Block (SMB) and Network File System (NFS) file services to clients. Nutanix Files instances are composed of a set of file server VMs (FSVMs). Files requires at least three FSVMs running on three nodes to satisfy a quorum for high availability.

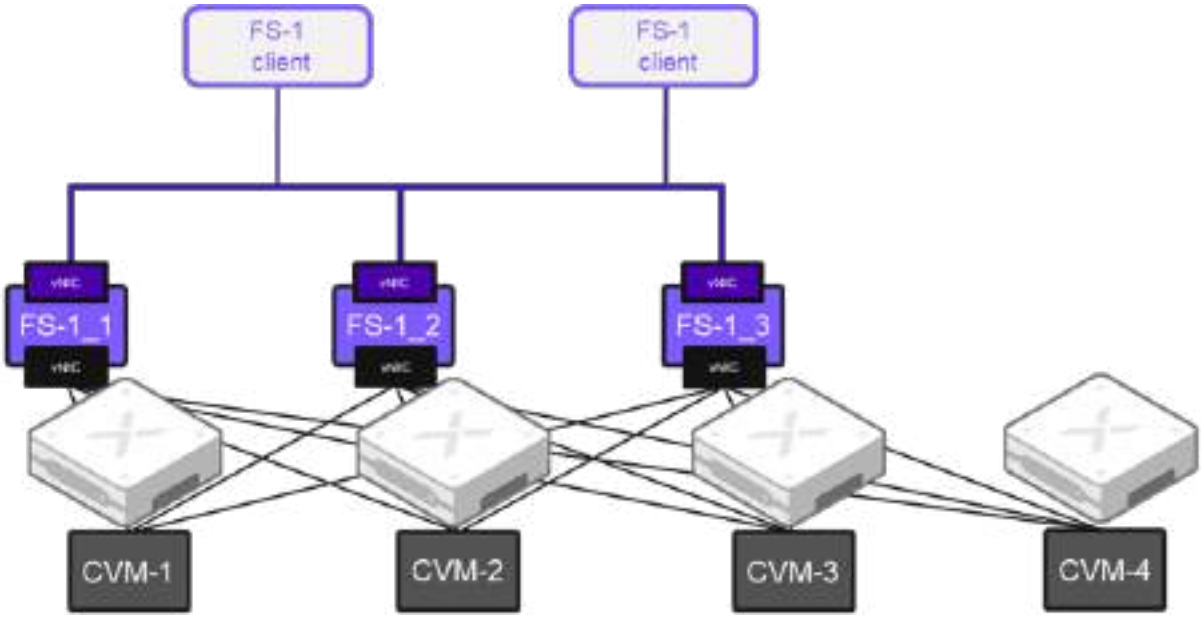


Figure 1: Nutanix Files Instances Run as VMs

File Server Virtual Machines

The file server VM (FSVM) incorporates all the security and hardening that goes into the Nutanix Controller VM (CVM). All the FSVMs have the same basic configuration: 4 vCPU and 12 GB of memory. You can add more vCPU, memory, and FSVMs to the cluster. For each file server the number of FSVMs must be less than or equal to the number of nodes in the Nutanix cluster; however, you can create multiple file server deployments if needed. Starting with Nutanix Files 5.0, each Files cluster can support up to 32 FSVMs.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 596

Single-FSVM deployments intended for one- and two-node Nutanix clusters are also supported and can be used in larger clusters.

Nutanix Files supports SMB and NFS from the same file server. Nutanix Files further enables simultaneous SMB and NFS access to the same share and data, commonly referred to as multiprotocol support. Both SMB and NFS share a common library, allowing a modular approach. InsightsDB is a NoSQL database that maintains the statistics and alerts for Nutanix Files. Zookeeper is a centralized service that maintains configuration information, such as domain, share or export, and IP information. The Minerva NVM Service talks to the local CVM and sends heartbeats to share health information and help with failover. The following figure maps the connections between all of these services.

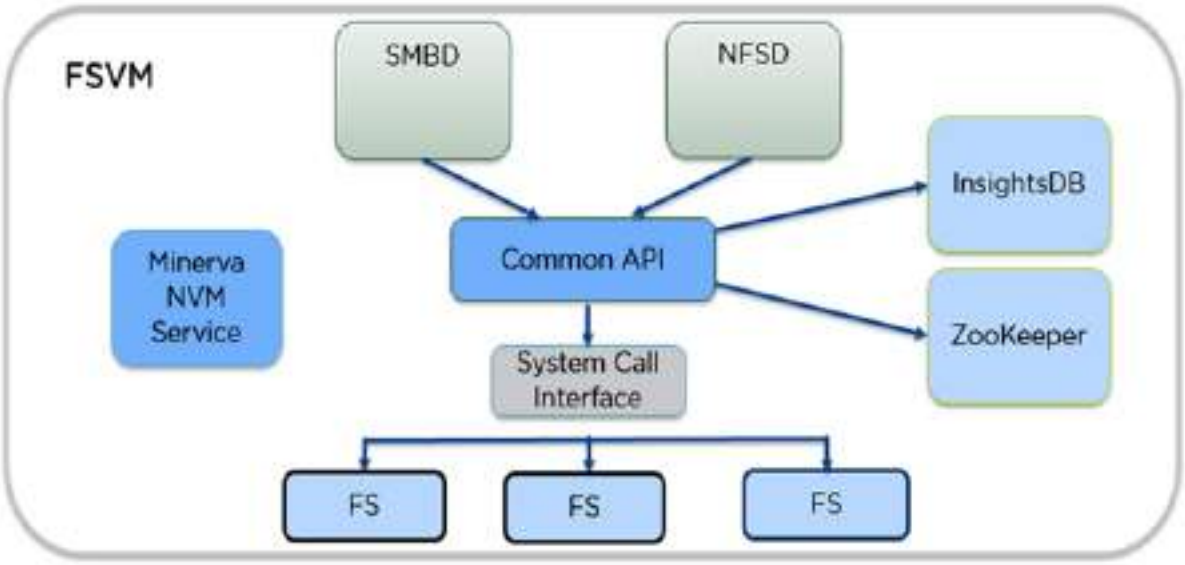


Figure 2: Data Path Architecture of Nutanix Files

Each FSVM stores file server data on multiple file systems that store share-specific data. The individual file system offers the snapshot capability to provide the Windows previous version feature to clients. By using separate file systems for each share or export, Nutanix Files can scale to support billions of files in one cluster.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 597

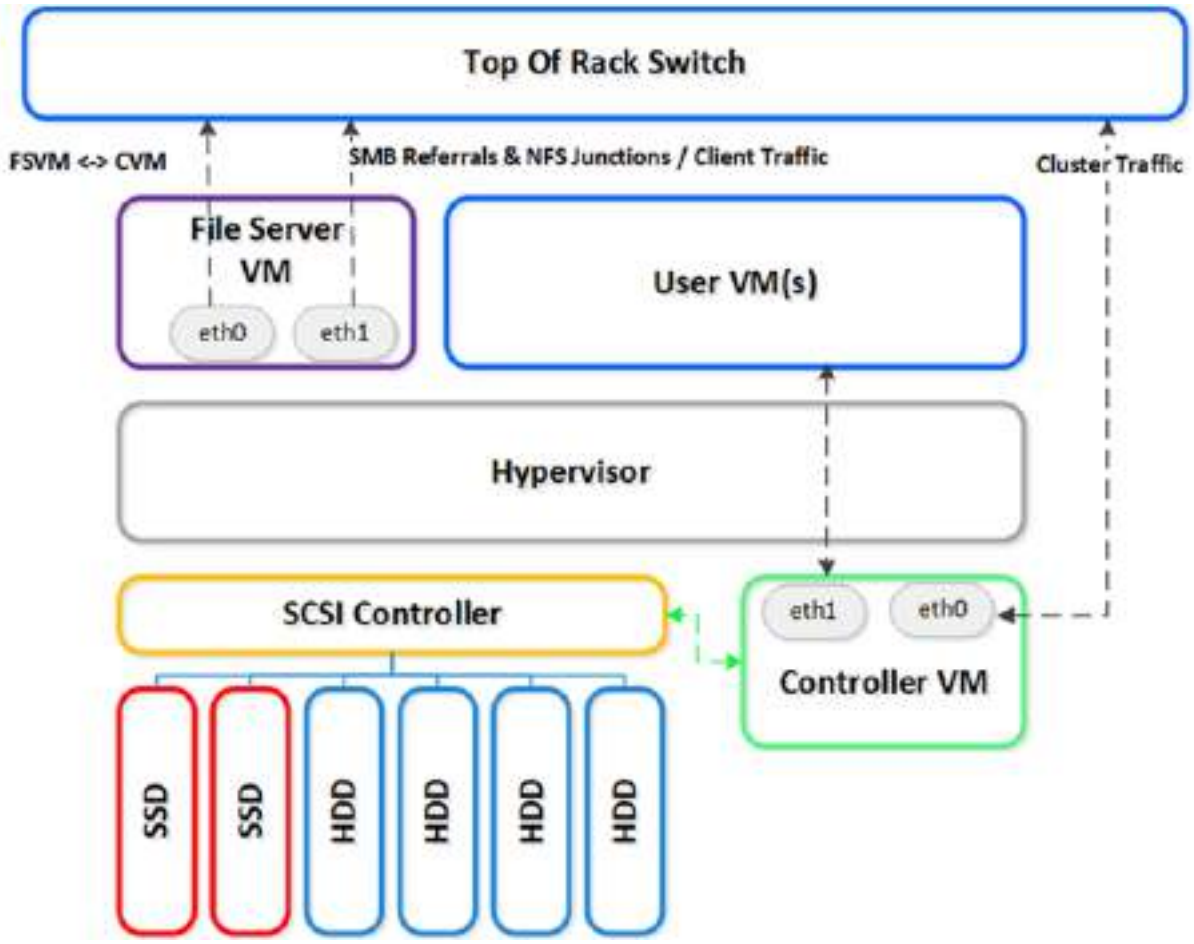


Figure 3: FSVM Internal Communication on One Node

The previous diagram shows one FSVM running on a node, but you can put multiple FSVMs on a node for multitenancy.

Networking

The FSVM has two network interfaces: the storage interface and the client interface. The FSVM service that talks to the CVMs uses the storage interface, which also provides access to Nutanix Volumes iSCSI vDisks in volume groups. The storage interface helps manage deployment, failover, and maintenance and enables control over one-click upgrades. Integration with the CVM lets the FSVM determine if a storage fault occurred and, if so, whether you must take action. The FSVM service sends a heartbeat to its local CVM service each second, indicating its state.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 598

We recommend that you place the FSVM storage interface on the same network VLAN as the Nutanix CVM iSCSI network to ensure maximum performance. By default, the iSCSI VLAN is the management interface (eth0 of the CVM). Optionally, you can create a segmented iSCSI network for isolation purposes.

The client interface allows clients to connect to SMB shares and NFS exports hosted on an FSVM. A client can connect to any FSVM client network interface to access file data. If a different FSVM provides the data, the client connection automatically redirects to the correct FSVM interface. If an FSVM fails, the client network address for the failed FSVM moves to another to preserve data access.

Multiple Client Networks

Starting with the Files 4.1 release, you can configure up to 10 client VLANs for a given file server. You might require multiple client networks for various reasons, including:

- Network isolation for different tenants for security purposes
- More compute efficiency by using a single file server with multiple isolated client networks, instead of deploying multiple file servers
- Routing traffic from multiple client networks to a single client network, which can lead to more complex routing and firewall management
- Using multiple client networks to avoid IP addressing limits for a given environment

The first client network that you configure during file server deployment becomes the primary network. The primary network communicates with Active Directory. You can add client networks after the initial deployment and modify the primary network if needed.

You can present common file shares across these different VLANs, or you can restrict share access to specific VLANs based on your security requirements.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 599

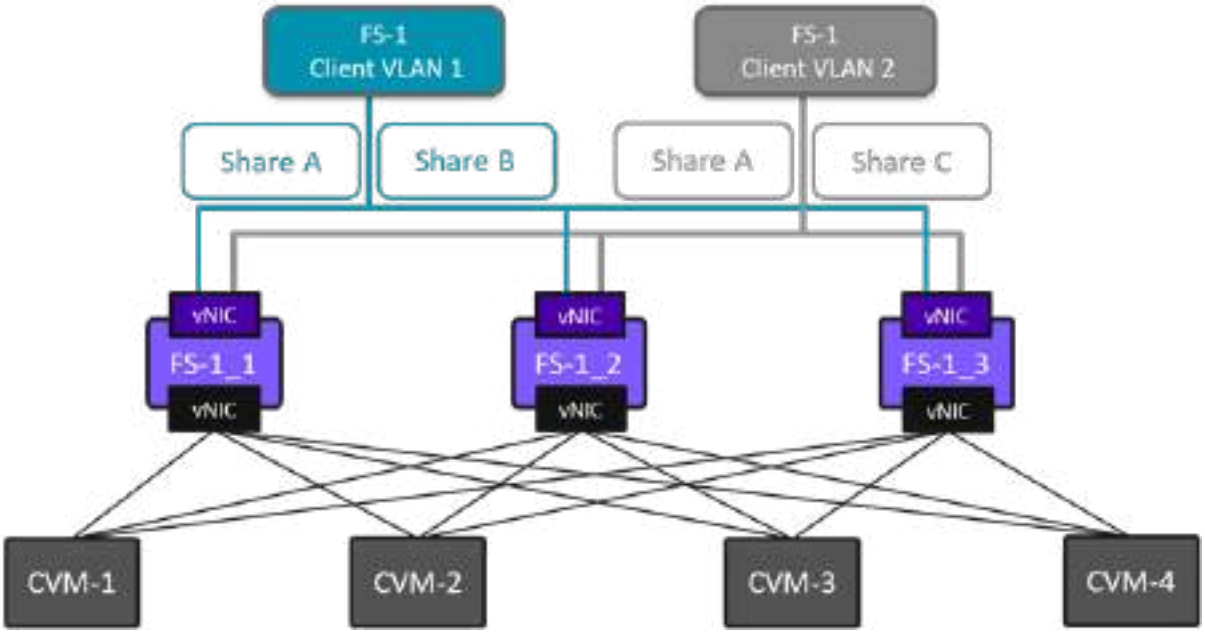


Figure 4: Multiple Client Networks with Common and Unique Shares

Client networks share the same vNIC within each FSVM. Because a vNIC is associated with a single virtual switch, all client networks must be trunked to the physical NICs associated with that virtual switch.

Storage

Each FSVM uses three separate vDisks:

- A 12 GB boot disk that contains the boot image
- A 45 GB disk (`/home/nutanix`) that contains the logs and software state
- A 45 GB disk for Cassandra data

Each FSVM also has a volume group that helps maintain auditing events and persistent handles for SMB Transparent Failover.

A Nutanix Files cluster is a single namespace that includes a collection of file systems used to support the SMB and NFS shares. The file systems support dynamic metadata, which enables you to store an unlimited number of files. The file system also supports variable block length allocations up to the default size of 64 KB. The variable block length

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 600

matches the size of the file; for example, a 1 KB file allocates 1 KB on the file system. Any file over 64 KB allocates in 64 KB increments.

While the default size is 64 KB, you can specify the maximum allocation size to improve performance. For environments with more random access patterns, you can choose a maximum allocation size of 16 KB. For environments with sequential patterns, you can choose 1 MB. These file systems use Nutanix volume groups as storage. For more information on the random or sequential file system options, see the Nutanix Files Performance tech note (requires Nutanix credentials).

Volume groups offer high availability for file systems and allow them to scale out. A volume group is a collection of logically related vDisks (or volumes) attached to the guest using iSCSI. Cluster CVMs balance the ownership of vDisks in a volume group, as demonstrated in the following figure.

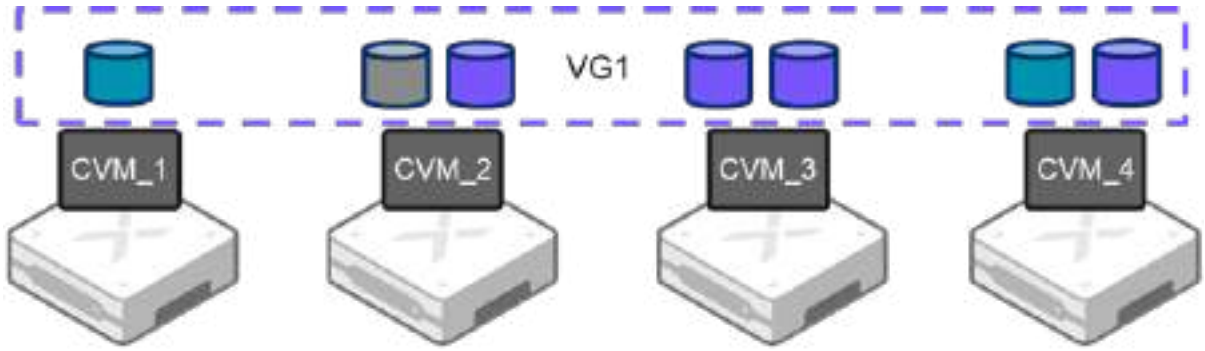


Figure 5: Volume Group Load Balancing

When an FSVM is down for maintenance or a fault occurs, one of the surviving FSVMs takes over volume group ownership and continues servicing requests.

Volume groups can contain up to 17 vDisks. The volume groups include 2 metadata vDisks, a separate intent log (SLOG) vDisk for synchronous random writes, and up to 14 data vDisks.

The initial file system pool created on the volume group uses seven drives and supports 40 TiB of data. The two metadata disks are pinned to SSD storage.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 601

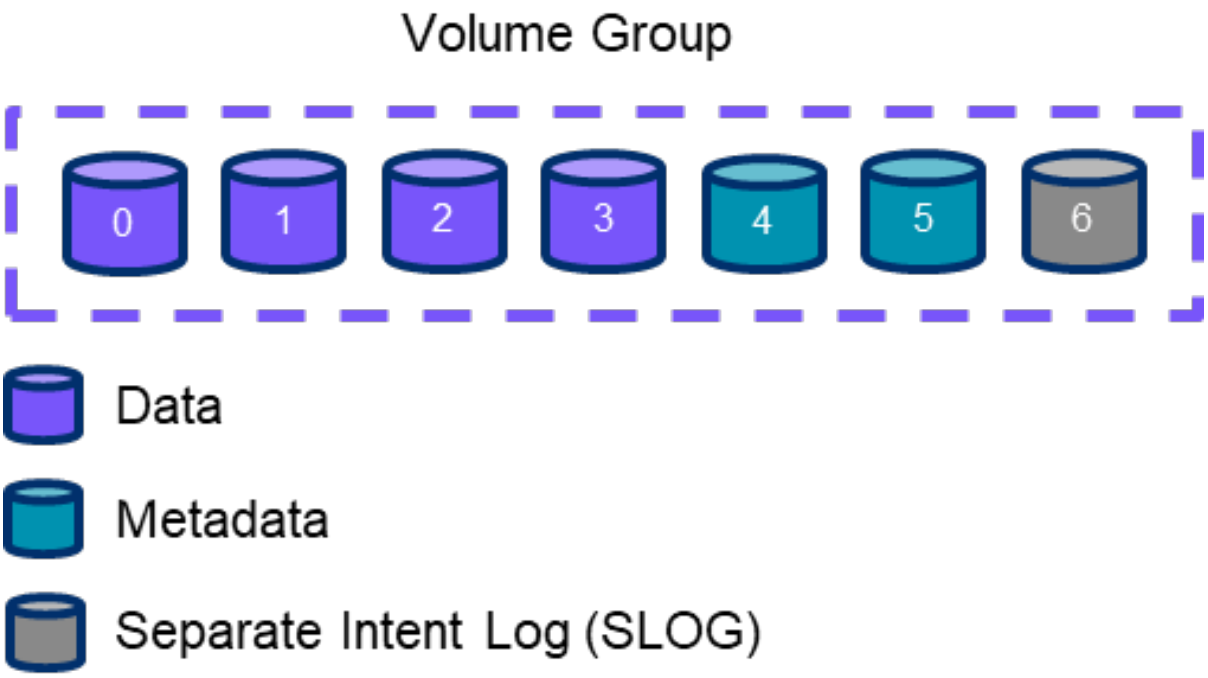


Figure 6: Initial 40 TiB File System Pool

Once this file system pool reaches 80 percent space utilization, Nutanix Files automatically expands it using a scale-up and scale-out approach, which varies depending on the Files version. Scaling up increases the file system pool size by allocating more space on the existing vDisks. Scaling out adds vDisks to the pool.

The maximum volume group sizes by Nutanix Files version are as follows:

- 2.x to 3.2: 40 TiB
- 3.2 to 3.6: 140 TiB
- 3.7 to 4.4: 280 TiB
- 5.0: 1,008 TiB

Note: You must create the file servers with Nutanix Files 3.0 or later to use the maximum size of 1,008 TiB.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 602

Exports and Shares

SMB shares and NFS exports have two configurations: Distributed and Standard.

- SMB shares:
  - Distributed (previously called home)
  - Standard (previously called general)
- NFS exports:
  - Distributed (previously called sharded)
  - Standard (previously called nonsharded)

A standard share is an SMB share or NFS export hosted by a single FSVM. A distributed share spreads the workload by distributing the hosting of top-level directories across FSVMs, which also simplifies administration.

> **Note:** You can store files in the root of distributed NFS shares. Distributed SMB shares don't allow files in the root.

Distributed Shares

Distributed shares and exports distribute data by dividing the top-level directories across all the FSVMs that make up the file server. Nutanix Files maintains the directory mapping for each responsible FSVM using InsightsDB. FSVMs use distributed file system (DFS) referrals for SMB and junctions for NFSv4 to ensure that clients can connect to the correct top-level directories.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 603

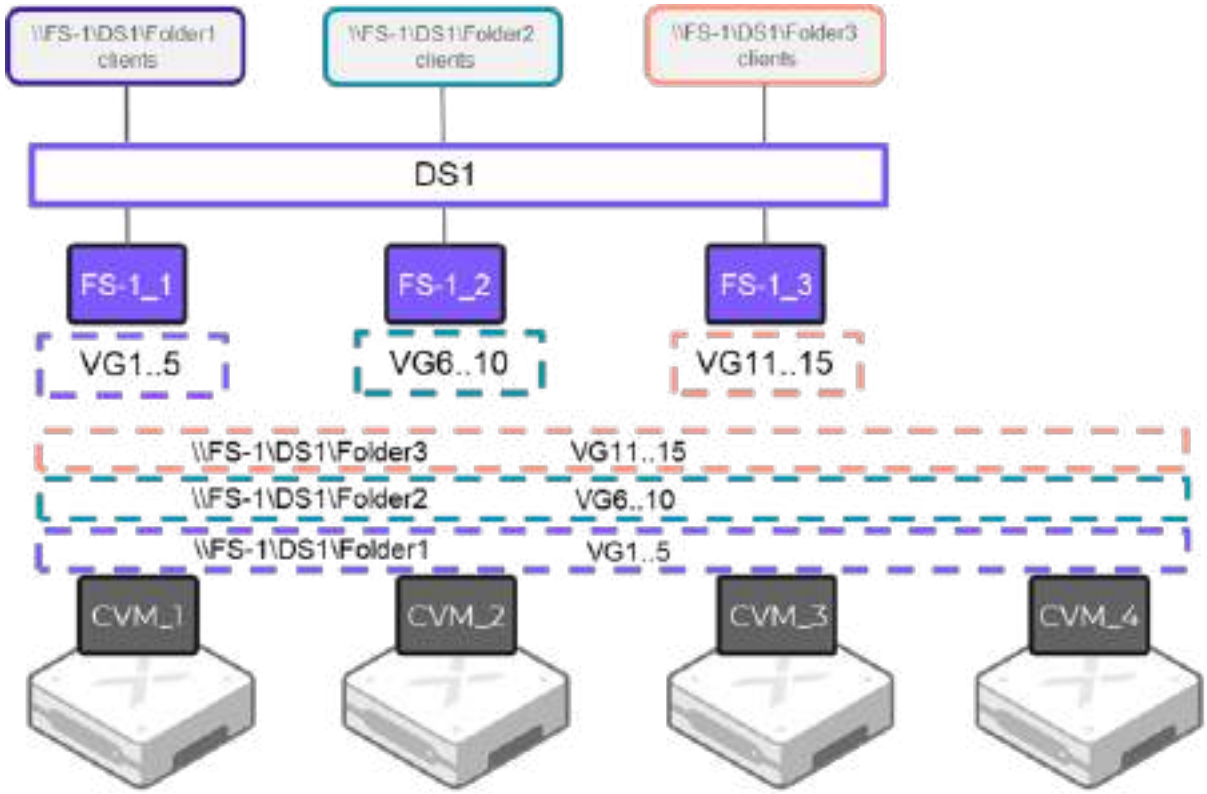


Figure 7: Distributed Directory Shares

Distributed share directories work well for home shares and exports because Nutanix Files automatically spreads the workload over multiple FSVMs per user (see the previous figure). If a user creates a share called `\\FS-1\DS1` that contains the top-level directories `\Folder1`, `\Folder2`, and `\Folder3`, those directories can be on FSVM-1, on FSVM-2, on FSVM-3, and so on. The FSVMs use a string hashing algorithm based on the directory names to distribute the top-level directories.

Distributed shares and exports begin with 5 volume groups for each FSVM (for example, 15 for a three-node cluster). Nutanix Files distributes the volume groups to different FSVMs in the file server cluster. When you have a large number of users, multiple volume groups improve load balancing across the FSVMs.

This distribution can accommodate a large number of users or directories in a single share or export. The scaling limits of more traditional designs can force administrators to create multiple shares or exports in which, for example, one set of users whose last

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 604

names begin with A through M run off one controller and users whose names begin with N through Z run off another controller. This design limitation leads to management overhead headaches and unnecessary Active Directory complexity. For these reasons, Nutanix Files expects to have one SMB distributed share for the entire cluster. If you need more than one home directory share, you can create additional shares as needed.

The top-level directories act as a reparse point—essentially a shortcut. Consequently, administrators must create directories at the root of the share for optimal load balancing. We recommend that you set permissions at the share or export root before you deploy user folders. This step allows newly created top-level directories to inherit permissions, so you don't have to adjust them after the fact using the Nutanix Files Microsoft Management Console (MMC) plug-in.

Use distributed shares for most of your use cases to ensure that user connections and data ownership are distributed across the FSVMs in the cluster.

Standard Shares

Standard shares and exports don't distribute top-level directories. A single file server always owns the files and subfolders for standard shares and exports. The following diagram illustrates three standard shares on the same file server.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 605

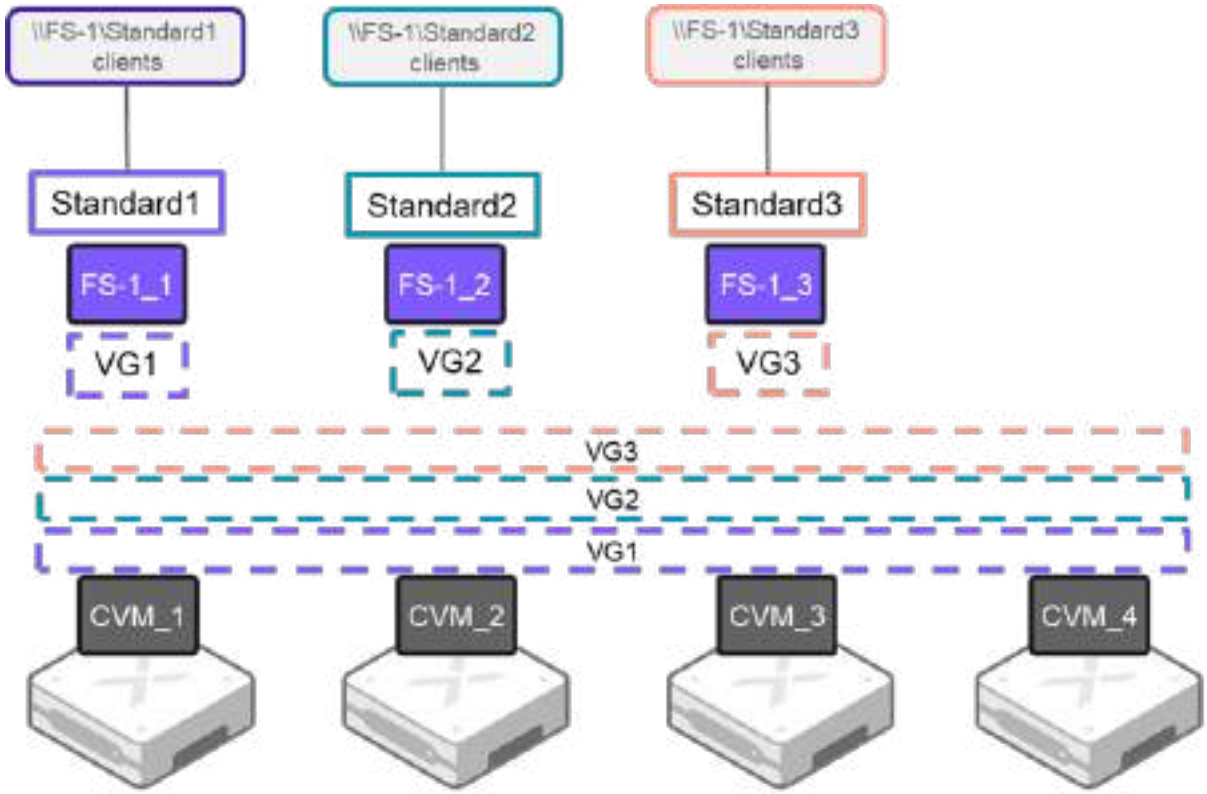


Figure 8: Three Standard Shares on the Same File Server

A single FSVM and volume group serve each standard share or export. Standard shares and exports can store files in the root of the share.

Volume Group and Storage Container Architecture

Nutanix Files supports the creation of up to 10 volume groups per FSVM. Once you reach this limit, new shares and exports use existing volume groups of the same type. For example, if you deploy a distributed share (15 volume groups) and 15 standard shares (creating 15 additional volume groups) on a three-node physical cluster, each FSVM hosts 10 volume groups: 5 for the distributed share and 5 for the standard shares. In this situation, the next share created uses an existing volume group because each FSVM is serving the maximum of 10 volume groups.

Every file server maps one-to-one to a storage container. Postprocess compression and erasure coding are on by default to save capacity. We don't recommend deduplication.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 606

Note: Erasure coding isn't a suitable data-reduction technology for desktop virtualization or user profile management solutions, such as FSLogix.

You can control inline compression on a share-by-share basis. When you create a share, compression is on by default. We recommend having inline compression at the share level and postprocess compression at the storage-container level. Depending on the version, Nutanix Files might enforce the container-level recommendations, so Nutanix recommends allowing Files to manage these settings.

Managing NFS Distributed Share Directories

In this section, we demonstrate how distributed top-level directories behave, and we provide the process of deleting a top-level directory.

Distributed share directories with NFSv4 introduce some unique behaviors. To balance performance across FSVMs, each top-level directory that you create becomes an automatically generated export. Nutanix Files mounts the export on demand when someone accesses the directory. Because these directories are exports rather than standard directories, it takes a few steps to remove a top-level directory.

To mount new distributed top-level directories, follow these steps:

1. Create a distributed share and mount it as /projects.

   You can see that mount on Linux using the df command:

   ```
   # df /projects
   Filesystem 1K-blocks Used Available Use% Mounted on
   1.1.1.10:/projects 1073741824 839455744 234286080 79% /projects
   ```

2. Create project directories:

   ```
   mkdir /projects/project1
   mkdir /projects/project2
   ```

3. Access the project directories:

   ```
   ls /projects/project1
   ls /projects/project2
   ```

   Accessing the directory, using ls in this case, mounts the automatically created top-level directory export. If you run df again you see two additional mount points:

   ```
   # df | grep project
   1.1.1.10:/projects 1073741824 839455744 234286080 79% /projects
   1.1.1.11:/projects/project1 1073741824 839455744 234286080 79% /projects/
   project1
   ```

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 607

```
1.1.1.12:/projects/project2 1073741824 839455744 234286080 79% /projects/
project2
```

These additional mount points allow a different FSVM to serve each export.

This behavior introduces additional steps when you delete a top-level directory. You can delete the project2 directory from any NFS client with the export mounted if you sign on as a user with the appropriate permissions.

To delete a distributed share export, follow these steps:

1. Delete the contents of the `project2` share.

   ```
   rm -rf /projects/project2/*
   ```

2. Unmount the `project2` share.

   ```
   umount /projects/project2
   ```

3. Delete the `project2` directory.

   ```
   rmdir /projects/project2
   ```

When you delete the top-level directory, it becomes inaccessible to other clients mounting the export. Processes that access the export after you delete it receive a Stale File Handle error.

Distributed shares with NFSv3 clients behave differently than those with NFSv4 clients. NFSv3 connections don't automatically mount the top-level directories of distributed shares. Because the top-level directories aren't submounted, you can rename and delete them without the additional steps required for NFSv4.

Nested Shares

Nutanix Files supports nested shares. Using a nested share, you can create a folder in an existing standard or distributed share and turn that folder into a directly accessible share. Nested shares are generally used to provide unique share-level permissions to folders in an existing file system. You can also use them to match existing environments for migration purposes. Nutanix Files version 4.4 supports up to 5,000 nested shares per file server.

Both SMB and NFS protocols support nested shares. Nested shares inherit some attributes from the parent share, but you can modify other attributes.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 608

- Nested share inherited attributes:
  - › Protocol type
  - › Maximum size
  - › Self-service restore
  - › Quota policy
- Nested share modifiable attributes:
  - › SMB access-based enumeration (ABE)
  - › NFS authentication and access
  - › NFS advanced settings

In the **Basics** tab of the **Create Share or Export** menu, you can create a nested share by providing its path in the **Share Path (Optional)** field.

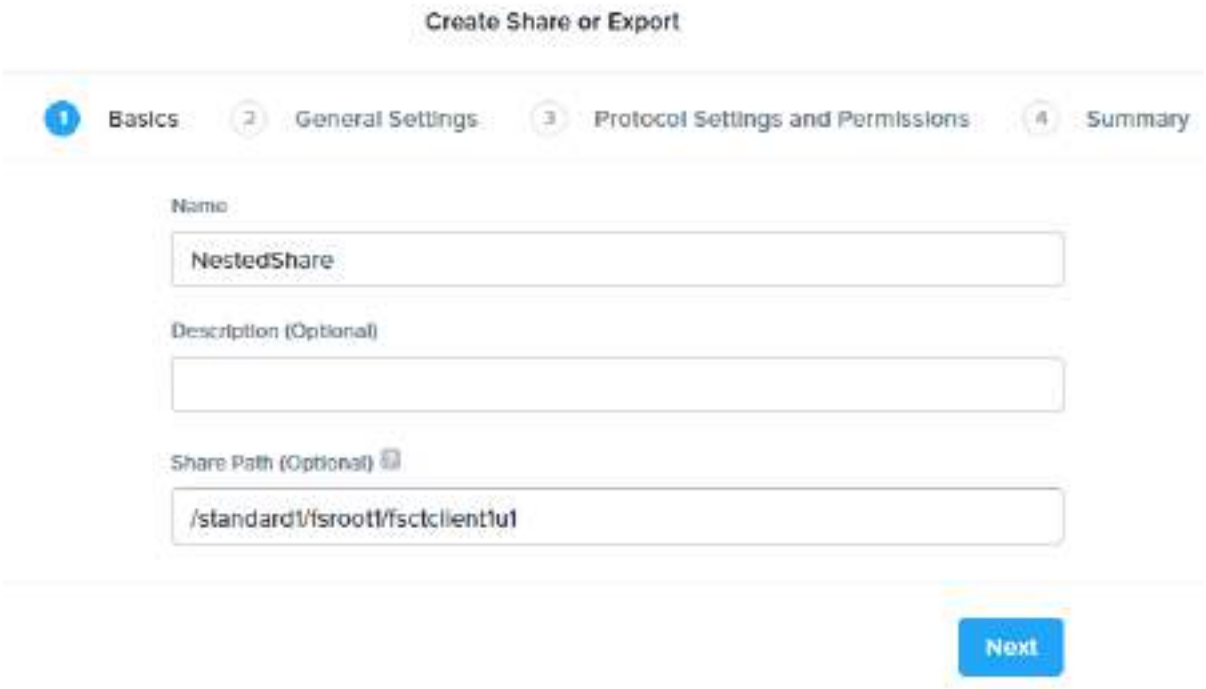


Figure 9: Create Share Menu with Nested Share Path

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 609

Connected Shares

The connected shares function mounts shares and exports as subfolders in other shares and exports. You can create a folder at any level of the folder hierarchy and mount either a standard or distributed share into that folder. The parent share hosting the folder can be a standard, distributed, or nested share.

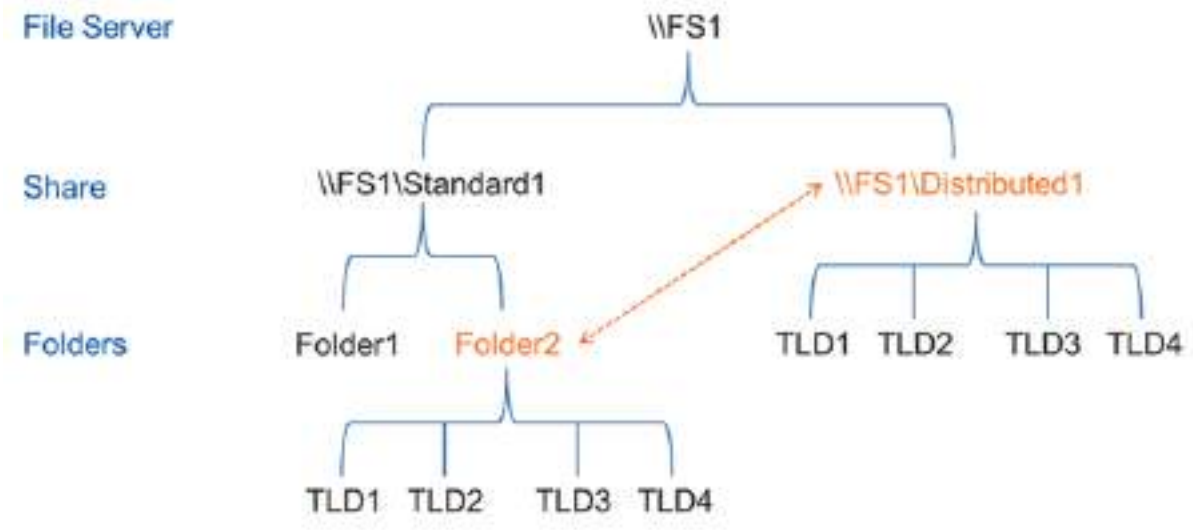


Figure 10: Submounting a Distributed Share into a Standard Share

Submounting shares and exports provides several benefits:

- You can use a distributed share at any level of a directory structure. Some applications have hardcoded folder paths where they store data or create directories. If you submount, you can establish a distributed share at the level that matches these application requirements.
- A folder adopts the size limit of the submounted shares, which enables folder-level quotas.
- A folder adopts the self-service restore setting for a submounted share, which enables folder-level snapshots.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 610

Write Once, Read Many Shares

Write once, read many (WORM) shares offer retention policies to ensure that files aren't inadvertently deleted. WORM shares are provided by failing file operations, which can cause file modification or deletion.

Not all applications work on a WORM share. Only applications that don't rely on operations that modify or delete files work normally.

Nutanix Files version 4.1 introduced share-level WORM support. WORM shares automatically commit files into a WORM state, specified by configuring a cool-off interval for the share. When a regular file in the share hasn't been changed—that is, the change time (or ctime) remains unchanged—for the duration of the cool-off interval, it transitions into a locked state. From there, the file goes into retention, also called commit. The file remains in retention until the end of its retention period, if one is specified; otherwise, the file is retained for the share's default retention period. When the retention period ends, the file transitions into an expired state. The purpose of the expired state is to facilitate the file's deletion.

You can only enable share-level retention (WORM) while creating a new share.

Nutanix Files version 4.2.1 introduced WORM compliance mode. Compliance mode prevents users from deleting files within their retention periods. You can also set a legal hold option protecting expired files from deletion. You cannot turn off compliance mode.

Directory Layout

Nutanix Files can store millions of files in a single share and billions of files across a multinode cluster with multiple shares. To achieve good response times for environments with high file and directory counts, think about directory design. Placing millions of files or directories in a single directory slows file enumeration, which might affect some applications.

For performance-sensitive applications, Nutanix recommends that you limit directory width—the number of files or directories in the root of a folder—to 100,000 objects. Increasing FSVM memory to cache metadata can help improve performance for environments with high object counts where directory enumeration is common.

Nutanix also recommends that you limit the number of top-level directories in distributed shares. The recommended number of top-level directories depends on the memory assigned to the FSVMs in the cluster. Don't permit your directory count to exceed 3,000

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 611

times the FSVM memory of one node. For example, for a three-node cluster with 12 GB of memory assigned to each FSVM, the maximum top-level directory count is 3,000 × 12 = 36,000.

Load Balancing and Scaling

Initial load balancing for a Nutanix Files cluster is based on the number of standard shares or the number of top-level directories you have in a distributed share. As explained in the Exports and Shares section, a standard share resides on a single volume group owned by one FSVM at a time. A distributed share is a collection of volume groups containing top-level directories. If some standard shares or top-level directories encounter a large workload and the volume groups supporting those workloads share an FSVM, a performance bottleneck can occur. Nutanix Files helps load balance workloads automatically when it detects potential performance problems by redistributing volume groups to different FSVMs for better load balancing across nodes.

Load balancing can occur in the following situations:

- When an administrator removes an FSVM from the cluster
- When the distribution of shares or top-level directories becomes poorly balanced during normal operation because of changing client usage patterns or suboptimal initial placement
- When increased user demand necessitates adding a new FSVM and its volume groups are initially empty

Nutanix Files addresses the second and third situations by maintaining usage statistics and patterns to detect per-FSVM load (in terms of CPU and memory utilization) and per–volume group load (in terms of user connections and latency of operations). Nutanix Files uses these statistics to make a load balancing recommendation, but the administrator must accept the recommendation before Files carries out the action. Nutanix calls this feature one-click performance optimization.

When Nutanix Files recommends a performance optimization, it provides the following choices:

- Scale up: Improve performance by adding vCPU and memory to the existing FSVMs.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 612

- Rebalance: Eliminate performance bottlenecks by redistributing the workload across the existing FSVMs.
- Scale out: Improve performance by adding new FSVMs to the existing file server.

Load balancing through volume group redistribution doesn't always improve performance. For example, if clients target a low-level share directory that can't be further distributed among FSVMs, performance doesn't improve. In such cases, Nutanix Files supports scaling up by adding vCPU and memory to the FSVMs. Scaling up is seamless to end users.

We recommend a scale-up operation for performance optimization if SMB connection limits reach 95 percent utilization over a two-hour time window.

A brief outage can happen during volume group migration and FSVM scale-out if you aren't using shares with continuous availability enabled. The file share or export requires a client reconnect after migration and scaling out. Most clients try to reconnect for 50–60 seconds, which limits the overall impact.

Load balancing also occurs for each vDisk in a volume group. Nutanix Volumes requires the administrator to configure an iSCSI data service IP address. The data service IP address is a highly available virtual IP address used as an iSCSI discovery portal. Each vDisk in a volume group represents its own iSCSI target that any CVM in the cluster can own. Nutanix Volumes uses iSCSI redirection to place and automatically load balance these sessions as needed. The load balancing feature for Nutanix Volumes is called the Acropolis Dynamic Scheduler (ADS).

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 613

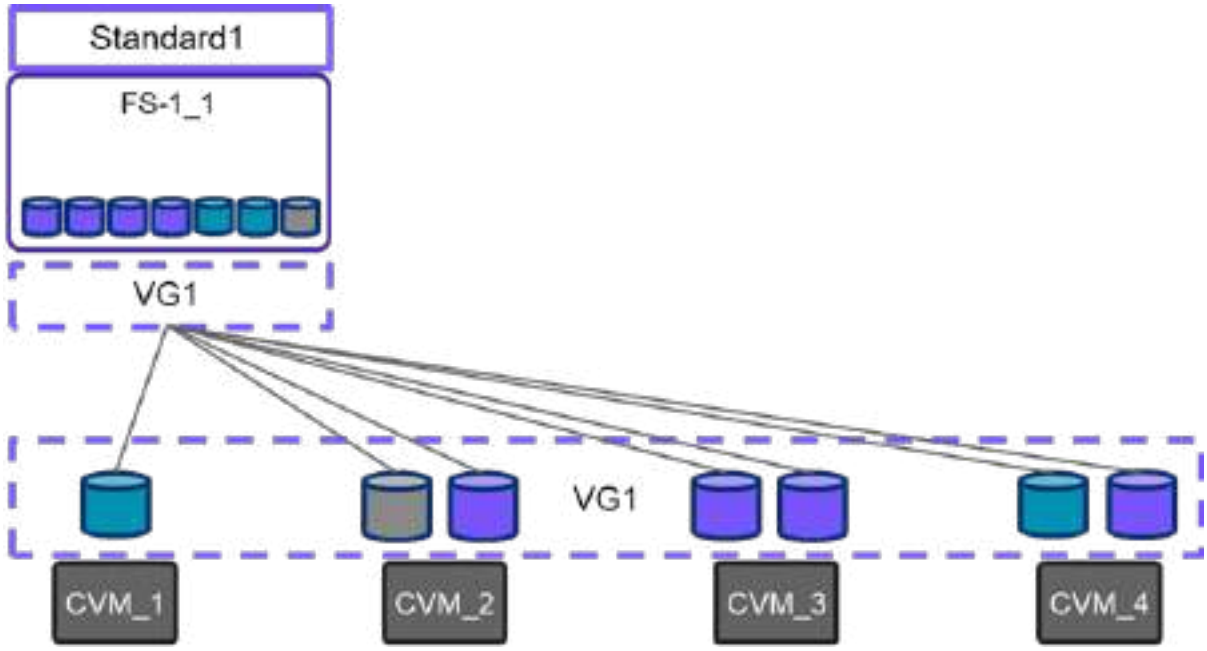


Figure 11: Load Balancing Volume Groups with Nutanix Volumes

For more information, see the Nutanix Volumes best practices guide.

High Availability

Nutanix designed Files to recover from a range of service disruptions, including when a local CVM or FSVM restarts or fails.

CVM Failure or Upgrade

If a CVM goes offline because of failure or planned maintenance, any active sessions against that CVM are disconnected, triggering the iSCSI client to sign on again. The new authentication occurs through the external data services IP, which redirects the session to a healthy CVM.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 614

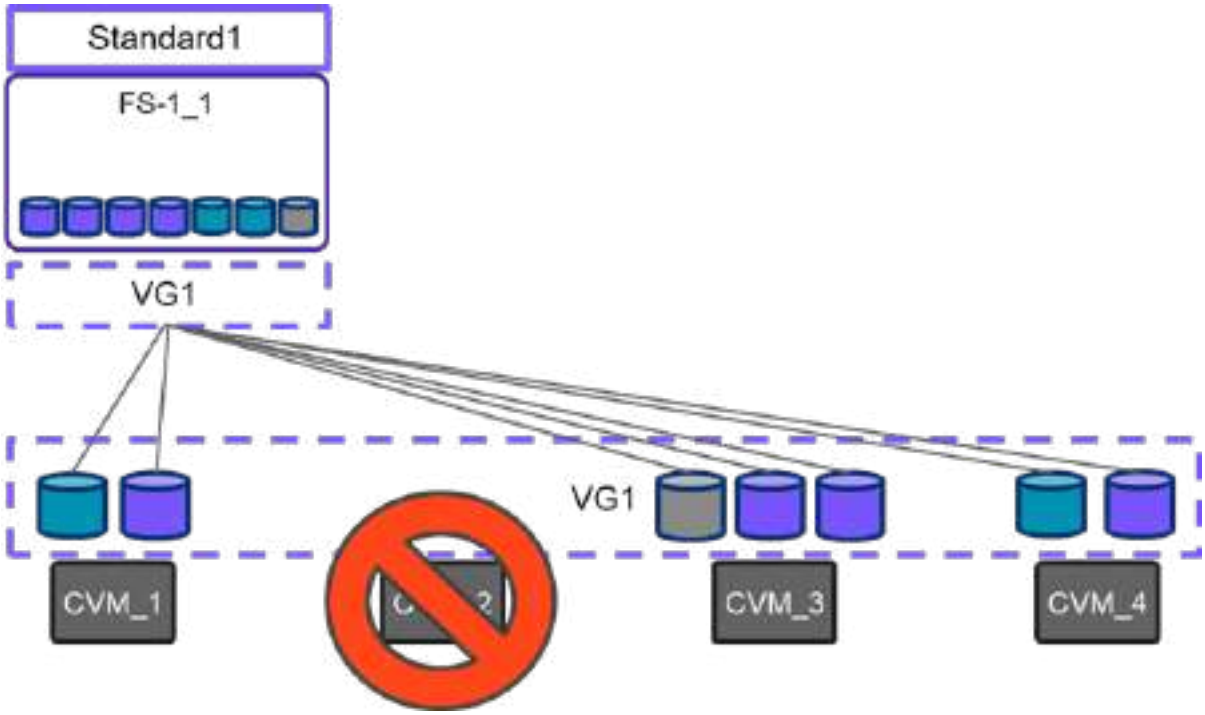


Figure 12: Nutanix Volumes High Availability for File Server Volume Groups

When the failed CVM returns to operation, the iSCSI session fails back. In the case of a failback, the system signs the FSVM off and redirects it to the appropriate CVM.

Node Failure

When a physical node fails completely, Nutanix Files uses leadership elections and the local Minerva CVM service to recover. The FSVM sends heartbeats to its local Minerva CVM service once per second, indicating its state. The Minerva CVM service keeps track of this information and can act during a failover.

Nutanix Files reinstates control using the following process:

1. Stop SMB and NFS services.
2. Disconnect the volume group.
3. Release the IP address and share and export locks.
4. Register the volume group with FSVM-1.
5. Present new shares and exports to FSVM-1 with eth1.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 615

When an FSVM fails, the Minerva CVM service unlocks the files from the failed FSVM and releases the external address from eth1. The failed FSVM's resources then appear on a running FSVM. The internal Zookeeper instances store this information to send it to other FSVMs, if necessary.

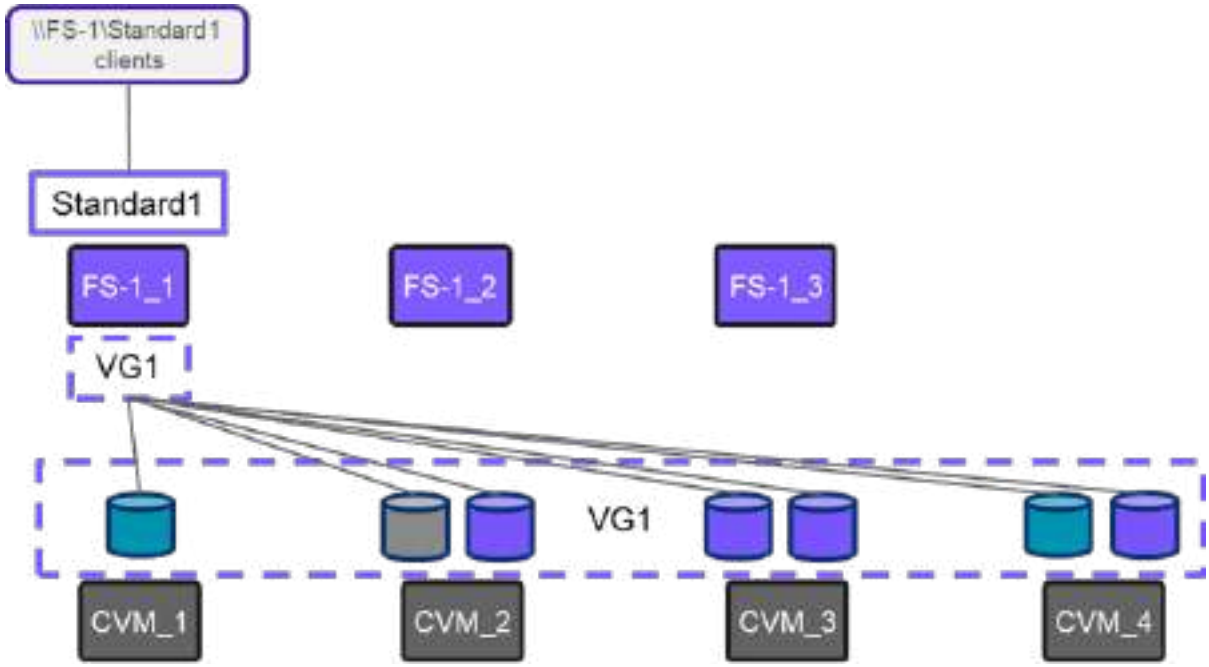


Figure 13: FSVM Ownership with Single Share and Volume Group Example

When an FSVM is unavailable, the remaining FSVMs volunteer for ownership of the shares and exports associated with the failed FSVM. The FSVM that takes ownership of the volume group informs the CVM that the volume group reservation has changed. If the FSVM that attempts to take control of the volume group is already the leader for a different volume group it has volunteered for, it relinquishes leadership for the new volume group immediately. This arrangement ensures distribution of volume groups even if multiple FSVMs fail.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 616

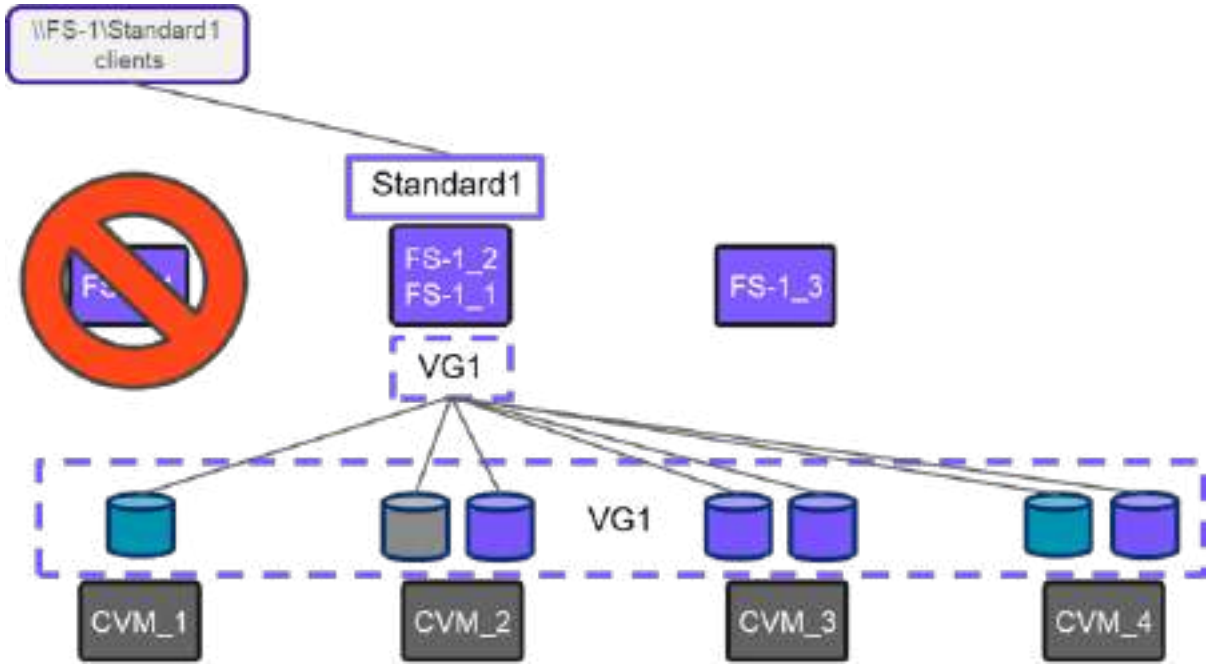


Figure 14: FSVM-1 Failure

The Nutanix Files Zookeeper instance tracks the original FSVM's ownership using the storage IP address (eth0), which doesn't float from node to node. Because FSVM-1's client IP address from eth1 is now on FSVM-2, client connections persist. The volume group and its shares and exports are reregistered and locked to FSVM-2 until FSVM-1 can recover and a grace period elapses.

The failover process typically takes between 30 and 180 seconds, and client operations can be affected during this time. SMB shares enabled for continuous availability and hard-mounted NFS shares experience I/O delays but maintain connections during high-availability events.

If an FSVM is offline for 30 minutes or longer, the Nutanix Files cluster redistributes core cluster services (such as Zookeeper) owned by the offline node. The cluster needs at least three online FSVMs in order to move services. Moving cluster services helps the Files cluster rebuild itself smaller and survive subsequent node failures.

When FSVM-1 comes back online and finds its shares and exports locked, it assumes that a high-availability event has occurred. After the grace period expires, FSVM-1 regains control of the volume group through the Minerva CVM service. Once the failed FSVM comes back online, the cluster automatically switches back to the larger size.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 617

Single-Node Environments

Nutanix Files clusters that only have one FSVM rely on hypervisor-based high availability to maintain services. If the physical node that owns the FSVM fails, the VM restarts on another physical node. Client connections are disrupted until the FSVM restarts.

Active Directory and SMB Operations

Nutanix Files SMB works with Active Directory. To deploy a cluster, you need domain privileges to create the machine account and the DNS entries for DFS referrals. The file server doesn't store these credentials.

Nutanix Files versions 3.6 and later simplified the permissions required to add domains when you create a file server. The delegated domain user permissions required are as follows:

- Create computer objects.
- Read servicePrincipalName.
- Write servicePrincipalName.

Nutanix Files can also create the required DNS entries automatically during file server creation. Automated DNS entry creation requires Microsoft Windows DNS and a user account with DNS admin permissions.

The maximum number of client connections depends primarily on how much memory the FSVM has. The following table provides Nutanix configuration recommendations as of Files version 5.0.

Table: Supported Active Client Connections

FSVM Memory	Supported Client Connections per FSVM	Supported Client Connections for Four-FSVM File Server Cluster
12 GB	500	2,000
16 GB	1,000	4,000
24 GB	1,500	6,000
32 GB	2,000	8,000
40 GB	2,750	11,000

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 618

FSVM Memory	Supported Client Connections per FSVM	Supported Client Connections for Four-FSVM File Server Cluster
60 GB	3,250	13,000
64 to 512 GB	4,000	16,000

You can continue deploying additional FSVMs if you have free nodes; you can also deploy multiple file servers.

Nutanix Files uses DFS referrals to direct clients to the FSVM that owns the targeted share or top-level directory. The following process takes place when a client sends a file access request.

1. When the user accesses their files, a DNS request might be triggered to resolve the file server name.
2. Using DNS round robin, DNS replies with an FSVM IP address.

   In this example, the IP address for FSVM-1 returns first.
3. The client sends a create or open request to FSVM-1.
4. The folder doesn't exist on this file server, so a STATUS_PATH_NOT_COVERED is returned.
5. The client then requests a DFS referral for the folder.
6. FSVM-1 looks up the correct mapping in the file server's Zookeeper and refers the client to FSVM-2.
7. A DNS request goes out to resolve FSVM-2.
8. The DNS request returns the IP address of FSVM-2.
9. The client receives access to the correct folder.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 619

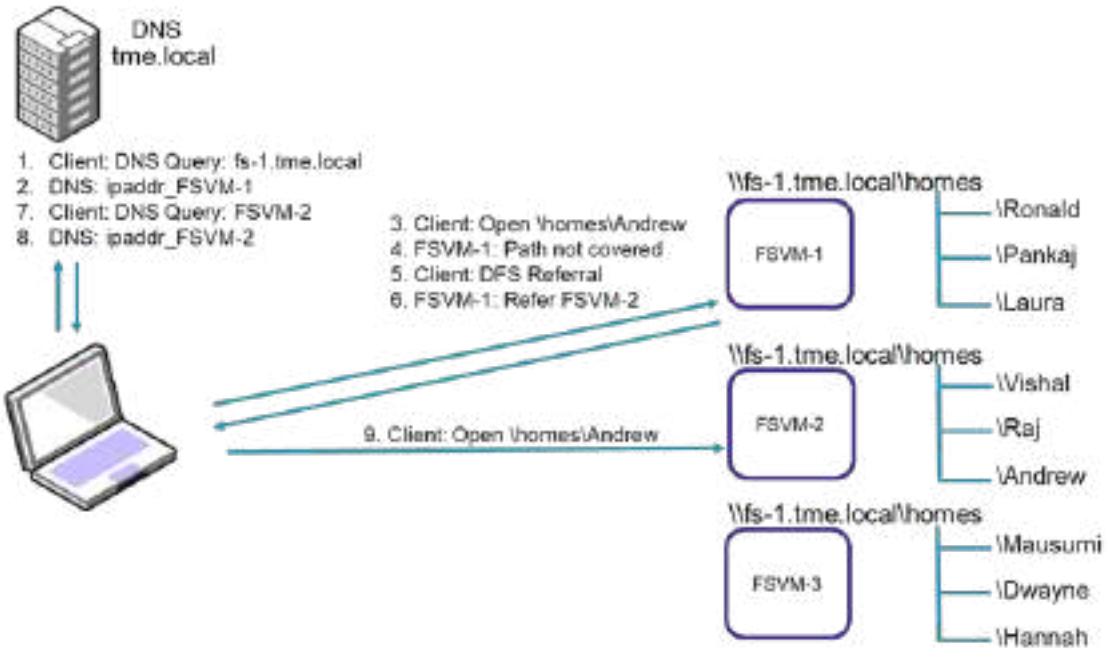


Figure 15: DNS Request for SMB

Managing Shares

You can manage Nutanix Files shares the same way that you manage traditional file servers. For standard shares and top-level directories in distributed shares, you can assign permissions with native tools such as Windows Explorer. NTFS-level permissions, also called Windows access control lists (ACLs) or NTACLs, manage all file and folder access.

The distributed share has some special requirements because of how Nutanix uses DFS referrals. DFS referrals have a single namespace even though the data contained in the share can be spread out over many FSVMs. Typically, to delete a user's home directory, you select the top-level directory and delete the entire directory subtree. However, when using a distributed export or share, you can't just delete the top-level directory because it's a separate share created internally by Nutanix Files. Because you can't directly delete a top-level directory, removing it requires additional steps.

You can choose between two options for renaming or deleting distributed share folders:

- Find out which FSVM hosts the folder and rename or delete the folder directly using the FSVM as the UNC path.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 620

- Use the Nutanix Files MMC snap-in to manage top-level directories. Any file server administrator can perform the MMC operations; you don't need to assign privileges manually. Establish a connection to the Files namespace and perform the following SMB share management tasks:

  1. Create, delete, rename, and change permissions for top-level directories.
  2. Change NTFS permissions for shares.

  > **Note:** Use the MMC Snap-In for Nutanix Files when you modify NTFS permissions at the root of a distributed share. The MMC Snap-In for Nutanix Files ensures that permissions propagate to the top-level directories based on inheritance.

You can modify share-level permissions with the Windows-native Shared Folders MMC. Simply launch the Shared Folders MMC and point it to the name of the Nutanix Files instance under the Another computer option. By default, all SMB shares have share-level ACLs set to Everyone with Full Control. Nutanix Files 4.4 also allows you to control share-level ACLs during share creation and editing.

> **Note:** We recommend leaving share permissions at Full Control and managing access with NTFS permissions.

You can also manage open file locks and user sessions with the Windows Shared Folders MMC.

Access-Based Enumeration

Access-based enumeration (ABE) is a Windows feature (SMB protocol) that filters the list of available files and folders on the file server to include only those the requesting user can access. This filter saves time for the user and helps the administrator to prevent users from accessing files not meant for them.

ABE doesn't control security permissions, and running ABE has associated overhead. Every time a user requests a browse operation, ABE must filter out objects the user doesn't have permission for. Even if the user has permission to access all contents of the share, ABE still runs, which uses additional CPU cycles and increases latency.

Don't turn on ABE for home directories (using a distributed share). Most users get their home mapping when they sign in and always have access to their own content, so we don't recommend ABE for home directory use cases.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 621

SMB Signing

SMB signing is a feature of the SMB protocol that enables a digital signature against each network packet. Digital signing helps verify the packet's origin and authenticity and prevent tampering, such as eavesdropping attacks.

Nutanix Files supports SMB signing and honors the signing request as configured from the SMB client. SMB signing is enabled but not enforced by default. The SMB signing configuration of the client negotiates with the file server to determine how signing is used. You can optionally enforce signing for all clients by setting signing as **Mandatory**. For more information on configuring signing as mandatory, see Security Harding in the Nutanix Files User Guide.

The SMB protocol uses AES-CMAC to compute signatures for SMB signing. This computation process can impact performance against the SMB share where you enabled signing. With Nutanix Files 3.2 and later, the signature computation uses the Intel processor AES-NI instruction set. The Intel processor hardware acceleration helps reduce the overhead associated with SMB signing.

SMB signing decreases the maximum performance possible for SMB shares.

SMB Encryption

Nutanix Files supports in-flight encryption of SMB data between clients and shares. SMB encryption isn't on by default with Nutanix Files. You can turn encryption on as needed on a share-by-share basis.

Clients must support encryption to access shares with encryption enabled. Nutanix Files offloads encryption processing using the Intel processor AES-NI instruction set to limit the performance impact.

SMB encryption decreases the maximum performance possible for SMB shares.

Durable SMB File Handles

Durable handles let SMB clients survive a temporary client-side connection loss after opening a file, allowing transparent client reconnection within a timeout. Nutanix Files supports durable handles for SMB clients with no configuration required. SMB 2.x and SMB 3.0 clients can use durable handles to reconnect transparently if a client-side network interruption occurs. The system doesn't maintain durable handles through unplanned file server events such as FSVM failures. Starting with Files 4.2, the system

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 622

maintains durable handles during file server upgrades, but it does so by best effort and provides no guarantees.

SMB 3.0 Transparent Failover

SMB 3.0 Transparent Failover is a feature of the SMB 3.0 protocol that enables fully nondisruptive operations against SMB shares. Transparent failover is often called continuously available file shares. File server–side failures or upgrade events persist file handles so that clients transparently reconnect to another FSVM without affecting applications. Nutanix Files versions 3.7.1 and later support SMB 3.0 Transparent Failover. Continuously available shares are intended for solutions that require nondisruptive operations, like Citrix App Layering and FSLogix.

> **Note:** SMB Transparent Failover enforces synchronous write operations, which might decrease the maximum possible performance for SMB shares.

DFS Namespace

DFS Namespaces (DFS-Ns) can logically organize shared folders on different servers or in different geographic locations into a single namespace. These shared folders appear to the user as a unified, hierarchical directory that they can navigate using any Windows client. The server names and their locations are completely hidden from the user, enabling large scale-out architectures.

The most common architecture is an Active Directory–integrated DFS-N, where the namespace is hosted on two or more domain controllers (namespace servers) and the file data is stored on member servers. Nutanix Files supports the use of DFS-Ns when you use Nutanix Files as a member server and Nutanix Files shares as folder targets in the namespace. You can use either distributed shares or standard shares within the namespace.

DFS-Ns are also commonly used in active-active replication scenarios. DFS-Ns allow multiple file servers hosting the same data to support a common folder. DFS-Ns help provide site affinity, based on Active Directory, for users to connect to the file server acting as a folder target. You need a replication engine to maintain the data when active-active scenarios are present. Nutanix supports the use of Peer Software as the replication engine for active-active scenarios. For more information on the Peer Software and Nutanix integration, see the PeerGFS and Nutanix Files datasheet.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 623

Active Directory, LDAP, and NFS Operations

The following sections describe the different levels of support Nutanix Files offers for NFSv4 and NFSv3 operations.

NFSv4

Nutanix Files supports NFSv4, which is more stateful than NFSv3 and includes advanced features such as strongly mandated security and DFS-like referrals. Moreover, most recent distributions of Linux, Solaris, and AIX use NFSv4 as the default client protocol.

Nutanix Files supports Active Directory, LDAP, and unmanaged access to NFSv4 exports. To make the transition from NFSv3 easier, Nutanix Files doesn't require administrators to configure Active Directory or LDAP. You can use AUTH_SYS or AUTH_NONE authentication. AUTH_SYS authenticates at the client, just like NFSv3.

By enabling Active Directory support, you can use three different levels of Kerberos authentication. Each of the following options uses Kerberos version 5:

- krb5, DES symmetric key encryption, and an MD5 one-way hash for Nutanix Files credentials.
- krb5i, in addition to krb5, uses MD5-based MAC on every request and response.
- krb5p, on top of krb5 and krb5i, makes the connection between client and server private by applying DES encryption.

When you deploy Nutanix Files for NFS, you can select Active Directory, LDAP, or leave it unmanaged.

The following steps illustrate what happens behind the scenes when a client sends a file access request using NFSv4. These steps are similar to the referral process for SMB.

1. The client sends a DNS request for the file server name.
2. Using DNS round robin, a DNS reply returns with an FSVM address.

   In this example, the IP address for FSVM-1 returns first.
3. The client sends a create or open request to FSVM-1.
4. If the mount doesn't exist on this file server, it returns NFS4ERR_MOVED.
5. The client requests a GETATTR(FS_LOCATIONS).

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 624

6. FSVM-1 looks up the correct mapping in the file server's Zookeeper and refers the client to FSVM-2.
7. A DNS request goes out to resolve FSVM-2.
8. The DNS request returns the IP address of FSVM-2.
9. The client receives access to the correct mount point.

NFSv3

Nutanix Files supports NFSv3. NFSv3 is enabled on each file server by default, but you can manually turn it off. All NFS exports have NFSv3 turned on or off based on this file server setting. Nutanix Files supports LDAP and unmanaged exports with NFSv3 but doesn't support Active Directory and Kerberos for NFSv3.

You must mount exports with the TCP protocol if clients use NFSv3.

Nutanix Files with NFSv3 includes support for both distributed and standard exports. Unlike NFSv4, NFSv3 doesn't support DFS-like referrals. Clients aren't redirected to the FSVMs that host a given distributed top-level directory or standard export; they connect to the first FSVM resolved using DNS. An internal remote procedure call (RPC) manages any file access requests to exports and top-level directories not hosted by the client-connected FSVM. This RPC sends or receives data between the client-connected FSVM and the FSVM that owns the required exports and volume groups. The following diagram illustrates this process.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 625

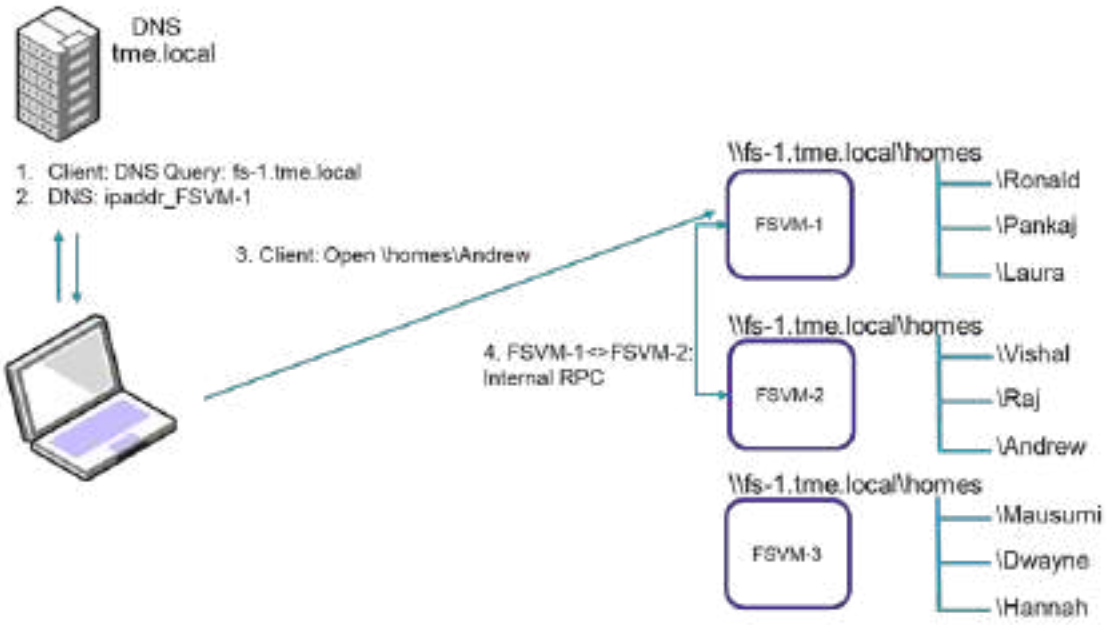


Figure 16: DNS Request for NFSv3

Multiprotocol

You can create file shares that are accessible from both SMB and NFS clients, referred to as multiprotocol shares. Multiprotocol shares allow simultaneous read access to the underlying file data from either protocol. Write access can also occur from either protocol, but not simultaneously to the same file. Authentication support for multiprotocol shares includes all protocols and authentication options available with Nutanix Files (such as Active Directory for SMB and LDAP, AUTH_SYS, AUTH_NONE, and Active Directory support for NFS).

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 626

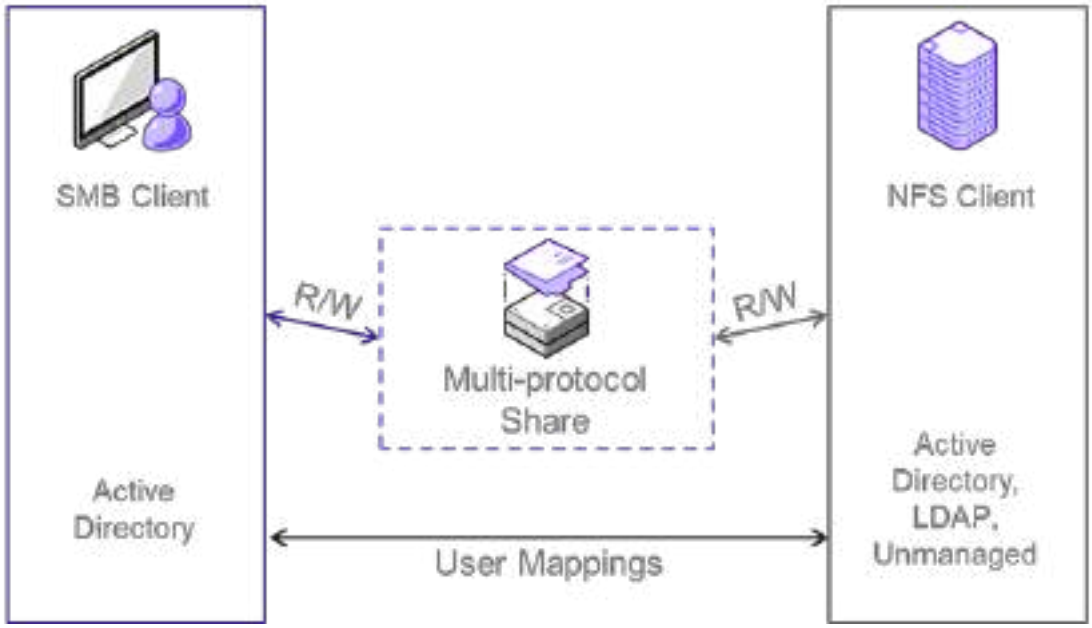


Figure 17: Multiprotocol Shares

Multiprotocol introduces the concept of a native protocol (either SMB or NFS) for a file share. You specify the native protocol and non-native protocol when you create the share.

You manage all access control for a multiprotocol share using the native protocol. For SMB, the native protocol is Windows ACLs, and for NFS, it's Unix mode bits. When non-native protocol access occurs, Nutanix Files maps user access to the permission applied with the native protocol. A mapping must exist between the user accounts using the non-native protocol and the user accounts with permission applied through the native protocol.

If you use Active Directory for both SMB and NFS with Kerberos, you don't need any explicit mappings because both have the same users and groups. You can use Identity Management for Unix (RFC 2307) to map NFS users to your Active Directory users with attributes. For LDAP or unmanaged accounts, or for Active Directory without Kerberos, you must create a mapping between the users and groups in Active Directory. You can use Prism or the nCLI to manage Nutanix Files user mappings.

You can configure a default index to map all non-native users and groups to a specific native user or group. You can also use a rule-based mapping for Active Directory and LDAP users—specifically, a template where the SMB name matches the NFS username.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 627

Additionally, you can configure explicit mapping, which overrides rule-based mapping. Explicit mapping consists of two mapping subcategories: one-to-one mapping lists and wildcard mapping. You can use the one-to-one mapping list to manually enter or upload a CSV file that maps users or groups across protocols. Use wildcards for many-to-one mapping. You can also deny share access for a specific user or group. For more information on creating user mappings, see the User Mapping section of the Nutanix Files User Guide.

The following table provides the user mapping requirements based on the directory service and authentication type.

Table: User Mapping Requirements

SMB Directory Service	NFS Directory Service	Export Authentication Type	Supported	User Mapping Required
Active Directory	Active Directory	Kerberos5*	Yes	No
Active Directory	Active Directory	System	Yes	Yes (Name-to-ID mapping)
Active Directory	Active Directory	None	Yes (Primary NFS only)	Yes (Name-to-ID mapping)
Active Directory	Active Directory + RFC 2307	Kerberos5*	Yes	No
Active Directory	Active Directory + RFC 2307	System	Yes	Yes (Name-to-ID mapping)
Active Directory	Active Directory + RFC 2307	None	Yes (Primary NFS only)	Yes (Name-to-ID mapping)
Active Directory	LDAP	System	Yes	Yes (Name-to-Name mapping)
Active Directory	LDAP	None	Yes (Primary NFS only)	Yes (Name-to-Name mapping)
Active Directory	Unmanaged	System	Yes	Yes (Name-to-ID mapping)
Active Directory	Unmanaged	None	Yes (Primary NFS only)	Yes (Name-to-ID mapping)

**Kerberos 5, 5i, and 5p.*

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 628

Quotas

Administrators can configure the default, user, and group quota space for any share. The default level is the quota limit for every user unless the administrator specifies otherwise. A user-level quota policy sets a specific amount of storage for a single user. For example, if an administrator allocates 1 GB, the user can't take more than 1 GB. A group-level quota policy extends a user policy to include all users for an entire Active Directory group, where each user can use the assigned quota value. For example, if the administrator sets a group's quota to 10 GB, each member of that group can use 10 GB. You can assign quotas for SMB, NFS, or multiprotocol-enabled shares. In the case of multiprotocol shares, administrators apply quotas using the native protocol. User or group policies are enforced for the non-native protocol based on the user mapping.

Notifications

Administrators can configure Nutanix Prism to send email alerts to the user and to other recipients using the same engine that sends cluster alerts. Designated users receive a warning email message when they reach 90 percent of quota and an alert email message when they reach 100 percent. You can also add departmental share owners to the email notification list. With Files 4.0, you can customize the email notification template.

The following table shows the order of precedence when dealing with quotas for a share.

Table: Order of Precedence for Quotas

Order of Precedence	Policy
1	User policy
2	Group policy (the group policy with the highest quota wins)
3	Default user policy

Enforcement

You can configure enforcement types for each quota-level category. Enforcement types determine if a user or group can continue to use the share after they consume their quota. A hard enforcement type prevents the user from writing on the share when they reach their quota limit. A soft enforcement type allows a user to write even if they exceed

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 629

the quota limit. Under either enforcement type, users over their quota receive an email notification every 24 hours until they resolve the issue.

Selective File Blocking

You can define a list of file names and file extensions to block from storage on SMB, NFS, and multiprotocol-enabled shares. You can define a list of files to block at the server level and at the share level. These entries can include wildcards for both the file name and file extension. For example, you can block the file pattern `encrypt*.*xt`.

In the **Create a share/export** window, you can define which file types to block with a comma-separated list of file names and extensions. File types blocked at the server level apply to all shares. When you define a list of file types at the share level, the share-level setting overrides the server-level setting.

When you attempt to create or rename a file with a blocked pattern, an access denied message appears. You can read, edit, or delete existing files created prior to a blocked file type policy. You can also use File Analytics to discover if any unwanted file types exist on a file server before you apply the policy. File Analytics can also search for file patterns matching known ransomware variants.

When you use Data Lens to manage your ransomware file name patterns, you can't see the patterns from within the file server or share specific blocking lists.

Files Manager

Prism Central and Nutanix Files support an integrated service called Files Manager, which discovers all Files instances running on clusters registered in Prism Central. Files Manager also provides views on all alerts and events across your file server farm. You can view the file server configurations and launch the Files console to manage the file servers.

From Files Manager, you can deploy and scale file servers, configure Smart Disaster Recovery and Data Synchronization, and apply role-based access control (RBAC) to fine-tune what users can create and control.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 630

Role-Based Access Control

With RBAC, a Super admin in Prism Central can delegate file server management to nonadmin users. You can control which file servers a user is allowed to view or manage, along with the operations they are allowed to perform, such as creating or deleting file servers, creating shares, or editing file server attributes. The Files Manager User Guide details the full capabilities and configuration of RBAC for Files.

Apply RBAC policies through Prism Central. RBAC policies aren't available when managing Nutanix Files with Prism Element.

File Analytics

Nutanix Files offers a rich auditing API that applications can subscribe to and receive real-time notifications of file-related events, including file creation, deletion, read, write, and permissions changes. A common use for these APIs is forwarding such events to a syslog server for retention and audit trails. Nutanix File Analytics consumes this native auditing API and delivers additional insights about the underlying data and user activity.

To deploy File Analytics using Nutanix Prism, follow these steps:

1. Download the Analytics bundle.
2. Perform a one-click deployment.
3. Launch the File Analytics page.
4. Enable analytics against some or all file server instances running on your cluster.

Enabling analytics requires a user account with administrative permissions to do an initial scan of the file server.

Intelligent Insights

File Analytics scans and continuously captures all file activity for registered file server instances. These logs show you what operations occurred against specific data and by specific users. File Analytics analyzes logged events to provide an initial dashboard of information:

- Capacity trend, which shows what's being consumed and how it's changed over time

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 631

- Data age, which is the calculation of the last time a file was modified and the percentage of data at varying age ranges
- Anomaly alerts, which show all file operations that exceed a given anomaly threshold, like the deletion of many files
- Permission denials, which are the number of permission-denial events for specific users over the selected time range
- File distribution by size, which shows the number of files in a given size range
- File distribution by type, which details storage consumption by file type, such as log files, image files, and video files
- The top five active users based on total operations over the selected time period
- The top five accessed files based on total operations over the selected time period
- File operations, which detail the most frequent types of operations (like file create, read, or write) over a selected period, including the trend over that time

The dashboard provides a quick and easy way to check capacity trends, data age, and file activity that might indicate malicious activity.

Data Age Analytics

File Analytics provides an extension called data age analytics to the data age widget on the dashboard. Data age analytics shows you how frequently users access your data over time ranges that you define. Once you customize the data age ranges to match your requirements, data age analytics shows you the hot-, warm-, or cold-data trends over the specified time, such as the last week, month, or a longer interval. You can also see the growth percentage of a given category in your designated range.

Audit Trails

With audit trails, you can search for a specific file or user to find all file- or user-related activity during a given time period. You can search for a specific file or user based on wildcards. The frequency and types of operations by users and against files, including the time they occurred, are displayed over your specified time period. You can further filter the audit trail based on operation type, such as open, read, write, delete, and other events.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 632

Search user and file activity to monitor access activity against sensitive data. You can also download the queried activity to a JSON- or CSV-formatted file for further reporting activities.

Anomaly Detection

With File Analytics, you can define anomaly alerts that represent specific operations as run by an individual or against the file server as a whole.

You can configure anomaly detection in the following ways:

- Specify anomaly events, such as permission changes, permission denials, file deletes, and file creates.
- Define an operation percentage and operation count as a part of the alert.
- Set the interval for when alert thresholds apply to the operations in question.
- Specify email recipients for anomaly event alerts.

The minimum operation percentage is based on the number of files. For example, if you have 1,000 files and define a minimum operation percentage of 5 percent, the defined event (such as create or delete) affected 50 files within the specified interval.

As anomaly events occur, the email addresses defined in the anomaly rule receive detailed information. You can also monitor each anomaly alert and track it over time with the usage anomalies dashboard. The dashboard shows you the users who caused the anomalies, the folders affected by the anomalies, the types of anomalies, and trends.

Strange access patterns that trigger anomalies can indicate malicious user, virus, or ransomware activity. Seeing this activity and being alerted in real time can help you stop these operations and better understand user access patterns across your organization.

Ransomware Intelligence

Ransomware is a persistent concern that requires multiple security controls and software layers to mitigate. Nutanix Files has long supported centralized antivirus scanning through Internet Content Adaptation Protocol (ICAP) with security vendors like Trend Micro, McAfee, BitDefender, and Symantec. Nutanix offers a comprehensive approach to ransomware threat mitigation across our portfolio of products. For more information, see our Ransomware Threat solution brief.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 633

To effectively respond to ransomware, a solution must provide the following protections:

- Prevent the infiltration of ransomware and malware
- Detect any infection attempts
- Alert the organization and initiate defensive measures
- Provide a comprehensive strategy for recovery, if necessary

Nutanix Files and File Analytics have many of the core features required to help detect, protect, analyze, and recover from ransomware. File Analytics combines these technologies into a comprehensive interface, built so that you can manage your ransomware strategy with Nutanix Files.

Ransomware protection starts with a dedicated dashboard in File Analytics that summarizes any detected vulnerabilities, including potentially compromised shares and clients. The dashboard also shows whether your shares are protected with Self-Service Restore (SSR) snapshots. You can enable SSR against the unprotected shares from this interface.

Nutanix Files can block file creation or rename operations for specific file names and extensions, including support for wildcards. When you enable ransomware protection in File Analytics, Files automatically adds the names and extensions of known ransomware variants to the blocking list. If anyone attempts a file creation or rename event involving these blocked file types, the event appears as a vulnerability that Files reports in the dashboard and emails to the designated users.

Custom Reporting

File Analytics captures real-time user audit data and file metadata for Nutanix Files environments. With File Analytics, you can mine this data more effectively by introducing a custom reporting page, so you no longer need to rely on the information available on the dashboard or through audit search.

When creating a new report, you first select an entity, such as files, folders, audit events, or users. You can then choose which attributes to filter with customizable values. For example, you can choose attributes like file size greater than or less than a given value, file age based on access time or creation date, or all audit events within a given time range. Finally, you can choose which columns of data to include in the report, like user

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 634

and file names, paths, clients, operation types, and other details associated with the entity.

Once you define the report, you can save it and run it again at any time.

Nutanix Data Lens

Nutanix Data Lens is a software as a service (SaaS) data security solution offering ransomware resilience and data analytics for unstructured data on Nutanix Cloud Platform. Data Lens offers global data visibility to proactively assess and mitigate data security risks by identifying anomalous activity, auditing user behavior, and adhering to compliance requirements while enabling efficient data life-cycle management. Along with providing the capabilities of File Analytics, Data Lens provides more robust ransomware protection, permissions monitoring, and tiering management.

Nutanix Data Lens centralizes information from all your clusters connected to Nutanix Pulse across various datacenter locations. Using cloud resources eliminates scaling constraints, allowing you to analyze an unlimited number of files and objects and unlimited amounts of data. For more information, see the Nutanix Data Lens tech note.

Smart Tier

Administrators with large Network Attached Storage (NAS) environments frequently look for ways to improve storage efficiency, simplify administration, and decrease cost. Nutanix Files provides a native tiering framework called Smart Tier to address these requirements. With Smart Tier, you can move cold or rarely used data to lower-cost storage while maintaining a single namespace. You can tier data to any qualified S3 API–compliant target, including on-premises solutions or the public cloud. Smart Tier also supports Azure Blob storage. Smart Tier helps hybrid multicloud environments handle unstructured data to retain long term, save money, or use a virtually limitless pool of local storage for your Nutanix Files workloads.

Smart Tier Architecture

The Nutanix Files tiering engine uses APIs over HTTPS to accept tiering and recall requests and to move data to Azure Blob or S3-compliant targets. Multiple targets are validated for tiering, including:

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 635

- Nutanix Objects
- Azure Blob
  - › Hot
  - › Cool
- Amazon S3
  - › Standard
  - › Infrequent Access (IA)
  - › Glacier Instant Retrieval (IR)
- Wasabi Cloud Storage

When you tier files, Nutanix Files maintains the file metadata while it moves the data to the target.

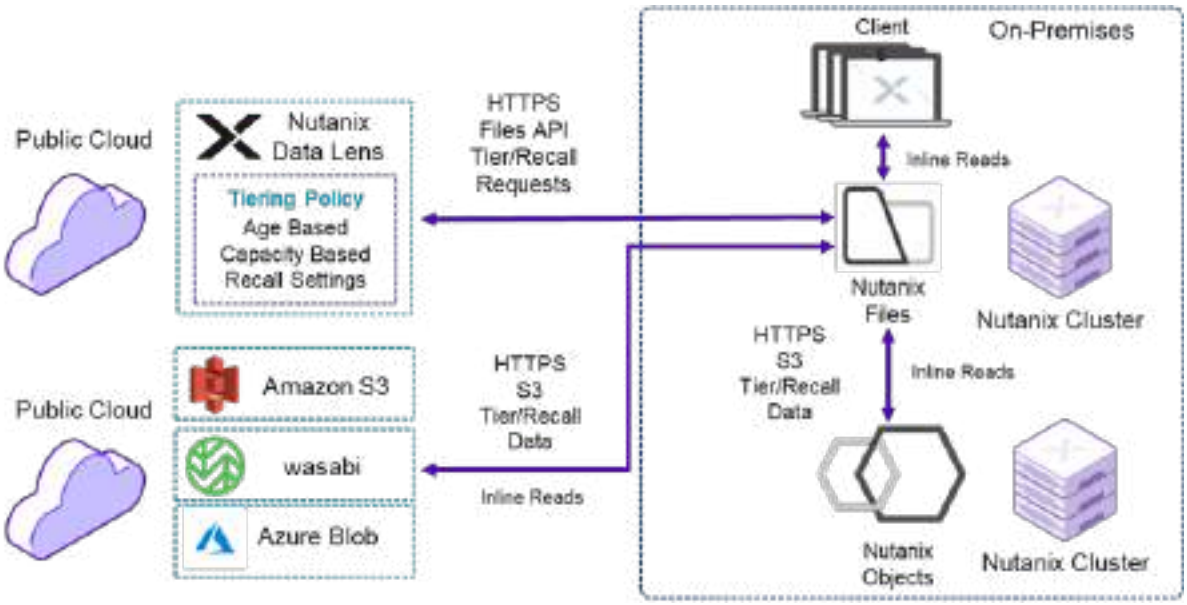


Figure 18: Smart Tier Architecture Example with Data Lens

Smart Tier maintains a file stub in the SMB or NFS share path where clients can perform inline reads to access the data. You can also recall files automatically, based on access patterns, or with manual recall operations. You can configure tiering policies and set

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 636

age- and capacity-based thresholds, manual or automatic tiering schedules, and recall settings.

Standard vs. Advanced Tiering

Standard tiering uses the Nutanix Files console local to the file server and requires no additional software or licensing. Standard tiering also supports manual or automatic tiering operations, inline reads of tiered data, setting a capacity threshold, defining the age and size of the files to tier, and manual recall operations at the share level.

Nutanix Data Lens manages advanced tiering, which supports the same functions as standard tiering but includes filtering by file type and owner and more granular recall operations at the file, folder path, or share level. Additionally, advanced tiering provides automatic recall based on access frequency along with share-level data age and file analytics.

Both standard and advanced tiering support the same tiering targets mentioned previously.

Smart Tier Configuration Using Data Lens

To configure Smart Tier, follow these steps:

1. Define a tiering location.

   The tiering location must be a supported S3-compliant target.
2. Configure the following components for your location:
   - Target URL over HTTPS
   - Bucket name
   - Access and secret keys
   - Retention period
   - Certificate (optional)

     The retention period determines when Nutanix Files deletes a tiered object after removing the stub from the file system.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 637

3. Define a capacity threshold and when-to-tier policy.

   The capacity threshold represents the percent of allocated space consumed before the system considers tiering. You also define whether the system performs the tiering policy manually or on an automated basis, and the time windows in which automated tiering occurs.
4. Define the formal tiering policy items:
   - Age of the data (based on the last file read or write operation)
   - Minimum file size (64 KB or larger)
   - Shares to exclude from the policy
   - Automatic recall settings

   When defining the automatic recall settings, you must determine whether to recall files automatically or manually and under what conditions (specifically, the number of times the file is accessed over a given period). If you choose to recall files manually, Data Lens lets you search for and choose individual files, folder paths, or shares to recall.

Tiered Data

When data reaches the configured age and the file server is at its capacity threshold, Smart Tier moves file data to the target. Smart Tier marks the previously consumed space as free, creating additional space in the share for new or recalled data.

Tiered files appear as regular files in their folder paths. SMB shares have an offline attribute set, which in Windows Explorer shows an X beside the file icon.

You can see the file size (size on disk), which represents just the metadata, and the actual file size, which represents the tiered data. You can retrieve the data inline (or read) from tiered files at any time, but you can't write to a tiered file directly. You need to either recall the file or make a separate copy to edit it.

Data Lens Advanced Ransomware Protection

Data Lens provides ransomware protection exceeding what File Analytics offers, as outlined in the Ransomware Intelligence section. Data Lens applies a file blocking list of over 5,600 signatures to the file server, providing more comprehensive protection.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 638

Data Lens can also detect new variants to help stop unknown exploits. For unknown variants, Data Lens looks at incoming audit events and applies algorithms to detect any suspicious event patterns. For example, ransomware attacks typically follow common patterns:

- Read, overwrite (encrypt), rename files, and repeat
- Read, write (encrypted new file), and delete

Data Lens looks for these various patterns and, once detected, inspects the mime type of the file. If the mime type reflects a potentially encrypted file, Data Lens marks the pattern as a ransomware attack.

In addition to setting up attack alerts, you can configure Data Lens to block users and clients from accessing a file share when a ransomware attack is detected. Blocked users or clients remain blocked until an administrator in the environment decides to unblock them.

Data Lens also provides a list of files affected by an attack. You can export that list and use it for reporting or remediation purposes. Data Lens gives a recommended snapshot for recovery, where you can perform a surgical restore using the provided file list, or use a one-click restore of the entire share.

Hypervisor-Specific Support

Nutanix supports ESXi and AHV for Files. For ESXi support, you need vCenter credentials to deploy Nutanix Files and to create DRS rules to keep the FSVMs on different nodes. You must register vCenter with the Nutanix cluster instances where you deploy Files. The deployment process generates the DRS rules for AHV automatically.

Data-at-Rest Encryption

Nutanix Files supports data-at-rest encryption (DARE) with self-encrypting drives (SEDs) or software-defined DARE using Nutanix AOS.

For AHV, you enable software encryption at the cluster level. For ESXi, you enable software encryption at either the cluster level or the storage container level. To enable storage container–level software encryption with Nutanix Files, you must use nCLI:

```
<ncli> storage-container edit enable-software-encryption=true
 name=<Files_Container_Name> force=true
```

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 639

3. Backup and Disaster Recovery

Following modern data protection methodologies, Nutanix provides quick restore access using Self-Service Restore (SSR) and site recovery with Smart Disaster Recovery and Nutanix-based snapshots.

Self-Service Restore

You can enable SSR at any time for SMB or NFS shares. The Windows previous version feature in each folder exposes SSR for SMB shares. SSR for NFS shares is exposed as a hidden snapshot directory in each folder.

SSR allows you to view snapshots of shares while the share is in use. The share snapshots are read-only, point-in-time copies.

You can view and restore removed or overwritten files, which means that you can choose a share snapshot from the same file at different times during the file's history. You can configure a snapshot schedule at the file-server level that applies to all shares in the file server. Nutanix Files supports 24-hour, daily, weekly, and monthly snapshots on a fixed schedule. The default snapshot policy includes:

- Hourly (24 per day)
- Once daily for seven days
- Four weekly
- Three monthly

You can configure a maximum of 50 total snapshots in the SSR schedule.

You can change the snapshot frequency to suit your requirements, including shorter intervals for same-day protection against accidental deletions. You can enable SSR during or after share creation. After share creation, you can change the current settings using the share update workflow feature. SSR supports both standard and distributed SMB shares.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 640

Nutanix Files version 4.4 introduces one-click, share-level restoration of the SSR snapshots. With share-level restores, you can revert an entire share to a previous point-in-time.

Asynchronous Protection Domains and Consistency Groups

Nutanix provides integrated, automated disaster recovery between Nutanix clusters. A Nutanix Files cluster can be protected with Prism and uses the same asynchronous replication with protection domains and consistency groups as any other Nutanix cluster.

A protection domain is a defined group of entities (VMs and volume groups) that you back up locally on a cluster and can replicate to one or more remote sites. A consistency group is a subset of the entities in a protection domain. Consistency groups are configured to snapshot a group of VMs or volume groups in a crash-consistent manner.

Use AOS node sizing guidelines when you determine your recovery point objective (RPO) requirements. Nutanix Files supports both asynchronous (RPO of one hour or longer) and NearSync (RPO down to one minute) schedules.

When you create a file server, Nutanix Prism automatically sets up a corresponding protection domain, which it annotates with the Nutanix Files cluster name. Prism also creates multiple consistency groups in a protection domain, including a group that includes all FSVMs.

Once you protect Nutanix Files, all future operations on it (such as adding or removing FSVMs or adding or deleting volume groups) automatically update the corresponding consistency group in the protection domain.

Cluster Migration, Failure, and Restoration

In the event of a Nutanix Files cluster failure, restore Files in a remote cluster by initiating the Activate workflow, which restores from the last good snapshot. If you're moving your file services because you need to shut the cluster down, as with a planned outage, the Migrate workflow shuts down all the FSVMs and takes a final snapshot for replication. You run the Migrate workflow from the Nutanix cluster that owns the active protection domain. You initiate both the Activate and Migrate workflows from the Data Protection menu in Prism.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 641

After you run either the Activate or Migrate workflow, you must activate the file server instance, which you can do from the File Server menu in Prism. Activating the file server might require you to configure network VLANs on the replica site before Nutanix Files becomes operational again. These VLANs can be in subnets that are the same as or different from the source site. The recovery process is like creating the file server, but in this context, you can change networks and IP addresses if necessary.

Cloning

Because Nutanix Files cloning doesn't affect the original Files cluster, it offers improved support for the following use cases:

- Backups at the primary and secondary sites
- Disaster recovery at the secondary site
- File server recovery from a specific point in time
- File server creation at the primary or remote site for testing or development
- File server clone copies

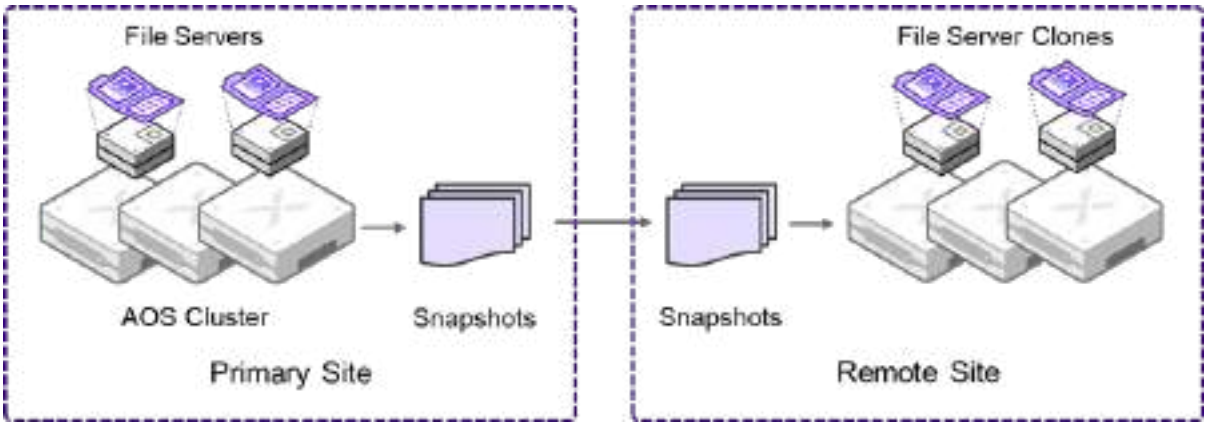


Figure 19: Nutanix Files Cloning Use Cases

Files uses Nutanix native snapshots to clone entire file servers. The clone is a thin copy that consumes minimal storage space. File server clones reside on the same container as the original and maintain the original security permissions. During the clone process you can specify new IP addresses and give the cloned file server a new name.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 642

Metro Availability

Files 4.4 introduces Metro Availability support for Nutanix Files environments. Metro Availability includes synchronous replication, which ensures file server writes are committed to both Nutanix clusters before acknowledgement, providing an RPO of zero. You can also automate failover between sites using a witness. When a failure is detected on one side of the relationship, the file servers are automatically restarted on the other cluster.

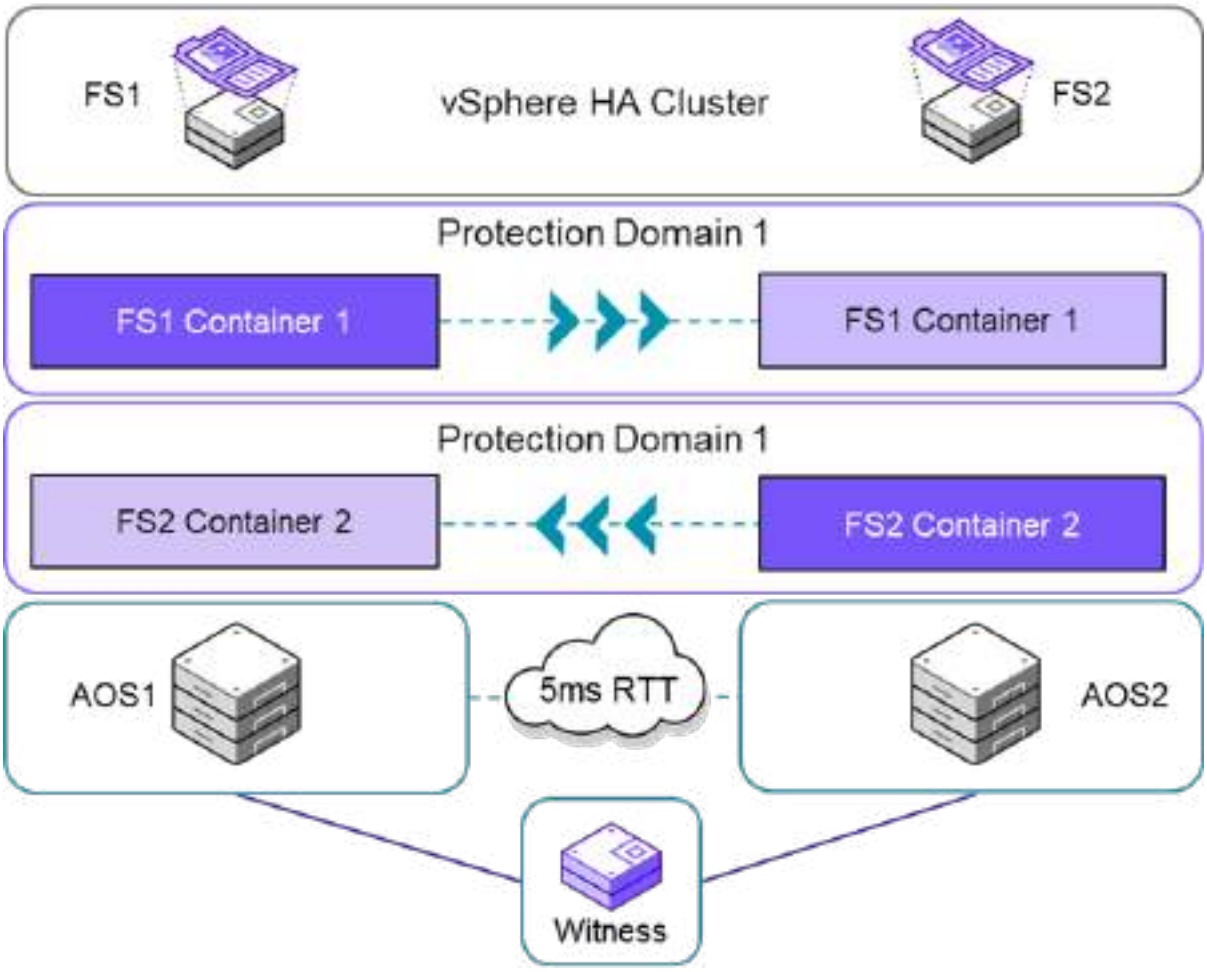


Figure 20: Nutanix Files in a Metro Configuration

Nutanix Files currently supports Metro Availability, including synchronous replication and automated failover, when using ESXi with VMware vSphere.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 643

Files Smart Disaster Recovery

In the past, Nutanix Files relied on the core snapshot and remote replication capabilities of Nutanix AOS. Using AOS had several benefits, including simplified and consolidated administration that aligned with the core hyperconverged infrastructure (HCI) environment. But it also included some drawbacks around granularity, node density, and the active-passive nature of share access and failover orchestration. Files Smart Disaster Recovery (Smart DR) helps address these challenges while maintaining the same simple and consolidated administrative experience. You can configure and manage Smart DR from Files Manager in Prism Central.

Smart DR changes several key areas of Nutanix Files remote replication. First, the AOS clusters no longer manage the replication engine using native Nutanix protection domains; instead, Nutanix Files manages replication directly. As with Files Self-Service Restore (SSR), Smart DR takes snapshots at the share (or file-system) level, replicating block-level incremental changes between source and target.

Replication occurs between active file servers running on their respective Nutanix clusters. Shares that function as replication targets are available in a read-only state. Replicating between active file servers helps shorten failover times, reduce your recovery time objective (RTO), and simplify using replicated data for backup consolidation or reporting.

Because Nutanix Files now manages replication, the node-density limits specific to AOS snapshots and replication no longer apply. You can now use our most storage-dense nodes with the benefits of native remote replication.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 644

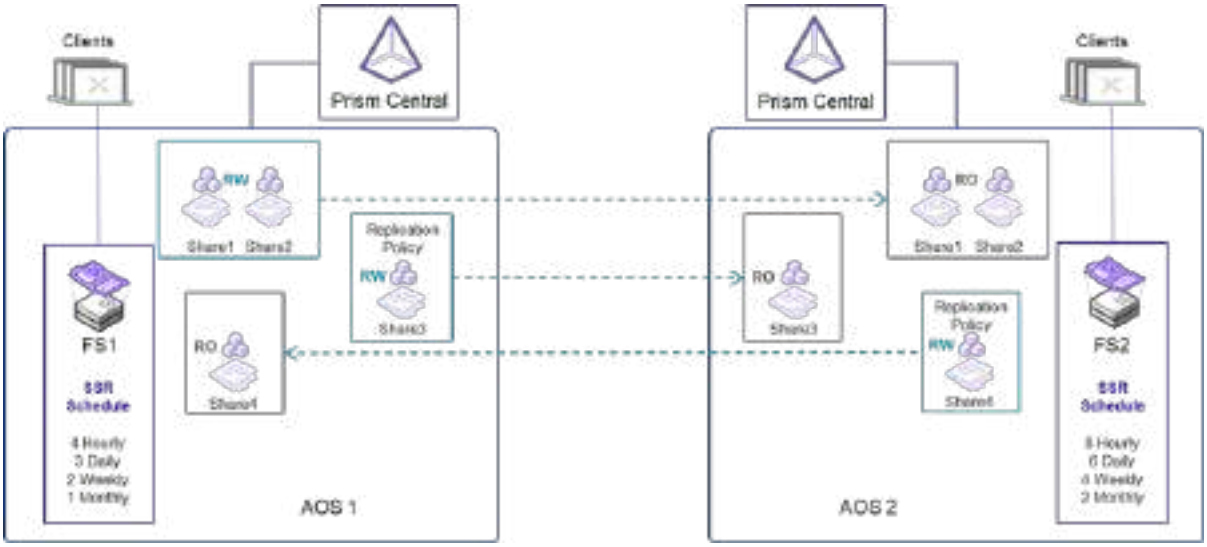


Figure 21: Files Smart DR

For the file systems that support the shares performing replication, you can now set policies on a share-by-share basis to manage your RPO at the share level instead of at the file server level. With Files version 4.4, the source and target file servers can be on AOS clusters registered to different Prism Central instances.

Replication Policies

A replication policy defines the share or group of shares you want to replicate. The policy also defines the source and target file servers and the replication frequency. You can create multiple policies as needed and specify a default policy for any newly created shares.

You can configure your replication schedule to be as short as one minute.

Monitoring

Files Manager in Prism Central provides SLA monitoring and job replication status at several levels. You can use the RPO compliance overview provided on the Data Protection Summary page to quickly understand if replication is keeping up with the defined policy.

You can also view each replication job to monitor its completion percentage, start and end times, amount of data synchronized, and average network bandwidth usage.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 645

Failover and Failback

You can manage planned or unplanned failover and failback from Prism Central. During failover operations, Prism Central orchestrates the required updates to the DNS and Active Directory service principal names (SPNs) to move the file server instance name from the source to the target.

With a planned failover, you can choose to begin replicating in the opposite direction automatically. Replicating after failover helps maintain service level agreements (SLAs) and RPOs during your failover testing or disaster avoidance operations.

Self-Service Restore Interoperability

With Nutanix Files 4.0, Smart DR supports replicating the snapshots between the source share and its target. The target share retention schedule doesn't have to match the source retention schedule. For example, if you configured the source file server to maintain the last two hourly snapshots, you can configure the target file server to maintain the last ten hourly snapshots, providing a longer retention window. Alternatively, you can match retention schedules to ensure that the same SSR copies exist in both sites for any failover event.

SSR schedules must have the same frequency type between the source and target. For example, if your daily snapshots are scheduled on your source, you must schedule daily snapshots on your target for them to be replicated and retained.

Files Smart DR Summary

Files Smart DR is an intelligent, simple, and effective way to replicate between Files instances, either on-premises or running on Nutanix Cloud Clusters on AWS or Azure.

In summary, Files Smart DR gives you the following advantages—all while maintaining easy, streamlined administration for your Nutanix environment:

- Prism Central integration
- Share-level replication policies
- Replication to an active read-only file server target
- Faster RTOs
- Support for storage-dense nodes

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 646

- SSR compatibility

Data Synchronization

Data synchronization through Smart Sync provides folder path–level asynchronous replication between Nutanix Files instances. You can achieve data synchronization through data consolidation and the Virtual Desktop Infrastructure (VDI) Sync feature.

Data Consolidation

Data consolidation allows you to replicate from multiple file server paths to a single target path for many-to-one replication. Both the source and target path are readable and writable. Changes within a source file will overwrite changes to the same file on the target. Replication can be specified down to 1-minute intervals.

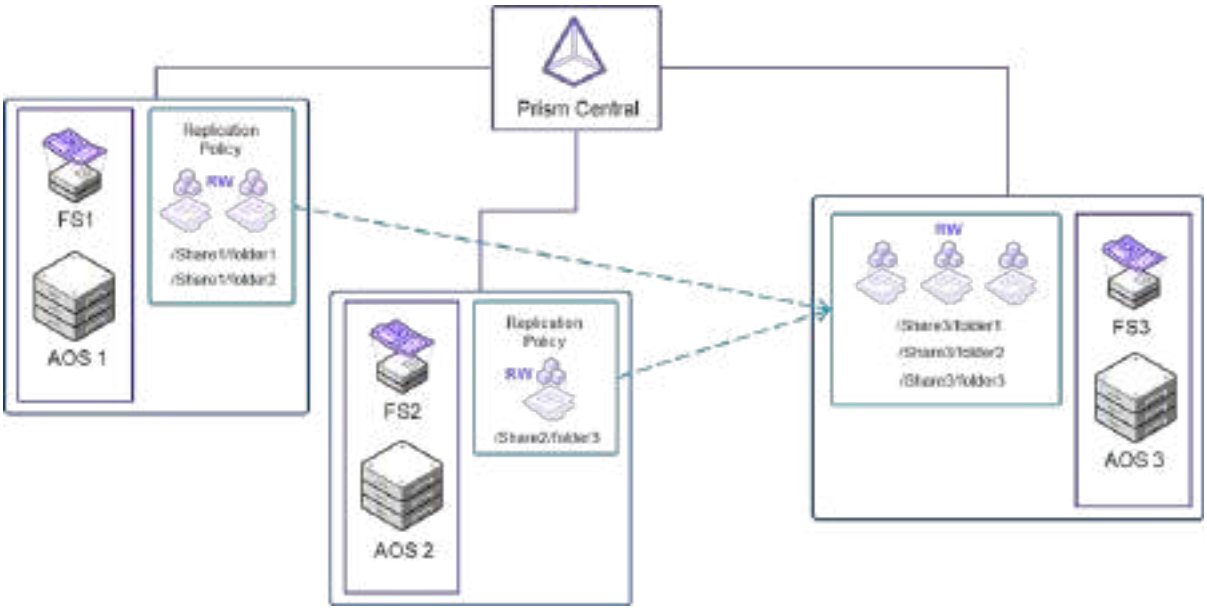


Figure 22: Data Consolidation Overview

You can optionally choose to exclude directories or file extension patterns from replication, allowing you to store only what's needed on your target system. Further, you can choose to not replicate delete operations, which is helpful if your goal is to consolidate data on a target while freeing space on a source system.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 647

For consolidation use cases, you can configure data synchronization through Files Manager in Prism Central to copy files from multiple sites to a single location for retention or centralized backup.

VDI Sync

VDI Sync replicates user profiles between file servers, enabling users to access their data locally based on where their VDI session resides. If a user travels between sites, they can access their user profile local to that site. VDI Sync is an active-active solution, meaning that both the source and target of replication are readable and writable and changes are replicated in both directions.

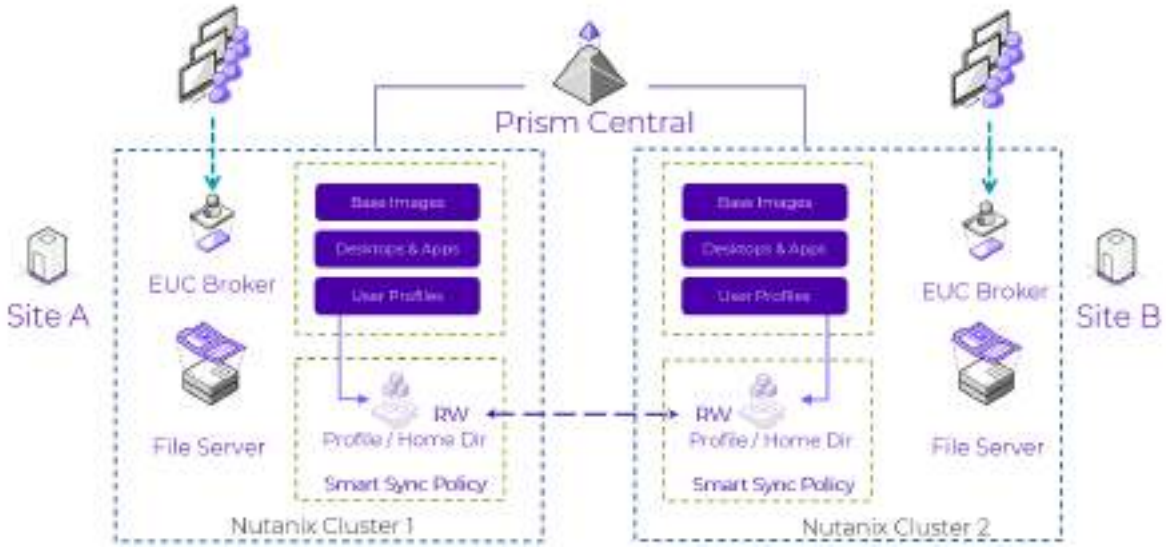


Figure 23: VDI Data Sync Overview

VDI Sync works by asynchronously replicating data between a source and target distributed share across two file servers. When a user connects to their profile on one of the file servers, the logon session is detected. That same user isn't allowed to connect to the peer file server. When the user disconnects their session and final replication is complete, they can connect to the other file server. Site-dependent connectivity is driven by the VDI broker configuration.

VDI Sync is not intended for collaboration use cases, where multiple users access and update replicated copies of the same data. It is intended for data accessed by the same user.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 648

4. Third-Party Integration

You can use third-party products with the Nutanix Files API for the following solutions:

- Antivirus protection
- File operations monitoring
- Backup

Antivirus

To protect users from malware and viruses, you need to address both the client and the file server. Nutanix currently supports third-party vendors that use Internet Content Adaptation Protocol (ICAP) servers. ICAP, which is supported by a wide range of security vendors and products, is a standard protocol that allows you to integrate file and web servers with security products. Nutanix chose this method to give customers wide latitude in selecting an antivirus solution that works best for their specific environments.

The following workflow is for an ICAP-supported antivirus solution:

1. An SMB client submits a request to open or close a file.
2. The file server determines if the file needs to be scanned, based on the metadata and virus scan policies. If a scan is needed, the file server sends the file to the ICAP server and issues a scan request.
3. The ICAP server scans the file and reports the scan results to the file server.
4. The file server takes an action based on the scan results:
   - If the file is infected, the file server quarantines it and returns an access denied message to the SMB client.
   - If the file isn't infected, it returns the file handle to the SMB client.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 649

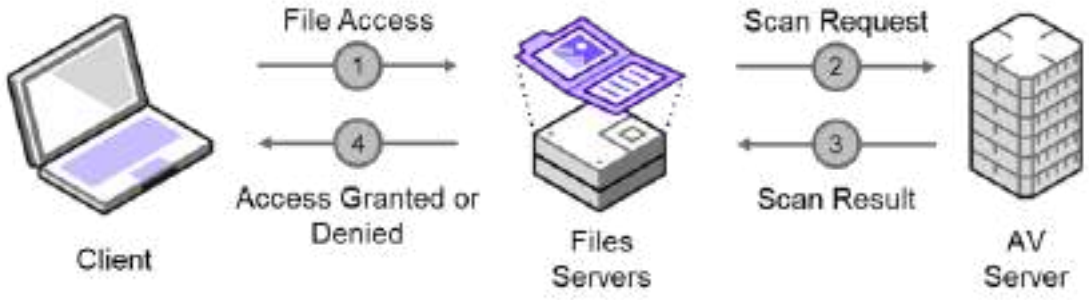


Figure 24: ICAP Workflow

The ICAP service runs on each Nutanix Files file server and can interact with more than one ICAP server in parallel to support scaling out the antivirus server. The scale-out nature of Nutanix Files and one-click optimization greatly mitigate any antivirus scanning performance overhead. If scanning affects Nutanix Files FSVM performance, one-click optimization recommends either increasing the virtual CPU resources or scaling out the FSVMs. This feature also helps both the ICAP server and Files scale out, ensuring fast responses from the customer's antivirus vendor.

We recommend configuring two or more ICAP servers for production.

Nutanix Files sets scanning defaults across the entire file server. You can enable scan on write and scan on read. Scan on write begins when the file is closed, and scan on read occurs when the file is opened. You can also exclude certain file types and sizes. Share scan policies can override any defaults set for the file server.

For each ICAP server, Nutanix Files spins up no more than 10 parallel connections per FSVM and randomly distributes the file scanning among all the ICAP servers. With heavier workloads, which might involve many scan requests and use all connections, you can give the scan servers more processing power to scan more files. As soon as the current scan finishes, the scan server picks up the next file from the queue, which keeps the number of active connections at 10.

Once Nutanix Files quarantines a file, the administrator can rescan the file, remove it from quarantine, or delete it. You can search quarantined files if you need to restore a file quickly.

If your antivirus vendor doesn't support ICAP, you can scan the shares by installing an antivirus agent on a Windows machine, then mount all the shares from the file server. With this approach, you can schedule scans for periods of low usage. At the desktop or

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 650

client level, you can set your antivirus solution to scan on write or scan only when files are modified. You can configure high-security environments to scan inline for both reads and writes.

For the latest list of qualified ICAP server vendors with Nutanix Files, see the Compatibility and Interoperability Matrix on the Nutanix Support portal.

File Operations Monitoring

File operations monitoring is a native Nutanix Files API used to forward all SMB and NFS operations run by clients to a registered target repository.

File operations monitoring can be broken down into two major areas for third-party vendors:

- File activity
- Audit

Partner software can register with the Nutanix Files instance to capture file activity events. Partner software can also make REST calls to Files to create a policy that defines the file notification types to receive and from which shares to receive them. The partner software uses a web client and communicates with the Nutanix Files file server using HTTPS requests. The HTTPS communication relies on SSL authentication. The HTTP server runs with either its unique self-signed SSL certificate or a Transport Layer Security (TLS) connection with the partner, exchanges the keys between the two parties, and sends messages to the partner server over this secure channel.

Third-party software can use different protocol communication methods such as syslog, Google, or Kafka protobuf. One common way to use the Nutanix file operations monitoring API is to forward events to a syslog server for any future auditing needs. The following vendors are integrated with this operations monitoring API:

- Peer Software: Includes the file operations monitoring API to support active-active deployments with real-time replication and file locking between heterogenous environments. For more information, see the PeerGFS and Nutanix Files datasheet.
- Netwrix: Provides comprehensive visibility into changes and data access across Nutanix Files instances. Netwrix offers an add-on for Nutanix Files. For more information, see the Netwrix website.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 651

- Varonis: Version 8.6 introduces support for Nutanix Files version 3.7.1 and later. This support includes Varonis' entire platform, DatAdvantage, DatAlert and DatAlert Analytics, DataPrivilege, Data Classification Engine, DatAnswers, Automation Engine, and Data Transport Engine.

Intelligent Backup

Traditional NAS backup approaches like Network Data Management Protocol (NDMP) are limited. Problems like complexity, performance (including the need for periodic full backups), and scale led Nutanix to develop a more modern backup solution: a changed file tracking (CFT) API for third-party backup vendors. This API shortens backup times because it doesn't perform a metadata scan across your file server, which might contain millions of files and directories. The CFT API promotes scalability, as backups can occur across multiple FSVMs in parallel. It also ensures that customers aren't locked into any one solution, because backups taken using the Nutanix Files API can be restored to other vendors.

CFT uses internal snapshots to track differences between backup windows. The backup software vendor requests the creation of these snapshots, and Files returns a list of the changed files in the form of a share. The backup software mounts the share onto the backup server to be read for backup.

Nutanix Files and a third-party backup vendor complete the following high-level steps to produce CFT backups:

1. The backup server takes a snapshot.
2. The backup server requests the differences between the current and previous snapshot.
3. The Nutanix Files server sends the differences as a share.
4. The backup server mounts the share and reads the changed files.
5. The backup server writes the changed data to the backup target.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 652

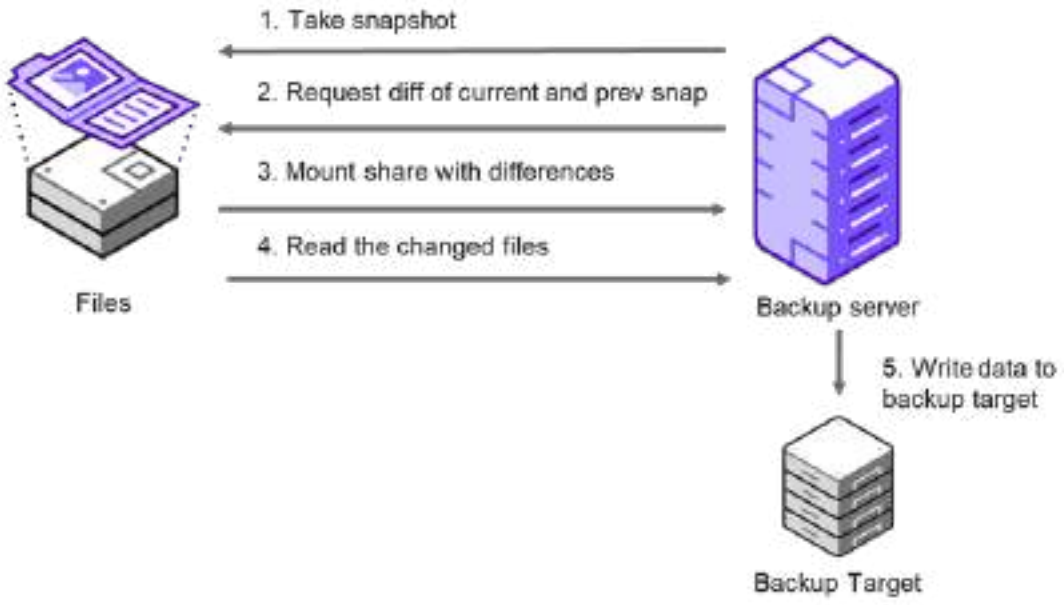


Figure 25: CFT Backup Process

Backup software can specify multiple shares and their respective snapshot information. Nutanix Files returns the list of URLs that map to the number of client streams that can start in parallel. Because shares are distributed evenly across the FSVMs based on load, the backup software can take advantage of all the FSVMs to drive throughput.

Multiple software vendors are integrated with the Nutanix Files CFT API, including:

- HYCU Backup and Recovery
- Commvault, version 11, service pack 15 (as of CFT API release 3.5)
- Veritas Netbackup 9.1
- Veeam 12

You can back up Nutanix Files shares with software that doesn't support CFT. One option is to run the backup application on a Windows machine and map the UNC path of the share as a drive to be backed up. Some vendors provide support for backing up file shares without mounting to a guest VM. These applications can read directly from the UNC path. For the full list of validated backup applications, see the Compatibility and Interoperability Matrix.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 653

Note: Don't try to back up the FSVMs. FSVMs are stateless, and data is stored in Nutanix volume groups. Back up Nutanix Files from the share level. You can protect FSVMs using Nutanix protection domains.

Because the system spreads different standard shares across the cluster, try to back up multiple shares at the same time with multiple subclients. The distributed share allows you to configure multiple data readers to drive throughput.

In the following example of backup using Commvault, we tested 400 users spread out on three FSVMs, placing the data on a home share. The Commvault backup job completed with the following results:

- Average throughput: 559.92 GB per hour
- Elapsed time: 5 minutes and 26 seconds
- Transfer time: 4 minutes and 19 seconds
- Number of files transferred: 57,147
- Failures: 0 (files and folders)
- Skipped files: 0
- Application size: 40.26 GB
- Data transferred on network: 118.95
- Compression: 49.90%

We found that adding more readers for the backup job can increase performance. The bottleneck was the media agent, which was the backup destination for the files. The media agent was virtualized and configured with only 8 vCPU. Increasing the media agent's vCPU shortened the backup time.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 654

5. Conclusion

Nutanix Files delivers on-demand performance and automated provisioning to provide highly scalable file management. It reduces the administration and configuration time needed to deploy and maintain your environment, providing a public cloud experience within your private cloud.

Nutanix storage and Prism make hosted file services highly resilient and easy to use—for example, you can configure the native data efficiency features of AOS, such as erasure coding (EC-X), for each individual file server. With Prism, you can administer network and resource management, Active Directory, fault tolerance, and Nutanix Files share and export management all in one place, vastly improving operational efficiency.

File Analytics gives you deep insight into your data, including storage consumption trends, file sizes, file counts, and data age. Analytics also provides end-to-end audit trails and anomaly detection. Data Lens uses advanced ransomware intelligence to detect, protect against, analyze, and recover from ransomware threats.

Because you can deploy Files in a new or existing Nutanix environment and in environments that are dedicated or mixed with other services, you can choose the architecture to take advantage of Files services. You can further deploy Files in the public cloud, either within NC2 environments or natively in AWS.

Nutanix Files streamlines design, implementation, and maintenance, providing an unrivaled experience for key use cases like end-user computing, video capture, medical imaging archives, application data, and the many other projects that store data in shared environments.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 655

About Nutanix

Nutanix offers a single platform to run all your apps and data across multiple clouds while simplifying operations and reducing complexity. Trusted by companies worldwide, Nutanix powers hybrid multicloud environments efficiently and cost effectively. This enables companies to focus on successful business outcomes and new innovations. Learn more at Nutanix.com.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 656

List of Figures

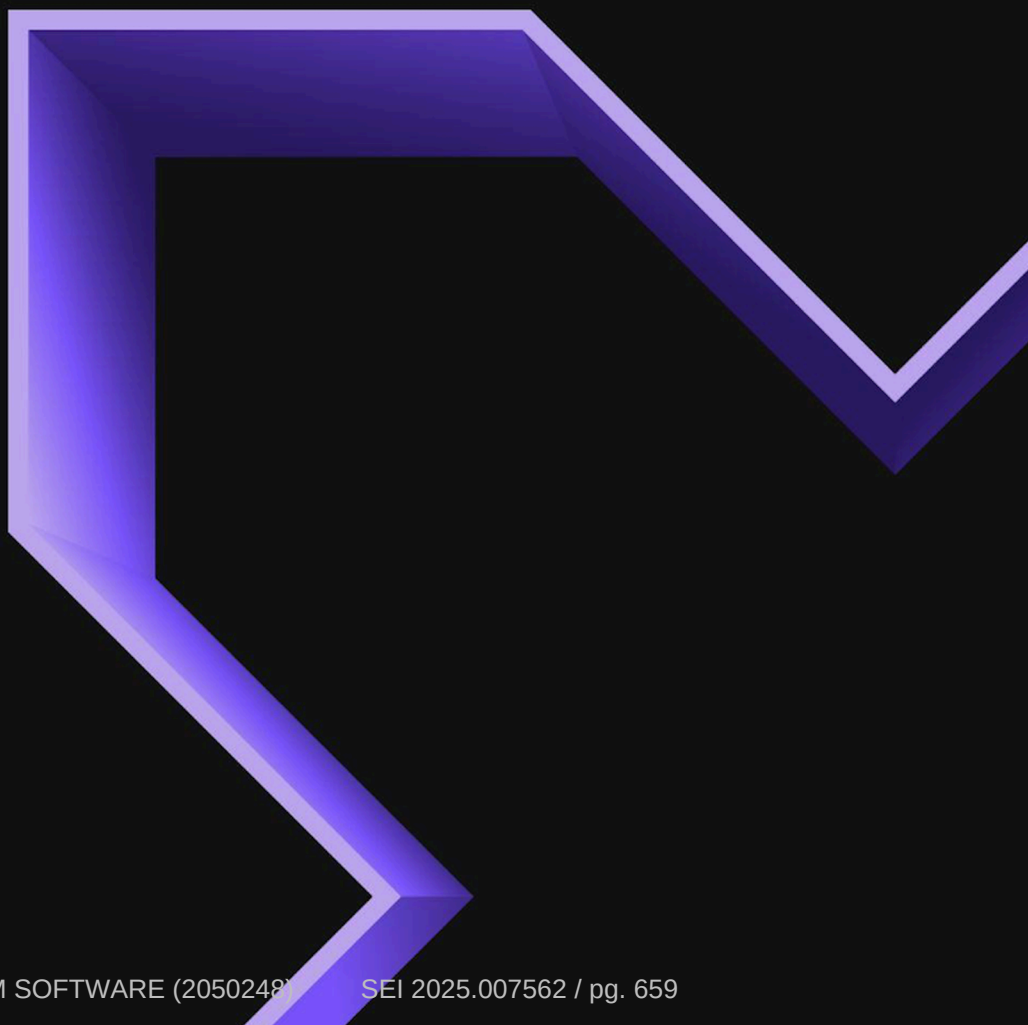
Figure 1: Nutanix Files Instances Run as VMs.... 8
Figure 2: Data Path Architecture of Nutanix Files.... 9
Figure 3: FSVM Internal Communication on One Node.... 10
Figure 4: Multiple Client Networks with Common and Unique Shares.... 12
Figure 5: Volume Group Load Balancing.... 13
Figure 6: Initial 40 TiB File System Pool.... 14
Figure 7: Distributed Directory Shares.... 16
Figure 8: Three Standard Shares on the Same File Server.... 18
Figure 9: Create Share Menu with Nested Share Path.... 21
Figure 10: Submounting a Distributed Share into a Standard Share.... 22
Figure 11: Load Balancing Volume Groups with Nutanix Volumes.... 26
Figure 12: Nutanix Volumes High Availability for File Server Volume Groups.... 27
Figure 13: FSVM Ownership with Single Share and Volume Group Example.... 28
Figure 14: FSVM-1 Failure.... 29
Figure 15: DNS Request for SMB.... 32
Figure 16: DNS Request for NFSv3.... 38
Figure 17: Multiprotocol Shares.... 39
Figure 18: Smart Tier Architecture Example with Data Lens.... 48
Figure 19: Nutanix Files Cloning Use Cases.... 54
Figure 20: Nutanix Files in a Metro Configuration.... 55
Figure 21: Files Smart DR.... 57
Figure 22: Data Consolidation Overview.... 59
Figure 23: VDI Data Sync Overview.... 60

Figure 24: ICAP Workflow.....62
Figure 25: CFT Backup Process.....65

File Analytics Guide

File Analytics 3.3

January 9, 2025



NUTANIX

Contents

File Analytics Overview....4
- Limitations....4
- Deployment Requirements....5
  - Network Requirements....6
- Deploying File Analytics....6
  - Enabling File Analytics on Prism Element....8
  - Enabling File Analytics on Prism Central....11
  - Disabling File Analytics....11
- Launching File Analytics....12
  - Launching File Analytics from Prism Element....12

Administration....13
- File Analytics VM Management....13
  - Removing File Analytics VMs....13
  - Restarting a File Analytics VM (FAVM)....13
- Role-based Access Control for File Analytics....14
- Updating Credentials....14
- Managing Deleted Share and Export Audits....14
- Changing an FAVM Password....15
- Configuring Event Quotas....15
- Upgrades....16
  - Upgrade File Analytics on a Dark Site....16

Dashboard....18
- Health....23
- Data Age....23
  - Configuring Data Heat Levels....24

Anomalies....25
- Configuring Anomaly Detection....27
- Configuring an SMTP Server....28

Audit Trails....31
- Viewing Audit Trails....31
- Audit Trails - Users....31
- Audit Trails - Folders....33
- Audit Trails - Files....34
- Audit Trails - Client IP....36

Ransomware Protection....38
- Ransomware Protection Features....38
- Enabling Ransomware Protection....39
- Configuring Ransomware Protection....40
- Enabling Self-Service Restore (SSR)....41

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 660

Reports..... 43
Reports Dashboard..... 43
Creating a Custom Report..... 48
Create a Pre-Canned Report..... 48

File Analytics Options..... 50
Updating Data Retention..... 50
Scanning the File System..... 50
Managing the Deny List..... 50
Managing File Categories..... 51
Data Protection..... 51
Configuring Disaster Recovery..... 51
Activating Disaster Recovery..... 52
Deploying File Analytics on a Remote Site (AHV)..... 52
Deploying File Analytics on a Remote Site (ESXi)..... 54

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 661

FILE ANALYTICS OVERVIEW

File Analytics provides data and insights on the operations and contents of a file server.

Once deployed, Nutanix Files adds a File Analytics VM (FAVM) to the Nutanix cluster. A single FAVM supports up to two file servers in the cluster. You must enable File Analytics separately for each file server. File Analytics protects data on the FAVM, which is kept in a separate volume group.

> **Note:** File Analytics supports dual-NIC configuration for segmented networks. Contact Nutanix Support for assistance.

Once you deploy File Analytics, a new File Analytics link appears on the file server actions bar. Use the link to access File Analytics on any file server that has File Analytics enabled.

> **Important:** To protect data on the FAVM, Nutanix recommends setting up a protection domain with a DR policy that has a minimum frequency of one week. See Data Protection on page 51.

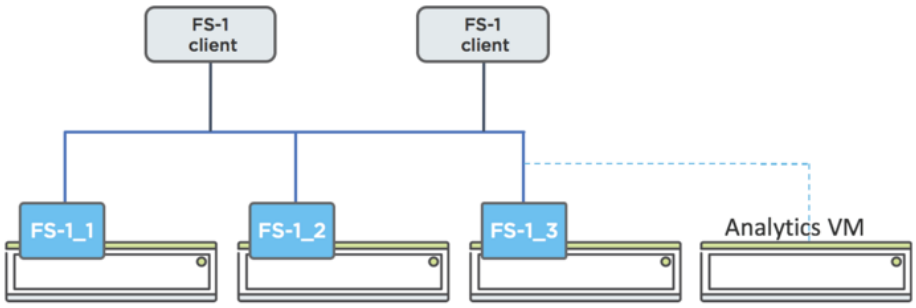


Figure 1: File Analytics VM

Features

File Analytics consists of the following salient features:

- The Dashboard includes widgets that offer overviews of file trends, data distribution, and file server operations. For more information, see Dashboard on page 18.
- Audit trails let you search for a specific user or file and view various widgets to audit activity. For more information, see Audit Trails on page 31.
- Anomalies let you create anomaly policies and view anomaly trends. For more information, see Anomalies on page 25.
- Ransomware protection lets you track ransomware events and configure self-service restore (SSR) snapshots. For more information, see Ransomware Protection on page 38.

  > **Caution:** Ransomware protection helps detect potential ransomware. Nutanix does not recommend using the File Analytics ransomware feature as an all-encompassing ransomware solution.

- Reports let you create custom reports or use pre-canned report templates. For more information, see Reports on page 43.

Limitations

Before deployment, review the list of File Analytics limitations.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 662

Depending on the data set size, file count, and workload type, enabling File Analytics can affect the performance of Nutanix Files. High latency is more common with heavy-file metadata operations (directory and file creation, deletion, permission changes, and so on).

To minimize the impact on performance, ensure that the host has enough CPU and memory resources to handle the File Analytics VM (FAVM), file servers, and guest VMs (if any). For more information on system requirements, see "System Limits" in the File Analytics Release Notes.

File Analytics has the following limitations:

- Only Prism admin can deploy File Analytics.
- File Analytics analyzes data from daily up to 1 year based on the configuration. File Analytics automatically deletes data beyond the defined configuration.

  > **Note:** After surpassing the audit event threshold, as specified in *File Analytics Release Notes*, Analytics archives the oldest events. Archived audit events do not appear in the Analytics UI.

- You cannot deploy or decommission File Analytics when a file server has high-availability (HA) mode enabled.
- You cannot use network segmentation for Nutanix Volumes with File Analytics.
- If file server DNS or IP changes, File Analytics does not automatically reconfigure.
- File Analytics does not collect metadata for files on Kerberos authenticated NFS v4.0 shares.
- File Analytics does not support hard links.
- You cannot enable File Analytics on a file server clone.
- You cannot move File Analytics to another storage container.
- File Analytics creates an unprotected Prism and an unprotected file server user for integration purposes. Do not delete these users.
- The legacy file blocking policy has an upper limit of 300 ransomware extensions.

  > **Note:** For higher limits, it is recommended to use Nutanix Data Lens.

- File Analytics does not support the following operations for graceful shutdown:
  - AHV: power cycle, turn off
  - ESXi: reset, turn off
- File Analytics log collection from CVM fails with a dual NIC setup.
- File Analytics does not collect metadata information on Keberos authenticated, offline, or encrypted shares.
- Teardown of File Analytics is unsuccessful with a dual-NIC setup.
- In CAC authentication-enabled environments, you cannot deploy or upgrade File Analytics. You can disable and re-enable CAC to perform deployment and upgrades.
- File Analytics does not support Prism Central-based Nutanix Disaster Recovery (Leap).
- See "System Limits" in the File Analytics Release Notes for more information.

Deployment Requirements

Meet the deployment requirements before deploying File Analytics.

Ensure you have performed the following tasks and your Files deployment meets the specifications.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 663

- Assign the file server administrator role to an Active Directory (AD) user. See "Managing Roles" in the *Nutanix Files Guide*.
- Log on as the admin in Prism Element to deploy the File Analytics server.
- Configure a VLAN with one dedicated IP address for File Analytics or use an IP address from an existing Nutanix Files external network. This IP address must have connectivity to AD, the control VM (CVM), and Files. See "Configuring a Virtual Network for Guest VM Interfaces" in the *Prism Web Console Guide*.

  Caution: Do not install File Analytics on the Nutanix Files storage internal network.

  Note: Do not use a 172.28.x.x subnet for the deployment, as this conflicts with the subnet for the Docker private bridge.
- (optional) Assign the file server administrator role to an LDAP user, see "Managing Roles" in the *Nutanix Files Guide*.
- Ensure that all software components meet the supported configurations and system limits. See the *File Analytics Release Notes*.

Network Requirements

Open the required ports and ensure that your firewall allows bi-directional Internet Control Message Protocol (ICMP) traffic between the FAVM and CVMs.

The Port Reference provides detailed port information for Nutanix products and services, including port sources and destinations, service descriptions, directionality, and protocol requirements.

In addition to meeting the File Analytics network requirements, ensure to meet Nutanix Files port requirements as described in the *Port Reference*.

Deploying File Analytics

Follow this procedure to deploy the File Analytics server.

Before you begin

Ensure that your environment meets all requirements prior to deployment, see Deployment Requirements on page 5.

Procedure

Deploying the File Analytics server.

1. Go to **Support Portal** > **Downloads** > **File Analytics**.
2. Download the File Analytics QCOW2 and JSON files.
3. Sign in to Prism Element (PE) with the user name and password of the Prism administrator.

   Note: An Active Directory (AD) user or an AD user mapped to a Prism admin role cannot deploy File Analytics.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 664

4. In PE, go to the **File Server** view and click the **Deploy File Analytics** action link.

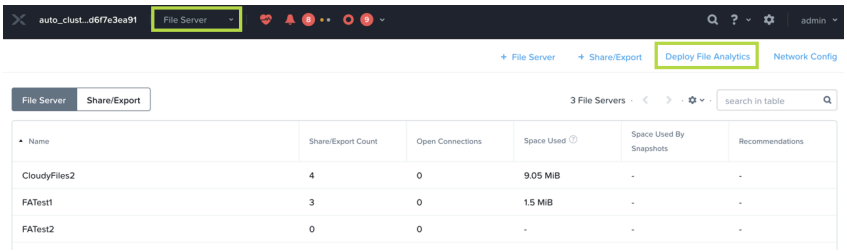


Figure 2: File Analytics

5. Review the File Analytics requirements and best practices in the **Pre-Check** dialog box.
6. In the **Deploy File Analytics Server** dialog box, do the following in the **Software Version** tab.

   » Under **Available versions**, select one of the available File Analytics versions. Continue to step 8.

   » Install File Analytics by uploading the installation binary files as described in the next step.

7. Upload installation files.

   a. In the **Upload binary** section, click **upload the File Analytics binary** to upload the File Analytics JSON and QCOW files.

Figure 3: Upload Binary Link

   b. Under **File Analytics Metadata File (.Json)**, click **Choose File** to choose the downloaded JSON file.

   c. Under **File Analytics Installation Binary** (.Qcow2) click **Choose File** to choose the downloaded QCOW file.

   d. Click **Upload Now** after choosing the files.

8. Click **Next**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 665

9. In the **VM Configuration** tab, do the following in the indicated fields:

   a. **Name**: Enter a name for the File Analytics VM (FAVM).

   b. **Server Size**: Select either the **small** or **large** configuration. Large file servers require larger storage configurations for the FAVM. By default File Analytics selects the large configuration.

   c. **Storage Container:** select a storage container from the drop-down list.
   The drop-down displays the storage containers.

   d. **Network List**: Select a VLAN.
   The FAVM must use the client-side network.
   If the selected network is **unmanaged**, enter more network details in the **Subnet Mask**, **Default Gateway IP**, and **IP Address** fields as indicated.

   > **Note:** For ESXi, do not use the Controller VM (CVM) backplane network. The CVM backplane network is not supported and any later upgrade operations might fail.

   > **Note:** Do not use a 172.28.x.x subnet for the deployment, as this conflicts with the subnet for the Docker private bridge.

10. Click **Deploy**.
    In the main menu drop-down, select the **Tasks** view to monitor the deployment progress.

Results

Once deployment process completes, File Analytics creates an FAVM and a new Files user to make REST API calls. Do not delete the FAVM, or the REST API user.

Enabling File Analytics on Prism Element

Steps for enabling File Analytics in Prism Element after deployment or disablement.

About this task

> **Attention:** Nutanix recommends enabling File Analytics during off-peak hours.

Follow these steps to enable File Analytics.

> **Note:** File Analytics saves all previous configurations.

Procedure

1. In the **File Server** view in **Prism**, select the target file server.
2. (Skip to step 3 if you are re-enabling a file server.) Click **Manage roles** to add a file server admin user. See *Managing Roles* in the *Nutanix Files Guide*.
3. In the **File Server** view, select the target file server and click **File Analytics** in the tabs bar.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 666

4. (Skip to step 5 if you are not re-enabling a disabled instance of File Analytics.) To re-enable File Analytics, click **Enable File Analytics** in the message banner.

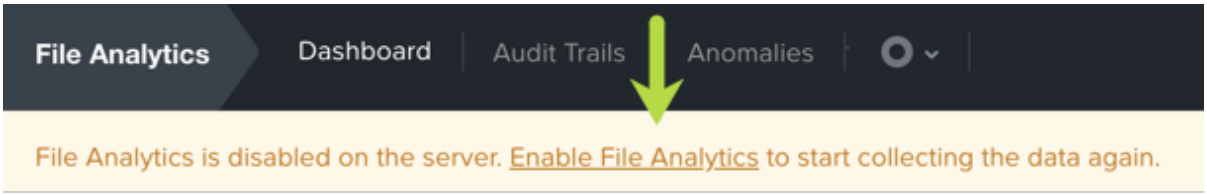


Figure 4: Enabling File Analytics Link

The **Enable File Analytics** dialog box appears. Skip the remaining steps, as the following steps are for enabling file servers that were not previously enabled.

First-Time Configuration Steps

5. In the **Data Retention** field, select a data retention period. The data retention period refers to the length of time File Analytics retains audit events.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 667

6. In the **Authentication** section, enter the credentials as indicated:

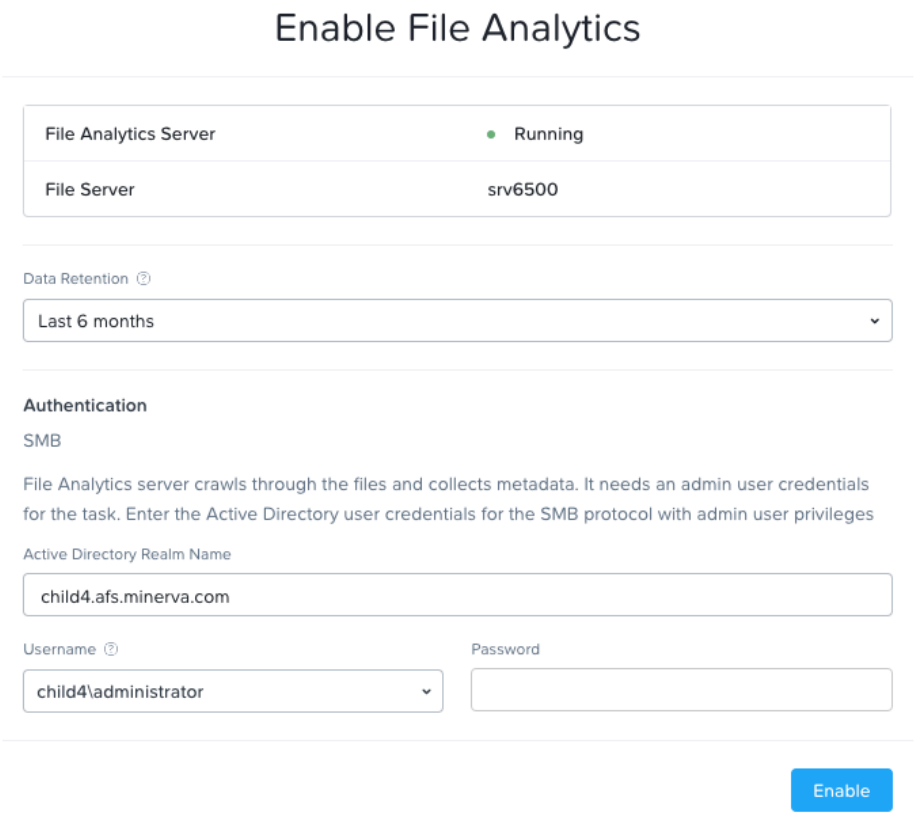
> **Note:** AD passwords for the file server admin cannot contain the following special characters: comma (,), single quote ('), double quote ("). Using the special characters in passwords prevents File Analytics from performing file system scans.

   a. (For SMB users only) In the **SMB** section, do the following in the indicated fields to provide SMB authentication details:

      - **Active Directory Realm Name**: Confirm the AD realm name for the file server.
      - **Username**: Enter the AD username for the file server administrator, see **File Analytics Prerequisites**.
      - **Password**: Enter the AD user password for the file server administrator.

   b. (For NFS users only) In the **NFS Authentication** section, do the following in the indicated fields to provide NFS authentication details:

      - **LDAP Server URI**: Enter the URI of the LDAP server.
      - **Base DN**: Enter the base DN for the LDAP server.
      - **Password**: Enter the LDAP user password for the file server administrator.



7. Click **Enable** .

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 668

Results

After enablement, File Analytics performs a one-time file system scan to pull metadata information. The duration of the scan varies depending on the protocol of the share. There is no system downtime during the scan.

Example

Scanning 3–4 million NFS or 1 million SMB files takes about 1 hour.

Enabling File Analytics on Prism Central

Enable File Analytics for Prism Central (PC) deployed file servers.

About this task

You must deploy the File Analytics VM (FAVM) before enabling File Analytics on PC. Do the following to enable File Analytics.

Procedure

1. In the Files Manager, select the target file server.
   The Files Console for the file server appears.
2. On the right, in the **File Analytics** pane of the Files Console, click **Launch File Analytics**.
   The **Enable File Analytics** page appears.
3. Under **Audit Data Retention**, select the event retention period from the pull-down list.
4. Under **NFS, SMB Authentication**, enter the authentication details in the indicated fields:
   a. **Active Directory Realm Name:** Enter the Active Directory realm name for join domain operations.
   b. **User Name:** Enter an AD username in the `domain|username` format or in the UPN format `username@ADrealm`. You must have the file server admin role. See "Managing Roles" in the *Nutanix Files User Guide*.
   c. **Password:** Enter the password for the specified user name.
5. Select **Next**.
   The **Configure Event Quotas** dialog displays. All configured file servers appear in the **File Server Name** column.
6. In the **Percentage of Threshold** column, enter an integer for each file server to indicate the threshold percentage allocated to the indicated file server.
   The combined total percentage of all file server thresholds must be 100%, and the combined number of events is 750,000,000.
7. Under **Email Recipients**, add a comma-separated list of email addresses for receiving quota limit notifications.
   The SMTP server details must be configured to add email recipients. You can update the **Percentage of Threshold** configuration after enabling Analytics. See Configuring an SMTP Server on page 28 and Configuring Event Quotas on page 15.
8. Select **Save & Enable**.
   The task to enable File Analytics begins, and the File Analytics dashboard loads once the task is completed.

Disabling File Analytics

How to disable File Analytics on a file server.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 669

About this task

Follow the steps as indicated to disable File Analytics.

Procedure

1. In **File Analytics** click the **gear icon** > **Disable File Analytics** .
2. In the dialog-box, click **Disable**.
   Disabling File Analytics turns off data collection on the file server. The following message banner appears.

   ```
   File Analytics is disabled on the server. Enable File Analytics to start collecting data again or Delete File Analytics Data.
   ```

What to do next

To delete data, click the **Delete File Analytics Data** link in the banner described in Step 2.

Launching File Analytics

Launch File Analytics from the Files Console for both Prism Element (PE) and Prism Central (PC) deployed file servers.

About this task

You can also launch File Analytics from the File Server view in Prism Element by clicking Launch File Analytics under the file server table.

About this task

Do the following to launch File Analytics in the Files Console from Prism Central.

Procedure

1. In Prism Central, click the name of a file server in the **File Servers** table.
   The **Dashboard** page of the Files Console appears.
2. in the File Analytics tile, click **Launch File Analytics**.

Launching File Analytics from Prism Element

Procedure

1. From the Prism views drop-down, select the **File Server** view.
2. Select the target file server from the entity tab.
3. Click the **File Analytics** action button below the entity table.

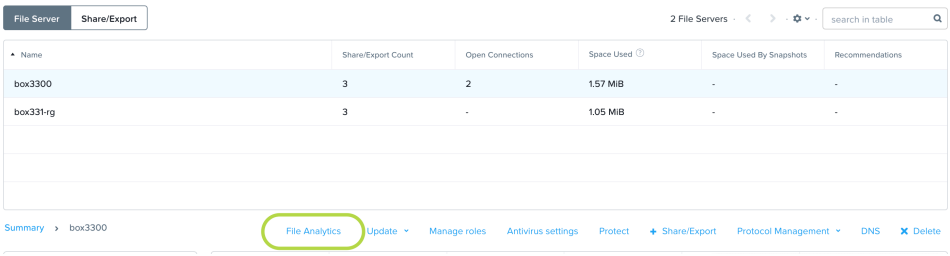


Figure 5: Launch File Analytics

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 670

ADMINISTRATION

Overview of administrative processes for File Analytics.

As an admin, you have the required permissions for performing File Analytics administrative tasks. For information on how to add a file server admin, see *Managing Roles* in the *Nutanix Files User Guide*.

Some of the primary administrative features of the File Analytics interface include the **Admin dropdown** to collect logs and view the current File Analytics version, a status icon to check the file system scan status, the **File server drop-down** to view the name of the file server for which data is displayed, and the **Health icon** to check the health of File Analytics.

The topics in this chapter describe the underlying procedures for administering your File Analytics environment. For advanced administrative options, refer to the File Analytics Options on page 50 chapter.

File Analytics VM Management

To update a File Analytics VM (FAVM), refer to the sizing guidelines in the File Analytics release notes and follow the steps in VM Management in the *Prism Element Web Console Guide*.

Removing File Analytics VMs

Remove a File Analytics VM (FAVM) by disabling it and deleting it from the cluster in Prism.

About this task

Follow the steps as indicated to remove an FAVM.

> **Note:** Do not delete an FAVM using the CLI, as this operation does not decommission the FAVM.

Procedure

1. Disable File Analytics on all file servers in the cluster. See Disabling File Analytics on page 11.
2. In the **File Server** view in Prism Element, do the following:
   a. In the top actions bar, click **Manage File Analytics**.
   b. Click Delete to remove the FAVM.

   When you delete an FAVM, you also delete all of your File Analytics configurations and audit data stored on the FAVM.

Restarting a File Analytics VM (FAVM)

How to gracefully stop and start a FAVM.

Procedure

1. Stop an FAVM.

```
nutanix@favm$ sudo shutdown -P now
```

2. Start an FAVM.

```
nutanix@favm$ sudo shutdown -r now
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 671

Role-based Access Control for File Analytics

Prism Element (PE) supports role-based access control (RBAC) that lets you configure customized access to File Analytics based on assigned roles.

From the PE dashboard, you can assign predefined built-in roles (system roles) to users or user groups. File Analytics supports the following built-in roles:

Note: Only administrators, super admin, or a Prism admin in PE, can create roles for File Analytics.

- **Viewer**: Grants you view-only access but does not let you perform any administrative,create or modify, tasks.
- **Cluster and User Admin**: Lets you view information, perform administrative tasks, and perform create and modify operations.

For more information on Role Based Access Control, refer to the "Controlling User Access (RBAC)", "Built-in Role Management", "Configuring Role Mapping", and "Managing Local User Accounts" sections in the *Security Guide*.

Updating Credentials

How to update authentication credentials for LDAP or Active Directory.

Procedure

1. Click **gear icon** > **Update AD/LDAP Configuration**.
2. To update Active Directory credentials, do the following in the indicated fields. Otherwise, move on to the next step.

   Note: AD passwords for the file server admin cannot contain the following special characters: comma (,), single quote ('), double quote ("). Using the special characters in passwords prevents File Analytics from performing file system scans.

   a. **Active Directory Realm Name:** Confirm or replace the realm name.

   b. **Username:** Confirm or replace the username.

   c. **Password:** Type in the new password.
3. To update the NFS configuration, do the following. Otherwise, move on to the next step.

   a. **LDAP Server URI:** Confirm or replace the server URI.

   b. **Base DN:** Confirm or replace the base distinguished name (DN).

   c. **Bind DN (Optional):** Confirm or replace the bind distinguished name (DN).

   d. **Password:** Type in the new password.
4. Click **Save**.

Managing Deleted Share and Export Audits

Manage the audit data of deleted shares and exports.

About this task

By default, File Analytics retains deleted share and export data. The dashboard widgets do not account for data of deleted shares and exports. The **deleted** marker appears next to deleted shares and exports in audit trails. The **Manage Share/Export Audit data** window displays a list of deleted shares and exports.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 672

Follow the steps as indicated to remove audit data for the deleted share or export.

> **Caution:** You cannot restore the deleted audit data of a deleted share or export.

Procedure

1. Click the **gear icon** > **Manage Deleted Share/Export Audit**.
2. Check the box next to the share or export name.
3. Click **Delete**.
4. In the confirmation window, click **Delete** to confirm the deletion of the data.
   In the **Manage Deleted Share/Export Audit** dialog, a progress bar displays the progress of the deletion task next to the share name. File Analytics can take several hours to finish a delete task.

Changing an FAVM Password

Update the password of a File Analytics VM (FAVM).

About this task

Follow the steps as indicated.

Procedure

1. Log on to an FAVM with SSH.
2. Change the Nutanix password.

   ```
   nutanix@favm$ sudo passwd nutanix
   ```

3. Respond to the prompts, providing the current and new Nutanix user passwords.

   ```
   Changing password for user nutanix.
   Old Password:
   New password:
   Retype new password:
   passwd: all authentication tokens updated successfully.
   ```

   The password must meet the following complexity requirements:

   - Be at least eight characters long
   - Have at least one lowercase letter
   - Have at least one uppercase letter
   - Have at least one number
   - Have at least one special character
   - Have at least a four characters difference from the old password
   - Should not be among the last ten passwords

Configuring Event Quotas

How to configure quotas for quotas for event limits.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 673

About this task

Event quotas set guardrails for the number of events on the file server. Email recipients receive notifications once a file server reaches 80% of its quota. If the file server reaches the max quota, File Analytics deletes the oldest event indexed for that file server.

Do the following to create an event quota.

Procedure

1. In the File Analytics web console, click the **gear icon** > **Configure Event Quotas**.
   The **Configure Event Quotas** dialog displays. All configured file servers appear in the **File Server Name** column.
2. In the **Percentage of Threshold** column, enter an integer for each file server to indicate the threshold percentage allocated to the indicated file server.
   The combined total percentage of all file server thresholds must be 100%, and the combined number of events is 750,000,000.
3. Under **Email Recipients**, add a comma-separated list of email addresses that will receive quota limit notifications.
4. Select **Save**.

Upgrades

Meet the requirements for performing File Analytics upgrades.

Before you proceed with the Analytics upgrade, ensure the following:

- You have a compatible version of AOS and Files.

  Refer to File Analytics Release Notes for compatibility details. You can upgrade both AOS and Files through Prism Element. See AOS Upgrade in the *Prism Element Web Console Guide*.
- You have checked the Analytics **Health** page to confirm that the deployment is healthy (green). See Health on page 23.
- The protection domain (PD) for the File Analytics VM (FAVM) does not include any other entities.
  - File Analytics does not support Prism Central-based Nutanix Disaster Recovery (Leap).
- You have Analytics enabled on at least one file server.

To upgrade File Analytics, perform inventory and updates using the Life-Cycle Manager (LCM); see the *Life Cycle Manager Guide* for instructions on performing inventory and updates.

> **Note:** The File Analytics UI is not accessible during upgrades.

During the upgrade process, Analytics takes a snapshot of the volume group (VG) that contains File Analytics data. If issues occur during an upgrade, Analytics restores the FAVM to the pre-upgrade state.

Upgrade File Analytics on a Dark Site

Upgrade File Analytics on a dark site using the Life Cycle Manager (LCM).

Before you begin

You need a local web server reachable by your Nutanix clusters to host the LCM repository.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 674

Procedure

1. From a device that has public Internet access, go to **Nutanix Portal** > **Downloads** > **Tools & Firmware**.
   a. Download the tar file lcm_dark_site_version.tar.gz.
   b. Transfer lcm_dark_site_version.tar.gz to your local web server and untar into the release directory.
2. From a device that has public Internet access, go to the Nutanix portal and select **Downloads** > **File Analytics**.
   a. Download the following files.
      - file_analytics_dark_site_version.tar.gz
      - nutanix_compatibility.tgz
      - nutanix_compatibility.tgz.sign
   b. Transfer file_analytics_dark_site_version.tar.gz to your local web server and un-tar into the release directory.
   c. Transfer the nutanix_compatibility.tgz and nutanix_compatibility.tgz.sign files to your local web server . Overwrite existing files as needed.
3. Log on to Prism Element.
4. Click **Home** > **LCM** > > **Settings**.
   a. In the **Fetch updates from** field, enter the path to the directory where you extracted the tar file on your local server. Use the format http://webserver_IP_address/release.
   b. Click **Save**.
      You return to the Life Cycle Manager.
   c. In the LCM sidebar, click **Inventory** > **Perform Inventory**.
   d. Update the LCM framework before trying to update any other component.
      The LCM sidebar shows the LCM framework with the same version as the file you downloaded.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 675

DASHBOARD

The **Dashboard** tab displays data on the operational trends of a file server.

Dashboard View

The **Dashboard** tab is the opening screen after launching File Analytics for a specific file server. The dashboard displays widgets, which refresh hourly, displaying data on file trends, distribution, and operations.

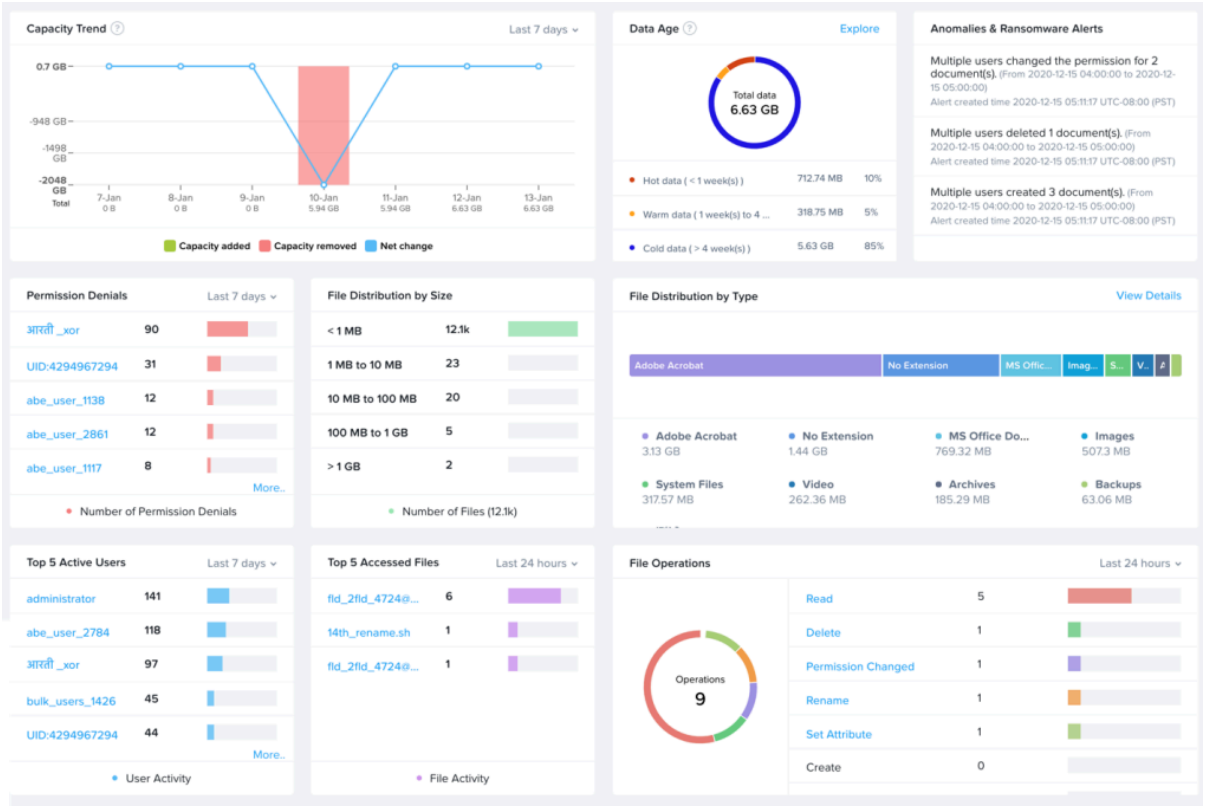


Figure 6: File Analytics Dashboard

Table 1: Dashboard Widgets

Tile Name	Description	Intervals
Capacity trend	Displays capacity trends for the file server, including capacity added, capacity removed, and net changes. Clicking an event period widget displays the **Capacity Trend Details** view.	7 days, the last 30 days, or the last 1 year.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 676

Tile Name	Description	Intervals
Data age	Displays the percentage of data by age. Data age determines the data heat, including hot, warm, and cold.	Default intervals are as follows: • Hot data – accessed within the last week. • Warm data – accessed within 2 to 4 weeks. • Cold data – accessed 4 weeks ago or later.
Permission denials	Displays users who have had excessive permission denials and the number of denials. Clicking a user displays audit details, see Audit Trails - Users on page 31 for more.	[user id], [number of permission denials]
File distribution by size	Displays the number of files by file size. Provides trend details for the top five files.	Less than 1 MB, 1–10 MB, 10–100 MB, 100 MB to 1 GB, greater than 1 GB).
File distribution by type	Displays the space used by various applications and file types. The file extension determines the file type. See the *File types* table for more details.	MB or GB
File distribution by type details view	Displays a trend graph of the top five file types. File distribution details include file type, current space used, current number of files, and change in space for the last 7 or 30 days. Clicking **View Details** displays the **File Distribution by Type** view.	Daily size trend for top 5 files (GB), file type (see the "File Type" table), current space used (GB), current number of files (numeric), change in last 7 or 30 days (GB).
Top 5 active users	Lists the users who have accessed the most files and the number of operations the user performed for the specified period. When there are more than five active users, the **more** link provides details on the top 50 users. Clicking the user name displays the audit view for the user, see Audit Trails - Users on page 31 for more.	24 hours, 7 days, 1 month, or 1 year.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 677

Tile Name	Description	Intervals
Top 5 accessed files	Lists the five most frequently accessed files. Clicking **more** provides details on the top 50 files. Clicking the file name displays the audit view details for the file, see Audit Trails - Files on page 34 for more.	24 hours, 7 days, 1 month, or 1 year.
Files operations	Displays the distribution of operation types for the specified period, including a count for each operation type and the total sum of all operations. Operations include: create, delete, read, write, rename, permission changed, set attribute, symlink, permission denied, permission denied (file blocking). Clicking an operation displays the **File Operation Trend** view.	24 hours, 7 days, 1 month, or 1 year.

Capacity Trend Details

Clicking an event period in the **Capacity Trend** widget displays the **Capacity Trend Details** view for that period. The view includes three tabs **Share/Export**, **Folder**, and **Category**. Each tab includes columns detailing entity details: **Name**. Net capacity change, capacity added, and capacity removed.

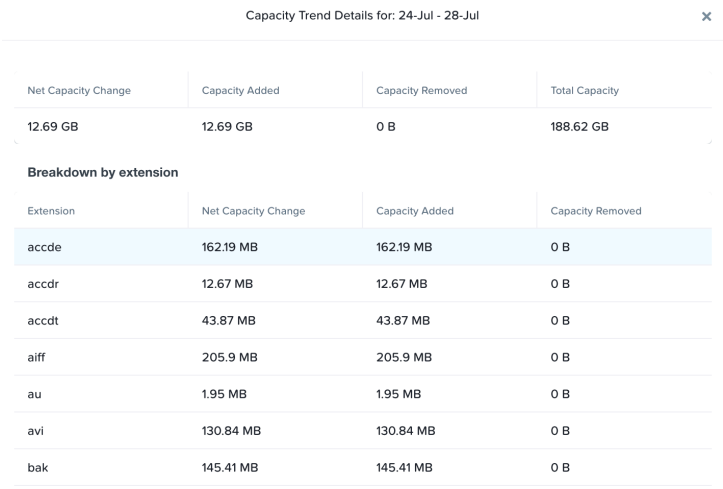


Figure 7: Capacity Trend Details View

Table 2: Capacity Trend Details

Category	Supported File Type
Name	Name of the share or export, folder, or category.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 678

Category	Supported File Type
Net capacity change	The total difference between capacity at the beginning and the end of the specified period.
Share name (for folders only)	The name of the share or export that the folder belongs to.
Capacity added	Total added capacity for the specified period.
Capacity removed	Total removed capacity for the specified period.

File Distribution by Type Details

Clicking **View Details** for the **File Distribution by Type** widget displays granular details of file distribution. See the **File Types** table for details.

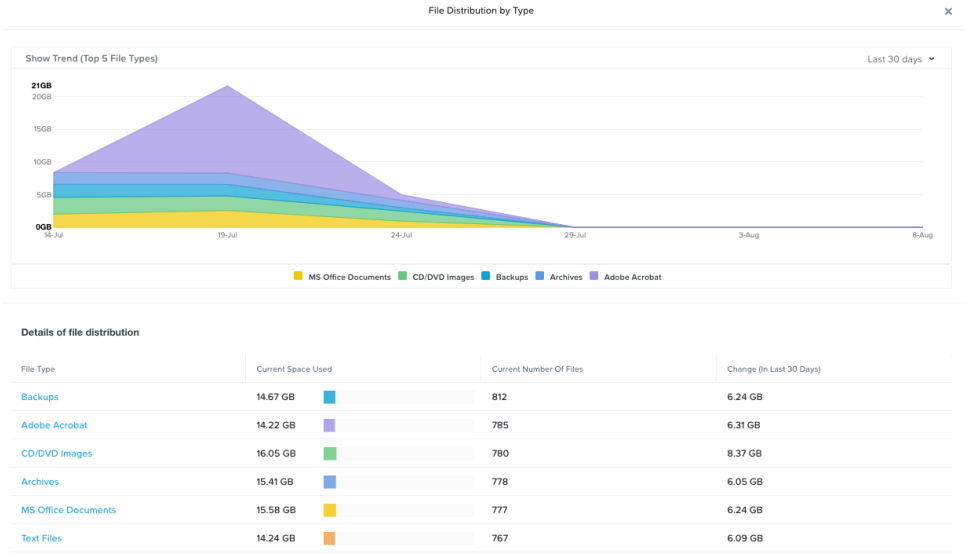


Figure 8: File Distribution by Type

Table 3: Details of File Distribution Parameters

Category	Supported File Type
File type	The name of the file type.
Current space used	The space capacity occupied by the file type.
Current number of files	The number of files for the specified file type.
Change (in last 30 days)	The increase in capacity over a 30-day period for the specified file type.

Table 4: File Types

Category	Supported File Type
Archives	.cab, .gz, .rar, .tar, .z, .zip
Audio	.aiff, .au, .mp3, .mp4, .wav, .wma

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 679

Category	Supported File Type
Backups	.bak, .bkf, .bkp
CD/DVD images	.img, .iso, .nrg
Desktop publishing	.qxd
Email archives	.pst
Hard drive images	.tib, .gho, .ghs
Images	.bmp, .gif, .jpg, .jpeg, .pdf .png, .psd, .tif, .tiff,
Installers	.msi, .rpm
Log Files	.log
Lotus notes	.box, .ncf, .nsf, .ns2, .ns3, .ns4, .ntf
MS Office documents	.accdb, .accde, .accdt, .accdr, .doc, .docx, .docm, .dot, .dotx, .dotm, .xls, .x
System files	.bin, .dll, .exe
Text files	.csv, .pdf, .txt
Video	.avi, mpg, .mpeg, .mov, .m4v
Disk image	.hlog, .nvram, .vmdk, .vmx, .vmxf, .vmtm, .vmem, .vmsn, .vmsd

File Operation Trend

Clicking an operation type in the **File Operations** widget displays the **File Operation Trend** view. The **File Operation Trend** view breaks down the specified period into smaller intervals and displays the number of occurrences of the operation during each interval.

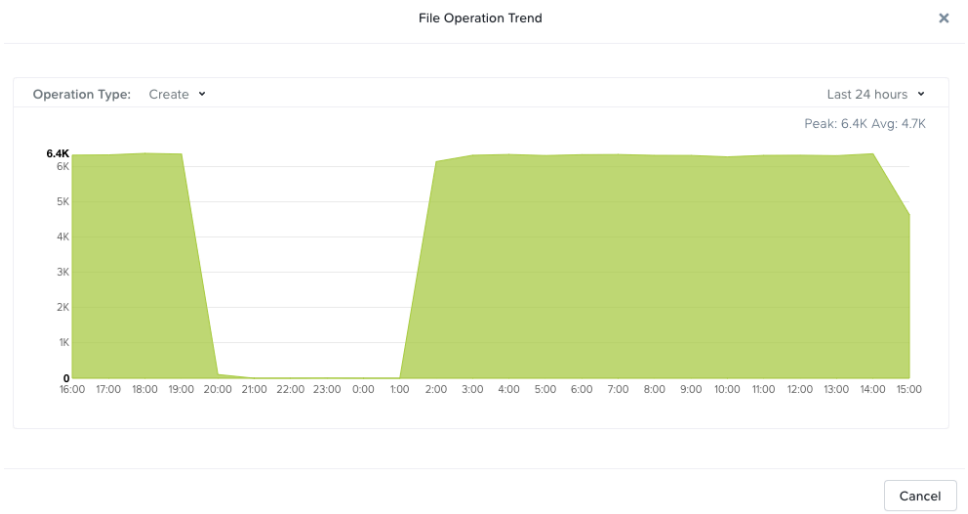


Figure 9: Operation Trend

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 680

Table 5: File Operation Trend View Parameters

Category	Description
Operation type	A drop-down option to specify the operation type. See *Files Operations* in the *Dashboard Widgets* table for a list of operation types.
Last (time period)	A drop-down option to specify the period for the file operation trend.
File operation trend graph	The x-axis displays shorter intervals for the specified period. The y-axis displays the number of operation trends over the extent of the intervals.

Health

The Health dashboard displays dynamically updated health information about each file server component.

The Health dashboard includes the following details:

- **Data Summary**: Data summary of all file servers with File Analytics enabled.
- **Host Memory**: Percent of used memory on the File Analytics VM (FAVM).
- **Host CPU Usage**: Percent of CPU used by the FAVM.
- **Storage Summary**: Amount of storage space used on the File Analytics data disk or FAVM disk.
- **Overall Health**: Overall health of File Analytics components.
- **Data Server Summary**: Data server usage by component.

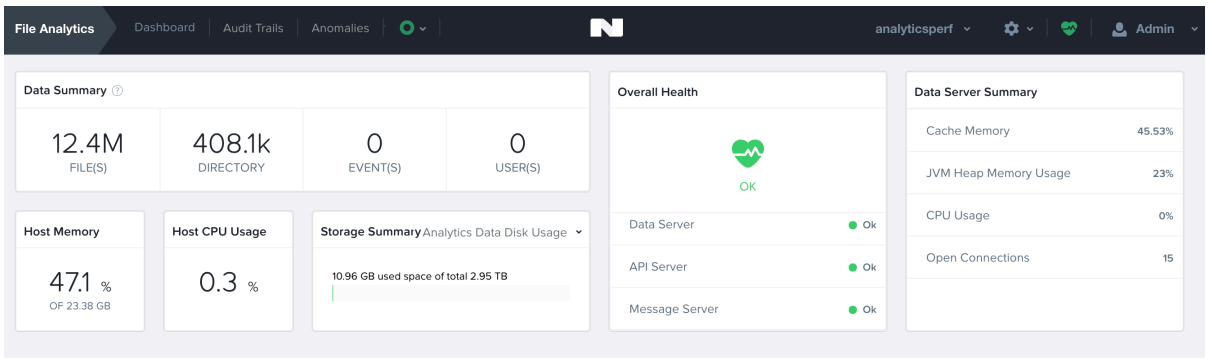


Figure 10: Health Page

Data Age

The **Data Age** widget in the dashboard provides details on data heat.

Data age, or heat, is share-level usage organized by share access frequency. There are three levels of data heat:

- *Hot*: Frequently accessed data, last accessed within the last week.
- *Warm*: Infrequently accessed data, last accessed within the last two to four weeks.
- *Cold*: Rarely accessed data, last accessed longer than four weeks ago.

You can define the limits of each data-age heat rather than using the default values. See Configuring Data Heat Levels on page 24.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 681

Configuring Data Heat Levels

Update the values that define the data heat levels.

Procedure

1. In the **Data Age** widget, click **Explore**.
2. Click **Edit Data Age Configuration**.
3. Do the following in the **Hot Data** section:
   a. In the entry field next to **Older Than**, enter an integer.
   b. In the dropdown, choose a value for **Week(s)**, **Month(s)**, or **Year(s)**.
4. Do the following in the **Warm Data** section to configure two ranges :
   a. In the first entry field, enter an integer to configure the first range.
   b. In the drop-down, choose a value for **Week(s)**, **Month(s)**, or **Year(s)**.
   c. In the second entry field, enter an integer to specify the second range.
   d. In the drop-down, choose a value for **Week(s)**, **Month(s)**, or **Year(s)**.
5. Do the following in the **Cold Data** section to configure four ranges :
   a. In the first entry field, enter an integer to specify the first range.
   b. In the drop-down, choose a value for **Week(s)**, **Month(s)**, or **Year(s)**.
   c. In the second entry field, enter an integer to specify the second range.
   d. In the drop-down, choose a value for **Week(s)**, **Month(s)**, or **Year(s)**.
   e. In the 3rd entry field, enter an integer to specify the 3rd range.
   f. In the drop-down, choose a value for **Week(s)**, **Month(s)**, or **Year(s)**.
   g. (optional) In the 4th entry field, enter an integer to configure the 4th range.
   h. In the drop-down, choose a value for **Week(s)**, **Month(s)**, or **Year(s)**.
6. Click **Apply**.

> **Note:** The new values do not affect the already calculated heat statistics. File Analytics uses the updated values for future data heat calculations.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 682

ANOMALIES

The **Anomalies** tab provides options for creating anomaly policies and displays dashboards for viewing anomaly trends.

You can configure anomalies for the following operations:

- Creating files and directories
- Deleting files and directories
- Permission changes
- Permission denials
- Renaming files and directories
- Reading files and directories

Define anomaly rules by defining the following thresholds:

- Users exceed an operation count threshold
- Users exceed an operation percentage threshold

Meeting the lower operation threshold triggers an anomaly.

Consider a scenario where you have 1 thousand files, the *`operation count threshold`* defined as 10, and the *`operation percentage threshold`* defined as 10%. The count threshold takes precedence, as 10% of 1 thousand is 100, which is greater than the count threshold of 10.

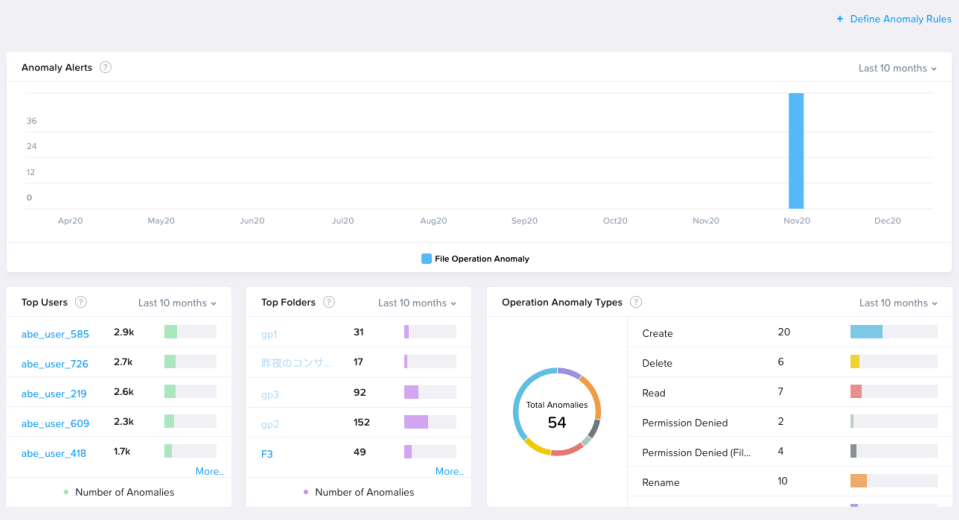


Figure 11: Anomalies Dashboard

Table 6: Anomalies Data Pane Descriptions

Pane Name	Description	Values
Anomaly Trend	Displays the number of anomalies per day or per month.	Last 7 days, Last 30 days, Last 1 year

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 683

Pane Name	Description	Values
Top Users	Displays the users with the most anomalies and the number of anomalies per user.	Last 7 days, Last 30 days, Last 1 year
Top Folders	Displays the folders with the most anomalies and the number of anomalies per folder.	Last 7 days, Last 30 days, Last 1 year
Operation Anomaly Types	Displays the percentage of occurrences per anomaly type.	Last 7 days, Last 30 days, Last 1 year

Anomaly Details

Clicking an anomaly bar in the **Anomaly Trend** graph displays the **Anomaly Details** view.

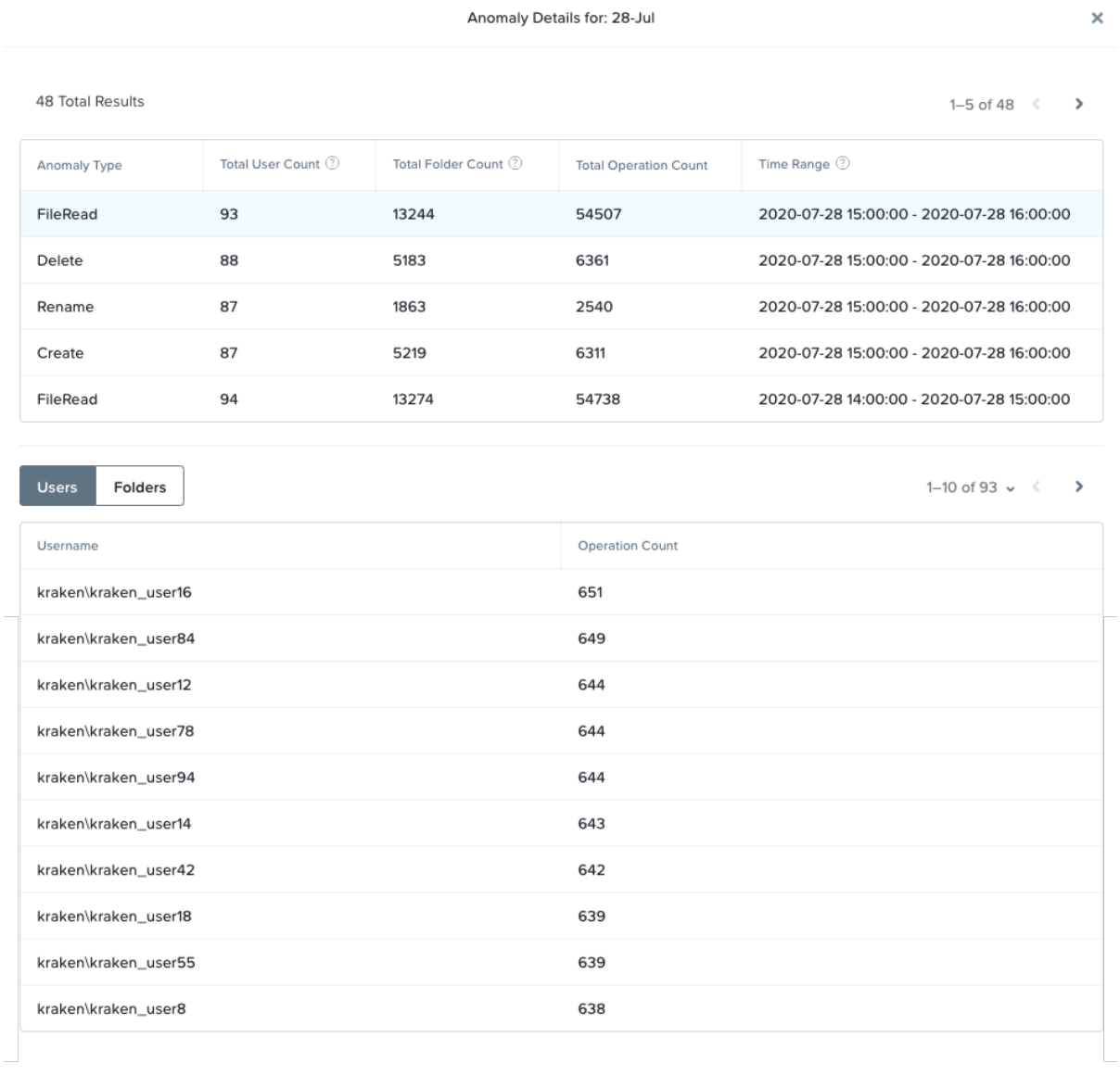


Figure 12: Anomaly Details View

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 684

Table 7: Anomalies Details View Total Results Table

Column	Description
Anomaly Type	The configured anomaly type. Anomaly types not configured do not show up in the table.
Total User Count	The number of users that have performed the operation causing the specified anomaly during the specified time range.
Total Folder Count	The numbers of folders in which the anomaly occurred during the specified time range.
Total Operation Count	Total number of anomalies for the specified anomaly type that occurred during the specified time range.
Time Range	The time range for which the total user count, total folder count, and total operation count are specified.

Table 8: Anomalies Details View Users/Folders Table

Column	Description
Username or Folders	Indicates the entity for the operation count. Selecting the **Users** tab indicates operation count for specific users, and selecting the **Folders** tab indicates the operation count for specific folders.
Operation count	The total number of operations causing anomalies for the selected user or folder during the time period for the bar in the **Anomaly Trend** graph.

Configuring Anomaly Detection

Steps for configuring anomaly rules.

About this task

To create an anomaly rule, do the following.

> **Note:** Configure an SMTP server for File Analytics to send anomaly alerts, see Configuring an SMTP Server on page 28.

Procedure

1. Click the **gear icon** > **Define Anomaly Rules.**.
2. In the **Anomaly Email Recipients** field, enter a comma-separated list of email recipients for all anomaly alerts and data.

> **Note:** File Analytics sends anomaly alerts and data to recipients whenever File Analytics detects an anomaly.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 685

3. To configure a new anomaly, do the following in the indicated fields:

   a. **Events**: Select a rule for the anomaly from one of the following:

      - Permission changed
      - Permission denied
      - Delete
      - Create
      - Rename
      - Read

      The event defines the scenario type for the anomaly.

   b. **Minimum Operations %**: Enter a percentage value for the minimum threshold.

      File Analytics calculates the minimum operations percentage based on the number of files. For example, if there are 100 files, and you set the minimum operations percentage to ***5***, five operations within the scan interval would trigger an anomaly alert.

   c. **Minimum Operation Count**: Enter a value for a minimum operation threshold.

      File Analytics triggers an anomaly alert after meeting the threshold.

   d. **User**: Choose if the anomaly rule is applicable for **All Users** or an **Individual** user.

   e. **Type:** the type determines the interval.

      The interval determines how far back File Analytics monitors the anomaly.

   f. **Interval** : Enter a value for the detection interval.

   g. (optional) **Actions**: Click the **pencil icon** to update an anomaly rule. Click the **x** icon to delete an existing rule.

Figure 13: Anomaly Configuration Fields

4. Click **Save**.

Configuring an SMTP Server

File Analytics uses a simple mail transport protocol (SMTP) server to send anomaly alerts.

About this task

To configure an SMTP server, do the following:

Procedure

1. Click the **gear icon** > **SMTP Configuration**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 686

2. In the **SMTP Configuration** window, enter the indicated details in the following fields:

   a. **Hostname Or IP Address**: Enter a fully qualified domain name or IP address for the SMTP server.

   b. **Port**: Enter the port to use.
   The standard SMTP ports are 25 (encrypted), 587 (TLS), and 465 (SSL).

   c. **Security Mode**: Enter the desired security mode from the drop-down list.
   The options are:

   - **NONE** (unencrypted)
   - **STARTTLS** (TTL encryption)
   - **SSL** (SSL encryption)

   (If security mode is "NONE" go to step e.)

   d. **User Name**: Enter a user name for logging into the SMTP server. Depending on the authentication method, the user name may require a domain.

   e. **Password**: Enter password.

   f. **From Email Address:** Enter the email address from which File Analytics will send the anomaly alerts.

   g. **Recipient Email Address:** Enter a recipient email address to test the SMTP configuration.

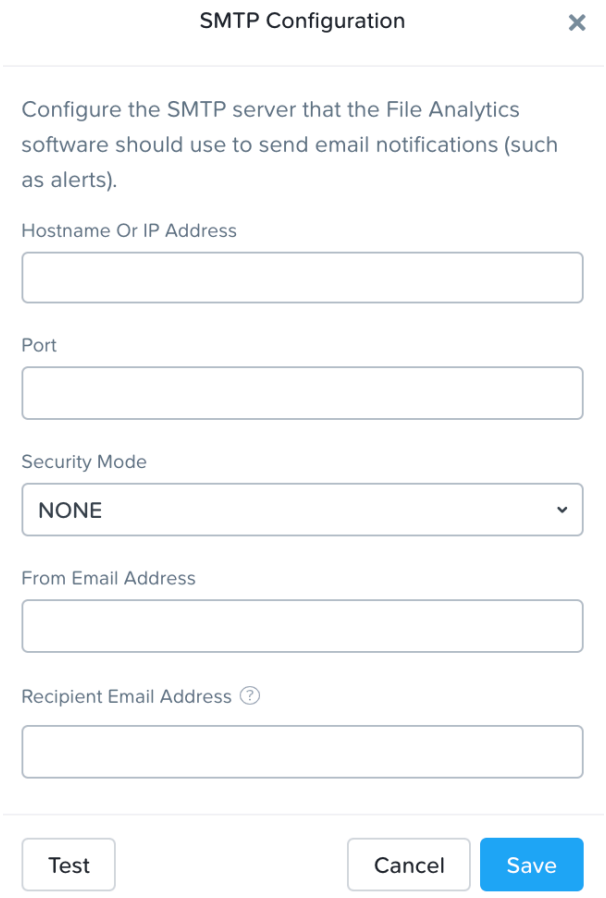


Figure 14: SMTP Configuration

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 687

3. Click **Save**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 688

AUDIT TRAILS

Use audit trails to look up operation data for a specific user, file, folder, or client.

The **Audit Trails** tab includes **Files**, **Folders**, **Users**, and **Client IP** options for specifying the audit type. Use the search bar for specifying the specific entity for the audit (user, folder, file, or client IP).

The results table presents details for entities that match the search criteria. Clicking the entity name , or client IP address, takes you to the Audit Trails dashboard for the target entity.

Viewing Audit Trails

Audit a user, file, client, or folder.

About this task

Follow the steps as indicated.

Procedure

1. Click the **Audit Trails** tab.
2. Select the **Files**, **Folders**, **Users**, or **Client IP** option.
3. Enter the audit trails target into the search bar.
4. Click **Search**.
5. To display audit results in the **Audit Trails** window, click the entity name or client IP address.

Audit Trails - Users

Details for client IP audit trails.

Audit Trails Search - Users

When you search by user in the **Audit Trails** tab, search results display the following information in a table.

- User Name
- Domain
- Last Operation
- Last Operation On
- Share Name
- Operation Date
- Action

Audit Details Page - Users

Clicking **View Audit** displays the **Audit Details** page, which shows the following audit information for the selected user.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 689

- A **User Events** graph displays various operations the user performed during the selected period and the percentage of time each operation has occurred per total operations during the specified period.
  - The **Filter by operations** drop-down contains operation filters, which you can use to filter the audit by operation type. Operations include:
    - Create File
    - Delete
    - Make Directory
    - Permission Changed
    - Permission Denied
    - Read
    - Remove Directory
    - Rename
    - Set Attribute
    - Write
    - Symlink
  - The **filter bar**, above the **User Events** graph, displays the filters in use.
  - Use the **From** and **To** fields to filter by date.
- The **Results** table displays operation-specific information. See more details below.
- The **Reset Filters** button removes all filters.

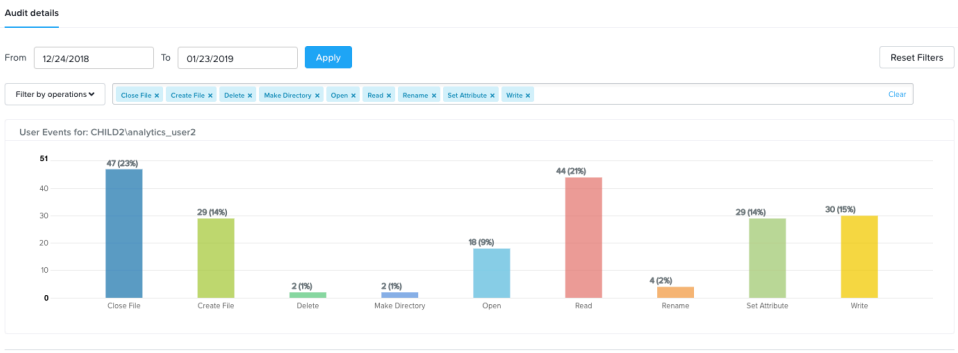


Figure 15: User Audit Details - Events

The **Results** table provides granular details of the audit results. The table displays the following data for every event.

- User Name
- User IP Address
- Operation
- Operation Date
- Target File

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 690

Click the **gear icon** for options to download the data as an XLS, CSV, or JSON file.

> **Note:** You can download a maximum of 10,000 events in CSV and JSON formats.

Audit Trails - Folders

Dashboard details for folder audits.

The following information displays when you search by file in the Audit Trails tab.

- Folder Name
- Folder Owner Name
- Share Name
- Parent Folder
- Last Operation
- Last Operation By
- Last Operation Date
- Action

The **Audit Details** page shows the following audit information for the selected folder.

- A **Folder Events** graph displays various operations performed on the file during the selected period, and the percentage of time each operation has occurred per total operations during that period.
  - The **Filter by operations** dropdown contains operation filters, which you can use to filter the audit by operation type. Operations include:
    - Select All
    - Make Directory
    - Permission Changed
    - Permission Denied
    - Remove Directory
    - Rename

      > **Note:** Rename operation shows both change of name and change of path for specific file or folder.

    - Set Attribute
  - A **filter bar**, above the File Events graph displays the filters in use.
  - Use the **From** and **to** fields to filter by date.
- The **Results** table displays operation-specific details.
- The **Reset Filters** button removes all filters.

The **Results** table provides granular details of the audit results. File Analytics displays the following data for every event.

- User Name
- Client IP

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 691

- Operation
- Operation Date

Click the gear icon for options to download the data as a CSV file.

> **Note:** The maximum limitation of downloading events to CSV and JSON format is 10,000.

Audit Trails - Files

Dashboards details for file audit.

Audit Trails for Files

When you search by file in the Audit Trails tab, the following information displays:

- File Name
- File Owner Name
- Share Name
- Parent Folder
- Last Operation
- Last Operation By
- Last Operation Date
- Action

> **Note:**
>
> - File Analytics does not support regular expression (RegEx) based search.
> - Up to 500 million files with latest 3 months of audit data is supported for a file server.

The **Audit Details** page shows the following audit information for the selected file.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 692

- A **File Events** graph displays various operations performed on the file during the selected period, and the percentage of time each operation has occurred per total operations during that period.
  - The **Filter by operations** dropdown contains operation filters, which you can use to filter the audit by operation type. Operation types include:
    - Close File
    - Create File
    - Delete
    - Make Directory
    - Open
    - Read
    - Rename

      Note: Rename operation shows both change of name and change of path for specific file or folder.
    - Set Attribute
    - Write
    - Symlink
  - A **filter bar**, above the File Events graph displays the filters in use.
  - Use the **From** and **to** fields to filter by date.
- The **Results** table displays operation-specific details.
  - The **Reset Filters** button removes all filters.

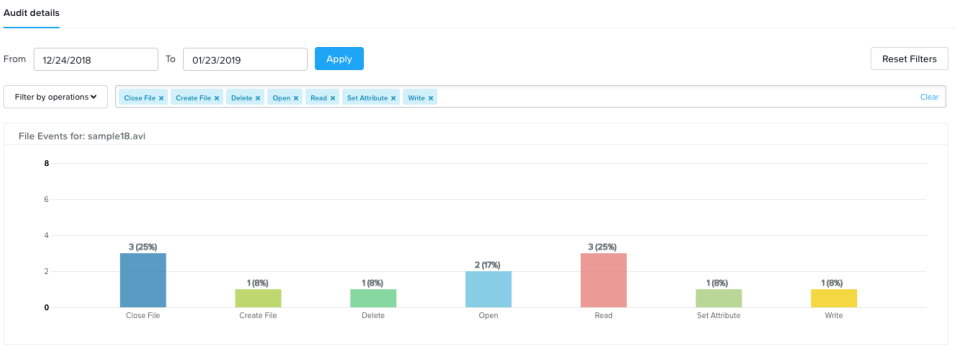


Figure 16: Files Audit Details - Events

The **Results** table provides granular details of the audit results. File Analytics displays the following data for every event.

- Username
- Client IP
- Operation
- Operation Date

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 693

Click the gear icon for options to download the data as a CSV file.

> **Note:** The maximum limitation of downloading events to CSV and JSON format is 10,000.

Audit Trails - Client IP

Dashboard details for client IP Audit Trails.

Audit Trails Search - Client IP

When you search by client IP in the **Audit Trails** tab, search results display the following information in a table.

- Client IP
- User Name
- Domain
- Last Operation
- Last Operation On
- Share Name
- Operation Date
- Action

The **Audit Details** page shows the following audit information for the selected client.

- A **User Events** graph displays various operations performed on the client during the selected period, and the percentage of time each operation has occurred per total operations during that period.
  - The **Filter by operations** dropdown contains operation filters, which you can use to filter the audit by operation type. Operation types include:
    - Create File
    - Delete
    - Make Directory
    - Permission Changed
    - Permission Denied
    - Read
    - Removed Directory
    - Rename
    - Set Attribute
    - Write
    - Symlink
    - Permission Denied (File Blocking)
  - A **filter bar**, above the File Events graph displays the filters in use.
  - Use the **From** and **to** fields to filter by date.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 694

- The **Results** table displays operation-specific details.
  - The **Reset Filters** button removes all filters.

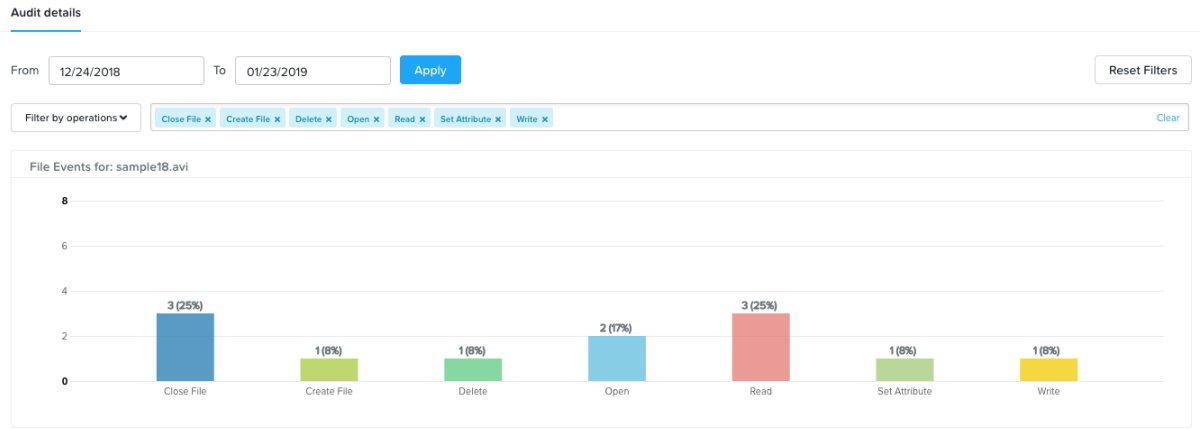


Figure 17: Files Audit Details - Events

The **Results** table provides granular details of the audit results. File Analytics displays the following data for every event.

- User Name
- Operation
- Target File
- Operation Date

Click the gear icon for an option to download the data as a CSV file.

> **Note:** The maximum limitation of downloading events to CSV and JSON format is 10,000.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 695

RANSOMWARE PROTECTION

File Analytics offers ransomware protection for your file server.

> **Caution:** Ransomware protection helps detect potential ransomware. Nutanix does not recommend using the File Analytics ransomware feature as an all-encompassing ransomware solution.

File Analytics scans files for ransomware in real-time and notifies you in the event of a ransomware attack once you configure email notifications.

Using a curated list of over 250 signatures that frequently appear in ransomware files, the Nutanix Files file blocking mechanism identifies and blocks files with ransomware extensions from carrying out malicious operations. You can modify the list by manually adding or removing signatures from Nutanix Files. See "File Blocking" in the *Nutanix Files User Guide*.

> **Caution:** Removing curated blocked signatures might prevent File Analytics from blocking some ransomware files.

File Analytics also monitors shares for self-service restore (SSR) policies and identifies shares that do not have SSR enabled in the ransomware dashboard. You can enable SSR through the ransomware dashboard.

Ransomware Protection Features

The ransomware dashboard includes panes for managing ransomware protection and self-service restore (SSR).

Ransomware Dashboard

The ransomware dashboard includes two main sections:

- The **SSR Status** pane for viewing, enabling, and managing SSR, see Enabling Self-Service Restore (SSR) on page 41.
- The **Vulnerabilities (Infection Attempts)** pane for viewing total vulnerabilities, vulnerable shares, malicious clients, and top recent ransomware attempts.
  - Clicking on the number of **total vulnerabilities** provides a detailed view of recent vulnerabilities.
  - Clicking on the number of **vulnerable shares** provides a detailed view of vulnerable shares.
  - Clicking on the number of **malicious clients** provides a detailed view of malicious clients.
- Click **Settings**, to enable and configure ransomware protection. See Enabling Ransomware Protection on page 39 and Configuring Ransomware Protection on page 40.
- Click **Download (.csv)** to download a list of blocked ransomware signatures.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 696

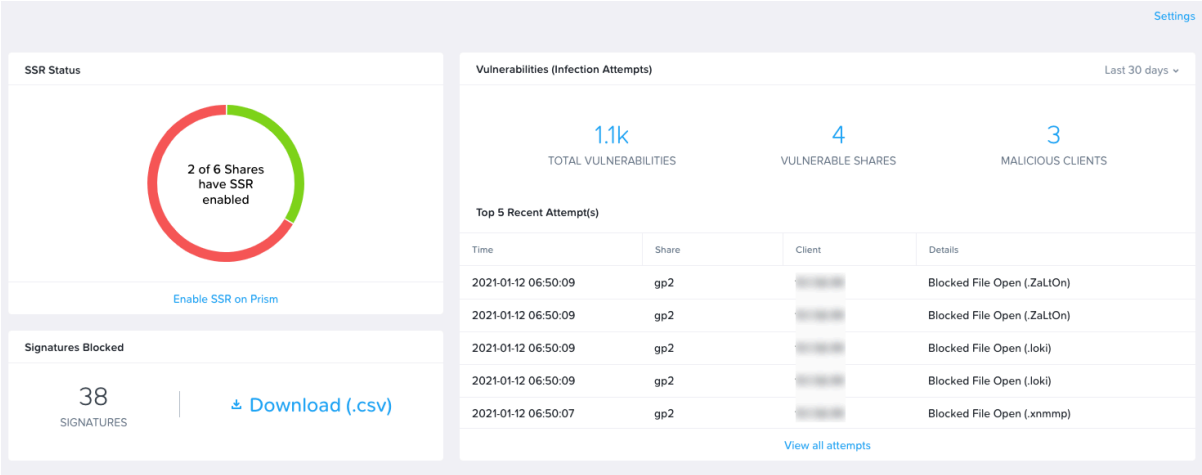


Figure 18: Ransomware Dashboard

Enabling Ransomware Protection

Enable ransomware protection on your file server.

Procedure

1. Go to **dropdown menu** > **Ransomware**.
2. In the message banner, click **Enable Ransomware Protection**.
3. (optional) Click **Configure SMTP to Add Recipients.**

> **Note:** This option appears only if you have not configured a simple mail transfer protocol (SMTP) server, see Configuring an SMTP Server on page 28.

4. Under **Ransomware Email Recipients**, add at least one email address. If there is a ransomware attack, File Analytics sends a notification to the specified email address.

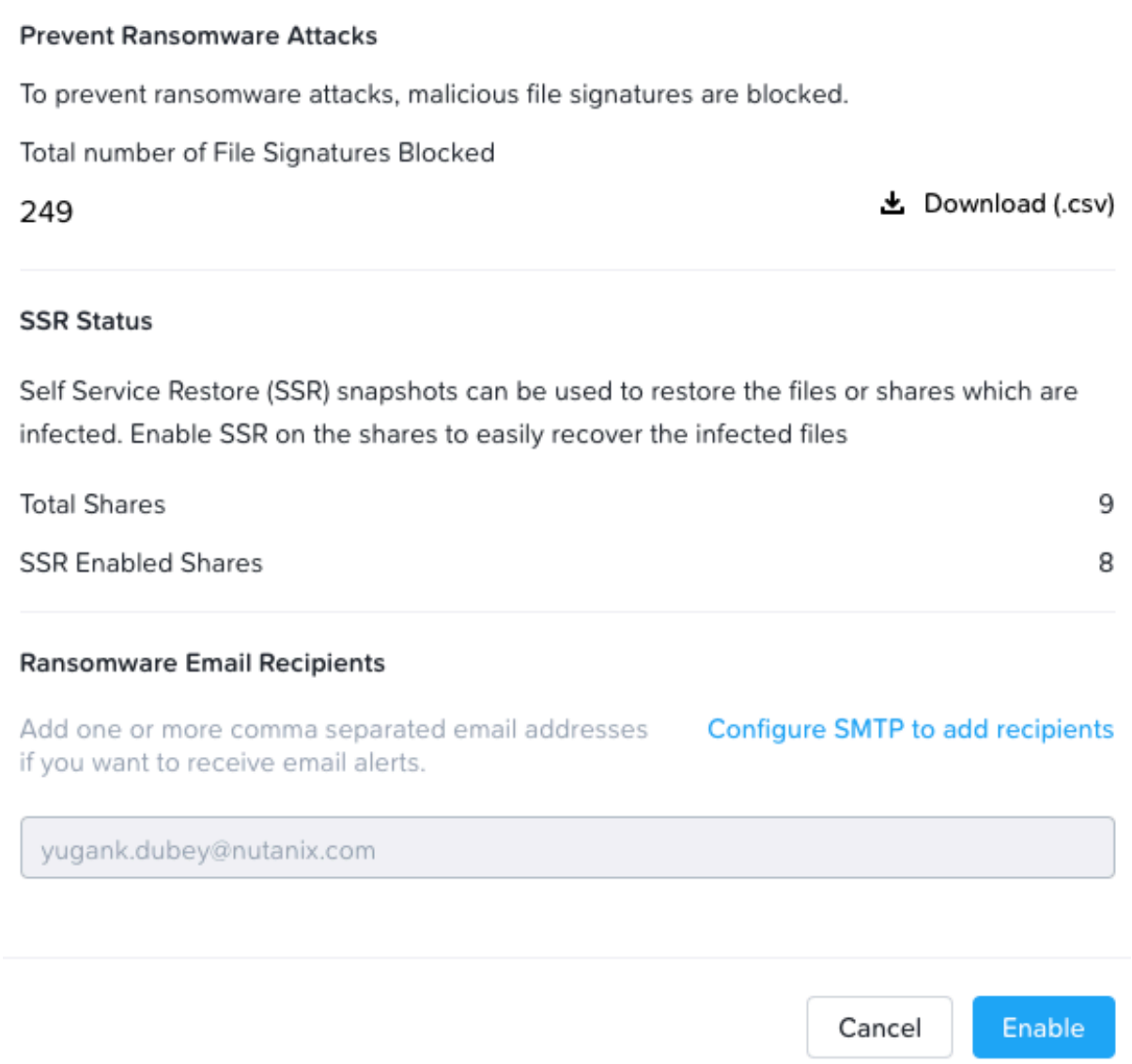


Figure 19: Ransomware Configuration View

5. Click **Enable**.
   See Configuring Ransomware Protection on page 40 for configuration steps.

Configuring Ransomware Protection

After enabling ransomware protection, you can update the ransomware protection configuration.

About this task

Do the following to add signatures to the blocked extension list.

Procedure

1. Go to **dropdown menu** > **Ransomware** > **Settings**.

2. (optional) Under **Search for blocked File Signatures**, enter ransomware signatures in the *.*`(signature)`* format.

   a. To check that the signature is blocked, click **Search**.

   b. If the signature is not blocked, click **Add to Block List**.

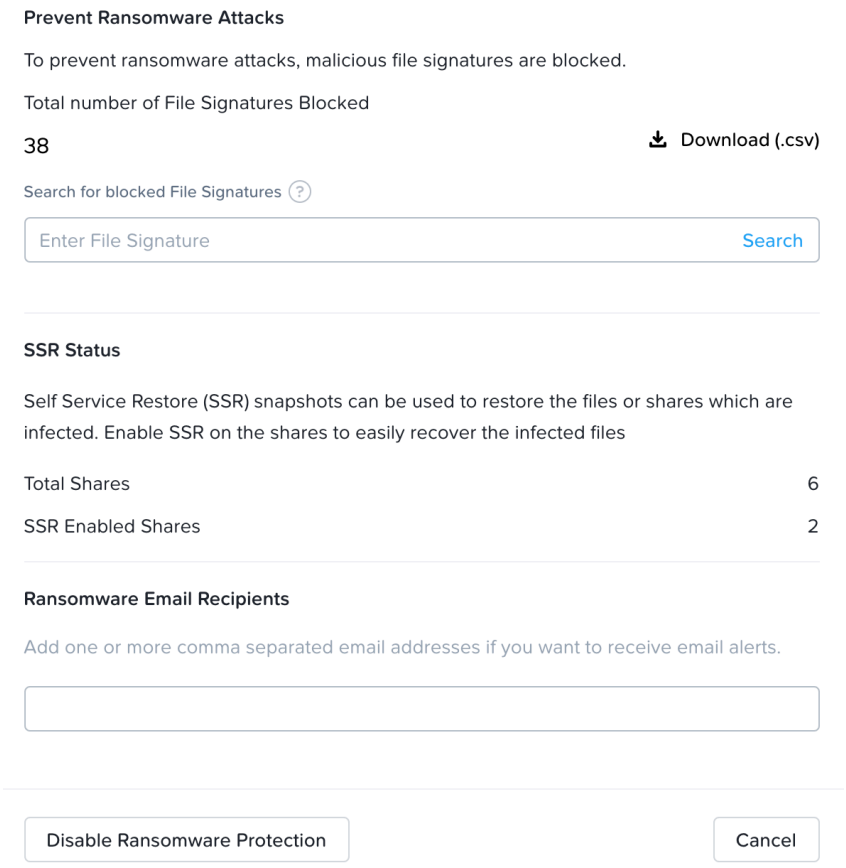


Figure 20: Ransomware Configuration View

3. (optional) To download a list of blocked ransomware signatures, click **Download (.csv)**.
4. (optional) Under **Ransomware Email Recipients**, add a comma-separated list of email addresses. In the event of a ransomware attack, File Analytics sends a notification to the specified email addresses.
5. (optional) To disable the ransomware protection feature, click **Disable Ransomware Protection**.

Enabling Self-Service Restore (SSR)

Enable SSR on unprotected shares identified by File Analytics.

Procedure

1. Go to **dropdown menu** > **Ransomware**.
2. Click **Enable SSR on Prism**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 699

3. Check the box next to the shares for which to enable SSR.

Figure 21: Enable SSR on Shares

4. Click **Enable SSR**.

REPORTS

Generate a report for entities on the file server.

Create a report with custom attribute values or use one of the File Analytics pre-canned report templates. To create a custom report, specify the entity, attributes (and operators for some attributes), attribute values, column headings, and the number of columns. Pre-canned reports define most of the attributes and headings based on the entity and template that you choose.

The **Reports** dashboard displays a table or previously generated reports. You can rerun existing reports rather than creating a template. After creating a report, you can download it as a JSON or CSV file.

Reports Dashboard

The reports dashboard includes options to create, view and download reports.

The **Reports** dashboard includes options to create a report, download reports as a JSON, download reports as a CSV, rerun reports, and delete reports.

The reports table includes columns for the report name, status, last run, and actions.

Clicking **Create a new report** takes you to the report creation screen, which includes a **Report builder** and a **Pre-canned Reports Templates** tabs. The tabs include report options and filters for report configuration.

Both tabs include the following elements:

- The **Define Report Type** section includes an **Entity** drop-down menu to select an entity.
- The **Define Filters** section includes an **Attribute** drop-down menu and an option to add more attributes by clicking **+ Add filter**.
- The **Add/remove columns in this report** section displays default columns. Clicking the columns field lets you add additional columns to the report. Clicking the **x** next to the column name removes it from the report.
- The **Define number of maximum rows in this report** section includes a **Count** section to specify the number of rows in the report.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 701

Table 9: Report Builder – Filter Options

Entity	Attributes (filters)	Operator	Value	Column
Events	event_date	• equal_to • greater_than • greater_than_equal_to • less_than • less_than_equal_to	(date)	• audit_path (object path) • audit_objectname (object name) • audit_operation (operation) • audit_machine_name (source of operation) • audit_event_date (event date in UTC) • audit_username (user name)
	Event_operation	N/A	• file_write • file_read • file_create • file_delete • rename • directory_create • directory_delete • SecurityChange (permission change) • set_attr • sym_link	

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 702

Entity	Attributes (filters)	Operator	Value	Column
Files	Category	• equal_to • greater_than • greater_than_equal_to • less_than • less_than_equal_to	(date)	• object_name (file name) • share_UUID (share name) • object_owner_name (owner name) • object_size_logical (size) • file_type (extension) • object_creation_date (creation date in UTC) • last_event_date (access date in UTC) • share_UUID (share name) • fileserver_protocol • object_ID (file id) • object_last_operation_name (last operation) • audit_username (last operation user • object_last_operation_name (last operation) • file_path (file path)
	Extensions	N/A	(type in value)	
	Deleted	N/A	Last (number of days from 1 to 30) days	
	creation_date	• equal_to • greater_than • greater_than_equal_to • less_than • less_than_equal_to	(date)	
	access_date	• equal_to • greater_than • greater_than_equal_to • less_than • less_than_equal_to	(date)	
	Size	• equal_to • greater_than • greater_than_equal_to • less_than • less_than_equal_to	(number) (file size) File size options: • B • KB • MB • GB • TB	

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 703

Entity	Attributes (filters)	Operator	Value	Column
Folders	Deleted	N/A	Last (number of days from 1 to 30) days	• object_name (Dir name) • object_owner_name (owner name) • object_creation_date (creation date in UTC) • last_event_date (access date in UTC) • share_UUID (share name) • object_last_operation_name (last operation) • audit_username (last operation user) • File server protocol • object_ID (file id) • file_path (Dir path)
	creation_date	• equal_to • greater_than • greater_than_equal_to • less_than • less_than_equal_to	(date)	
Users	last_event_date	• equal_to • greater_than • greater_than_equal_to • less_than • less_than_equal_to	(date)	• user_login_name (user name) • Last operation • last_event_date (access date in UTC) • last_operation_audit_path

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 704

Table 10: Pre-Canned Reports – Filters

Entity	Pre-canned report template	Columns
Events	• PermissionDenied events • Permission Denied (file blocking) events	• audit_path (object path) • audit_objectname (object name) • audit_operation (operation) • audit_machine_name (source of operation) • audit_event_date (event date in UTC) • audit_username (user name)
Files	• Largest Files • Oldest Files • Files not accessed for last 1 year • Files accessed in last 30 days	• object_name (file name) • share_UUID (share name) • object_owner_name (owner name) • object_size_logical (size) • file_type (extension) • object_creation_date (creation date in UTC) • last_event_date (access date in UTC) • share_UUID (share name) • fileserver_protocol • object_ID (file id) • object_last_operation_name (last operation) • audit_username (last operation user • object_last_operation_name (last operation) • file_path (file path)
Users	• Top owners with space consumed • Top active users • All users	• user_login_name (user name) • Last operation • last_event_date (access date in UTC) • last_operation_audit_path

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 705

Creating a Custom Report

Create a custom report by defining the entity, attribute, filters, and columns.

About this task

Follow the steps as indicated.

Procedure

1. Go to **dropdown menu** > **Reports**.
2. Click **Create a new report**.
3. In the **Report Builder** tab, do the following:
   a. In the **Define Report Type** section, select an entity from the drop-down menu.
   b. In the **Define Filters** section, select an attribute from the attributes dropdown.
   c. Under **Value**, specify the values for the attribute (some attributes also require to specify an operator in the **Operator** field).
   d. (optional) click **+ Add filter** to add more attributes.
   e. In the **Add/Remove column in this report** section, click **x** for the columns you want to remove.
   f. In the **Define maximum number of rows in this report** section, type in , or use the **-**and **+** buttons, to specify the number of rows in your report. This value indicates the number of records in the report.
4. Click **Run Preview**.
   The **Report Preview** section populates.
5. Click **Generate report**.
   a. Select either the **CSV** or **JSON** option.

Create a Pre-Canned Report

Use one of the pre-canned File Analytics templates for your report.

Procedure

1. Go to **dropdown menu** > **Reports**.
2. Click **Create a new report**.
3. In the **Pre-Canned Reports Templates** tab, do the following:
   a. In the **Define Report Type** section, select an entity from the drop-down menu.
   b. In the **Define Filters** section, select an attribute from the attributes dropdown.
   c. In the **Add/Remove column in this report** section, click **x** for the columns you want to remove.
   d. In the **Define maximum number of rows in this report** section, type in, or use the **-** and **+** buttons, to specify the number of rows in your report. This value indicates the number of records in the report.
4. Click **Run Preview**.
   The **Report Preview** section populates.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 706

5. Click **Generate report**.
   a. Select either the **CSV** or **JSON** option.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 707

FILE ANALYTICS OPTIONS

This section provides information on additional File Analytics features and options.

You can get more insight into the usage and contents of files on your system by configuring and updating File Analytics features and settings. Some options include scanning the files on your file server on demand, updating data retention, and configuring data protection.

Updating Data Retention

The data retention period determines how long File Analytics retains event data.

About this task

Follow the steps as indicated to configure data retention.

Procedure

1. In File Analytics, click **gear icon** > **Update Data Retention**.
2. In the **Data Retention Period** drop-down, select the period for data retention.
3. Click **Update**.

Scanning the File System

Once enabled, File Analytics scans the metadata of all files and shares on the system. You can perform an on-demand scan of shares in your file system.

About this task

To scan shares, perform the following task.

Procedure

1. In File Analytics, click the **gear icon**.
2. In the drop-down list, click **Scan File System**.
3. In the list of shares, select the target shares for the scan.
4. Click **Scan**.
   The status of the share is **In Progress**. Once the scan is complete, the status changes to **Completed**.

Managing the Deny List

Deny users, file extensions, and client IP addresses.

About this task

Use the deny feature to block audit events on specified file extensions or by specified users and clients. You cannot deny files without an extension.

Procedure

1. Click the **gear icon** > **Define Rules for Deny List**.
2. Click the pencil icon in the *Client IPs*, *File Extensions*, *Users* row.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 708

3. Add a comma-separated list of entities to be blocked.
4. Click the **done** icon in the updated row.
5. Click **Close**.

Managing File Categories

File Analytics uses the file category configuration to classify file extensions.

About this task

The capacity widget in the dashboard uses the category configuration to calculate capacity details. Follow the steps as indicated to manage the file categories.

Procedure

1. Click **gear icon** > **Manage File Category**.
2. To create a category, click **+ New Category**. (Otherwise, move on to step 3).
   a. In the **Category** column, name the category.
   b. In the **Extensions** column, specify file extensions for the category.
3. To delete an existing category, click the **x icon** next to the category. (Otherwise, move on to step 4)
4. To modify an existing category, click the **pencil icon** next to the category and modify the specified file extensions.
5. Click **Save**.

Data Protection

Configure File Analytics disaster recovery (DR) using Prism Element.

File Analytics only supports Async disaster recovery. File Analytics does not support NearSync and Metro Availability.

Create an Async protection domain, configure a protection domain schedule, and configure remote site mapping. The remote site must have symmetric configurations to the primary site. The remote site must also deploy File Analytics to restore a File Analytics VM (FAVM).

For information on disaster recovery, see the *Data Protection and Recovery with Prism Element* guide.

> **Tip:** To protect data on the FAVM, Nutanix recommends setting up a protection domain with a DR policy that has a minimum frequency of one week.

Configuring Disaster Recovery

To set up disaster recovery for File Analytics, create an async protection domain, configure a protection domain schedule, and configure remote site mapping.

About this task

By default, the File Analytics volume group resides on the same container that hosts vDisks for Nutanix Files.

Procedure

1. If you have not done so already, configure a remote site for the local cluster.
   See the *Configuring a Remote Site (Physical Cluster)* topic in the *Prism Web Console Guide* for this procedure.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 709

2. Create an async DR protection domain for the File Analytics volume group as the entity. The volume group name is `File_Analytics_VG`.

   See *Configuring a Protection Domain (Async DR)* in the **Prism Web Console Guide**.

3. In the **Schedule** tab, click the **New Schedule** button to add a schedule.

   Add a schedule, as File Analytics does not provide a default schedule. See *Creating a Protection Domain Schedule (Files) Nutanix Files Guide*.

4. Configure local and remote container mapping.

   See the *Configuring Disaster Recovery (Files)* section in the *Nutanix Files Guide* for steps to configure mapping between local and remote containers.

5. Create a protection domain schedule.

   See *Creating a Protection Domain Schedule (Files)* in the *Nutanix Files Guide*.

Activating Disaster Recovery

Recover a File Analytics VM (FAVM) after a planned or unplanned migration to the remote site.

About this task

Perform the following steps on the remote site.

Procedure

1. Fail over to the protection domain for disaster recovery activation.

   See the *Failing Over a Protection Domain* topic in the *Data Protection and Recovery with Prism Element Guide*.

2. Fail back the protection domain to the primary site.

   See the *Failing Back a Protection Domain* topic in the *Data Protection and Recovery with Prism Element Guide*.

Deploying File Analytics on a Remote Site (AHV)

Deploy a File Analytics VM (FAVM) after a planned or unplanned (disaster) migration to the remote site.

About this task

To perform disaster recovery, deploy and enable File Analytics on the remote site. Restore the data using a snapshot of the volume group from the primary FAVM.

Before you begin

Ensure that the Nutanix Files and AOS versions match the versions on the remote and primary sites.

About this task

Use the following commands from the command prompt inside the FAVM.

Procedure

1. Deploy a new File Analytics instance on the remote site, see Deploying File Analytics on page 6.

   > **Caution:** Do not enable File Analytics.

   The remote site requires an iSCSI data service IP address to configure the FAVM on the remote site. This procedure deploys a new volume group File_Analytics_VG and deletes in a subsequent step.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 710

2. On the remote site, create a volume group by restoring the snapshot of the File_Analytics_VG.

   See *Restoring an Entity from a Protection Domain* in *Data Protection and Recovery with Prism Element* guide. For the **How to Restore** step, use the **Create new entities** option, and specify a name in the **Volume Group Name Prefix** field. The restored volume group name format is *prefix*-File_Analytics_VG.

3. To configure the FAVM on the remote site, follow these steps:

   > **Caution:** If the IP address of the File Analytics VM has changed on the remote site, contact Nutanix Support before proceeding.

4. Log on to the FAVM with SSH.

   > **Tip:** See KB 1661 for default credential details.

5. Discover all storage devices accessed by the FAVM.

   ```
   nutanix@favm$  sudo blkid
   ```

6. Copy the cvm.config file to the temporary files directory.

   ```
   nutanix@favm$ sudo cp /mnt/containers/config/common_config/cvm.config /tmp/
   cvm.config
   ```

7. Stop the File Analytics services.

   ```
   nutanix@favm$  sudo systemctl stop monitoring
   ```

   ```
   nutanix@favm$  docker stop $(docker ps -q)
   ```

   ```
   nutanix@favm$  sudo systemctl stop docker
   ```

8. Un-mount the volume group.

   ```
   nutnix@avm$ sudo umount /mnt
   ```

9. Detach the volume group File_Analytics_VG from the FAVM.

   See the "Managing a VM (AHV)" topic in the *Prism Element Web Console Guide*.

10. Attach the cloned volume group *prefix*-File_Analytics_VG to the FAVM.

    See "Managing a VM (AHV)" in the *Prism Element Web Console Guide*.

11. Restart the FAVM to discover the attached volume group.

    ```
    nutanix@avm$ sudo reboot
    ```

12. Log on to the FAVM with SSH.

    > **Tip:** See KB 1661 for default credential details.

13. Discover all storage devices accessed by the FAVM.

    ```
    nutanix@favm$  sudo blkid
    ```

    ```
    /dev/sr0: UUID="ALPHA-NUMERIC-UUID" LABEL="cidata" TYPE="NUMERIC-ISO"
    /dev/sda1: LABEL="_master-x86_64-2" UUID="ALPHA-NUMERIC-UUID" TYPE="ext4"
    ```

    The FAVM discovers the attached volume group and assigns to the /dev/sdb device.

14. Delete the deployed volume group File_Analytics_VG.

    See the "Modifying or Deleting a Volume Group" topic in the *Prism Element Web Console Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 711

15. Rename the restored volume group *prefix*-File_Analytics_VG to File_Analytics_VG.

    See the "Modifying or Deleting a Volume Group" topic in the *Prism Element Web Console Guide*.

16. Create a backup of the cvm.config file.

```
nutanix@favm$ mv /mnt/containers/config/common_config/cvm.config \
/mnt/containers/config/common_config/cvm_bck.config
```

17. Copy the cvm.config file from the /tmp directory to /common_config/ on the FAVM.

```
nutanix@favm$ sudo mv /tmp/cvm.config /mnt/containers/config/common_config/
```

18. Get ownership of the cvm.config.

```
nutanix@favm$ sudo chown nutanix: /mnt/containers/config/common_config/cvm.config
```

19. Reconfigure the password of the user on Prism for internal FAVM operations. Specify a pass-phrase for *new_password*. File Analytics uses the password only for internal communication between Prism and the FAVM. You must issue the same command twice.

```
nutanix@favm$ sudo python3 /opt/nutanix/analytics/bin/reset_password.py --
user_type=prism \
 --password='new_password' --local_update
```

```
nutanix@favm$  sudo python3 /opt/nutanix/analytics/bin/reset_password.py --
user_type=prism \
--password='new_password' --prism_user=admin --
prism_password='Prism_admin_password'
```

20. In File Analytics, go to **gear icon** > **Scan File System** to check if File Analytics can initiate a file system scan.

    If you receive errors, disable and re-enable File Analytics, see Disabling File Analytics on page 11 and Enabling File Analytics on Prism Element on page 8.

Deploying File Analytics on a Remote Site (ESXi)

Deploy a File Analytics VM (FAVM) after a planned or unplanned (disaster) migration to the remote site.

About this task

To perform disaster recovery, deploy and enable File Analytics on the remote site. Restore the data using a snapshot of the volume group from the primary FAVM.

Before you begin

Ensure that the Nutanix Files and AOS versions match the versions on the remote and primary sites.

About this task

Use the following commands from the command prompt inside the FAVM.

Procedure

1. Deploy a new File Analytics instance on the remote site, see Deploying File Analytics on page 6.

   Caution: Do not enable File Analytics.

   The remote site requires an iSCSI data service IP address to configure the FAVM on the remote site. This procedure deploys a new volume group File_Analytics_VG and deletes in a subsequent step.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 712

2. On the remote site, create a volume group by restoring the snapshot of the File_Analytics_VG.

   See *Restoring an Entity from a Protection Domain* in *Data Protection and Recovery with Prism Element* guide. For the **How to Restore** step, use the **Create new entities** option, and specify a name in the **Volume Group Name Prefix** field. The restored volume group name format is *prefix*-File_Analytics_VG.

3. In the **Storage Table** view, go to the **Volumes** tab.

   a. Copy the target IQN prefix from the **Volume Group Details** column.

   > **Tip:** Click the tooltip to see the entire IQN prefix.

Configure the FAVM on the remote site

4. To configure the FAVM on the remote, follow these steps:

   > **Caution:** If the IP address of the File Analytics VM has changed on the remote site, contact Nutanix Support before proceeding.

5. Log on to the FAVM with SSH.

   > **Tip:** See KB 1661 for default credential details.

6. Discover all storage devices accessed by the FAVM.

   ```
   nutanix@favm$  sudo blkid
   ```

7. Copy the cvm.config file to the temporary files directory.

   ```
   nutanix@favm$ sudo cp /mnt/containers/config/common_config/cvm.config /tmp/
   cvm.config
   ```

8. Stop the File Analytics services.

   ```
   nutanix@favm$  sudo systemctl stop monitoring
   ```

   ```
   nutanix@favm$  docker stop $(docker ps -q)
   ```

   ```
   nutanix@favm$  sudo systemctl stop docker
   ```

9. Un-mount and log off from all iSCSI targets.

   ```
   nutnix@avm$ sudo umount /mnt
   ```

   ```
   nutnix@avm$ sudo /sbin/iscsiadm -m node -u
   ```

10. Remove the disconnected target records from the discoverydb mode of the FAVM.

    ```
    nutanix@favm$  sudo /sbin/iscsiadm -m node –o delete
    ```

11. Discover all storage devices accessed by the FAVM.

    ```
    nutanix@favm$  sudo blkid
    ```

    ```
    /dev/sr0: UUID="ALPHA-NUMERIC-UUID" LABEL="cidata" TYPE="NUMERIC-ISO"
    /dev/sda1: LABEL="_master-x86_64-2" UUID="ALPHA-NUMERIC-UUID" TYPE="ext4"
    ```

    The output does not show the /dev/sdb device.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 713

12. Get the File Analytics Linux client iSCSI initiator name.

```
nutanix@favm$  sudo cat /etc/iscsi/initiatorname.iscsi
```

The output displays the initiator name.

```
InitiatorName=iqn.xxxx-xx.com.redhat:ALPHA-NUMERIC-ID
```

13. Copy the iSCSI initiator name.

14. Remove the iSCSI initiator name from the client whitelist of the deployed volume group File_Analytics_VG.

See the "Modifying or Deleting a Volume Group" topic in the *Prism Element Web Console Guide*.

15. Whitelist the FAVM client on the cloned volume group *prefix*-File_Analytics_VG using the iSCSI initiator name of the FAVM client.

See the "Modifying or Deleting a Volume Group" topic in the *Prism Element Web Console Guide*.

16. Let the Analytics initiator discover the cluster and its volume groups.

```
nutanix@favm$  sudo /sbin/iscsiadm --mode discovery --type sendtargets --portal
  data_services_IP_address:3260
```

Replace *data_services_IP_address* with the data service IP address. Clicking the Nutanix cluster name in Prism displays cluster details including the data service IP address. The output displays the restored iSCSI target from step 2.

17. Connect to the volume target by specifying IQN prefix.

```
nutanix@favm$  sudo /sbin/iscsiadm --mode node --targetname iqn_name --
portal data_services_IP_address:3260,1 --login
```

Replace *iqn_name* with the IQN prefix and ensure it ends with the `-tgt0` suffix.

Replace *data_services_IP_address* with the data service IP address.

18. Restart the FAVM to restart the iSCSI host adapters, which allows the discovery of the attached volume group.

```
nutanix@favm$  sudo reboot
```

19. Log on to the FAVM with SSH.

> **Tip:** See KB 1661 for default credential details.

20. Discover all storage devices accessed by the FAVM.

```
nutanix@favm$  sudo blkid
```

The FAVM discovers the attached iSCSI volume group and assigns to the /dev/sdb device.

```
/dev/sr0: UUID="ALPHA-NUMERIC-UUID" LABEL="cidata" TYPE="NUMERIC-ISO"
/dev/sda1: LABEL="_master-x86_64-2" UUID="ALPHA-NUMERIC-UUID" TYPE="ext4"
/dev/sdb: UUID="ALPHA-NUMERIC-UUID" TYPE="ext4"
```

21. Delete the deployed volume group File_Analytics_VG.

See the "Modifying a Volume Group" topic in the *Prism Element Web Console Guide*.

22. Rename the restored volume group *prefix*-File_Analytics_VG to File_Analytics_VG.

See the "Modifying or Deleting a Volume Group" topic in the *Prism Element Web Console Guide*.

23. Create a backup of the cvm.config file.

```
nutanix@favm$ mv /mnt/containers/config/common_config/cvm.config \
/mnt/containers/config/common_config/cvm_bck.config
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 714

24. Copy the cvm.config file from the /tmp directory to /common_config/ on the FAVM.

```
nutanix@favm$ sudo mv /tmp/cvm.config /mnt/containers/config/common_config/
```

25. Get ownership of the cvm.config.

```
nutanix@favm$ sudo chown nutanix: /mnt/containers/config/common_config/cvm.config
```

26. Reconfigure the password of the user on Prism for internal FAVM operations. File Analytics uses the password only for internal communication between Prism and the FAVM. You must issue the same command twice.

```
nutanix@favm$ sudo python3 /opt/nutanix/analytics/bin/reset_password.py --
user_type=prism \
 --password='new_password' --local_update
```

```
nutanix@favm$  sudo python3 /opt/nutanix/analytics/bin/reset_password.py --
user_type=prism \
--password='new_password' --prism_user=admin --
prism_password='Prism_admin_password'
```

Replace *new password* with a new pass phrase.

Replace *Prism_admin_password* with the password of the Prism admin.

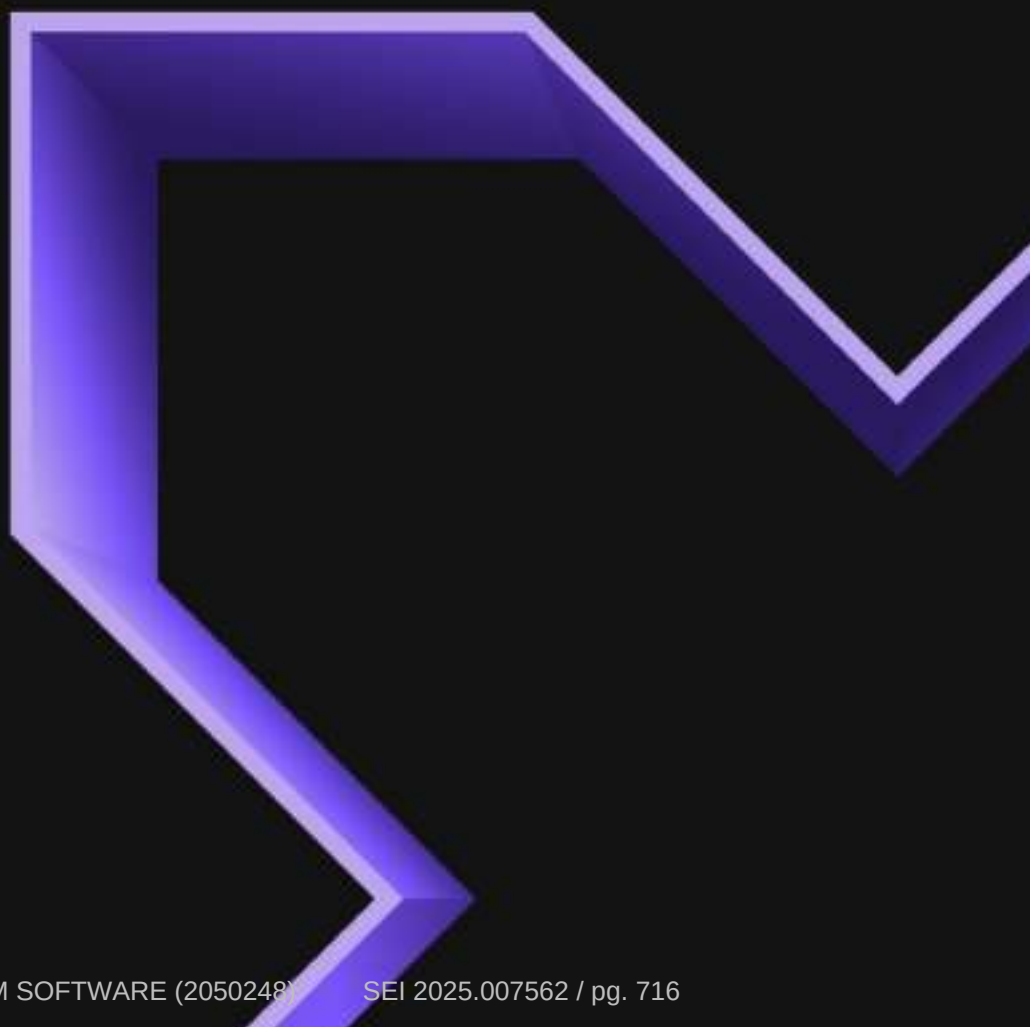
27. In File Analytics, go to **gear icon** > **Scan File System** to check if you can initiate a file system scan.

> **Note:** If you receive errors, disable and re-enable File Analytics, see Disabling File Analytics on page 11 and Enabling File Analytics on Prism Element on page 8.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 715

Objects User Guide

Objects 4.2
January 28, 2024



NUTANIX

Contents

Nutanix Objects Overview 6
- Salient Features of Objects 6
- Usage of Objects 7
- Use Cases and Recommendations for NFS on Objects 8
- NFS-S3 Interoperability 8
- Advantages of Objects 10
- Objects Architecture 11
- Terminology Reference 12
- Objects Workflow 13

Enabling Objects 14

Finding Objects Version 18

Objects Security Hardening Instructions 19
- Protecting Objects Network with Flow (Microsegmentation) 21

Objects License Management 25
- Open Source Software Usage 25

Objects LCM Upgrades 26
- Microservices Platform (MSP) 27
  - Finding the MSP Version 27
  - Finding the Primary and Secondary MSP Clusters 27
  - Upgrading MSP Controller 27
- Upgrading Objects Manager 28
- Upgrading Objects Service 29

Role-based Access Control for Objects 30
- Prerequisites for Configuring Role-based Access Control for Objects 30
- Role-Based Access Control Workflows for Objects 31
  - Objects Permissions 31
  - Creating Full Administrator Role for Objects 32
  - Creating View-only Administrator Role for Objects 33
  - Creating Bucket Administrator Role for Objects 33
  - Creating Infra Administrator Role for Objects 36
  - Creating a Custom Role for Objects 37

Deployment and Network Prerequisites 40
- Deployment Prerequisites - AHV and ESXi 40
- Prerequisites - ESXi 41
- Network Configuration 42

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 717

AHV Configuration....43
ESXi Configuration....47
Shared Versus Single Network....54
URL and Port Requirements....55
Limitations....59
Limitations of NFS....59

Federation Overview....61
Prerequisites - Federated Namespace....61
Creating Federated Namespace....62
Managing Federated Namespace....65
Viewing Federated Namespaces....66
Deleting Federated Namespace....67
Errors in Federated Namespace....68

Object Store Service Deployment....70
Object Store Instance Naming Conventions....70
Creating or Deploying an Object Store (Prism Central)....70
Viewing Object Store Deployments....78
Access Objects Endpoints....81
Viewing Object Store Summary....81
Deleting an Object Store....82
Object Store Expansion....83
Expanding Storage for an Object Store....84
Scaling Out an Object Store....88
Managing FQDN and SSL Certificate....93
Adding FQDNs....94
Setting up SSL Certificate for an Object Store....96
Deploying Object Store on Nutanix Cloud Cluster....98
Deploying Object Store at a Dark Site (Offline Deployment)....98

Types of Objects Users....105

Directory Configuration and Access Key Generation....106
Objects IAM-High Availability Overview....106
Configuring Directories....106
Generating Access Key for API Users....110
Viewing API Users....114
Managing API Keys....115
Deleting API Users....116

Bucket Creation, Operations, and Bucket Policy Configuration....118
Bucket Naming Conventions....118
Creating and Configuring an S3 Bucket....118
Creating and Configuring an NFS Bucket....120
Managing NFS Allowlist....124
Bucket Policy Configuration....127
Object Versioning....127
Lifecycle Policies....128
Cloud Tiering....130
Legal Hold for Objects....138

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 718

WORM Bucket....139
Configuring a Bucket for Static Website Hosting....141
Cross-Origin Resource Sharing (CORS) Overview....144
Adding Tags to a Bucket....146
Viewing Buckets....147
Bucket Summary....149
Updating a Bucket....150
Sharing a Bucket....151
Bucket Access Policies....153
Listing the Shared Buckets....157
Viewing Bucket Users....158
Editing User Access....159
Deleting a Bucket....161

Objects Browser....163
Administrator Workflow: Objects Browser....163
Launching the Objects Browser....165
Supported Operations....167
Bucket Operations....167
Object CRUD Operations....179
Bucket Summary....188

Objects Streaming Replication....189
Replication Guarantees and Topologies....190
Replication Prerequisites....193
Adding Remote Prism Central as Availability Zone....193
Setting up IAM Synchronization with a Different PC....195
Prerequisites for Creating a Replication Rule....197
Creating Replication Rules for Buckets....198
Objects Streaming Replication Scenarios....200
Deleting a Replication Relation....201
Viewing Bucket Replication Statistics....201
Achieving Fault Tolerance for IAM....203

Baseline Replicator Tool....206
Accessing and Running the Baseline Replicator Tool....206

Objects Prometheus Exporter....209

Monitoring and Alerts....211
Viewing Performance of Object Stores....211
Viewing Performance of Buckets....212
Viewing Object Store Usage....214
Assigning Quota Policy to a User....215
Viewing Alerts....218
Nutanix Objects Specific Alerts....219

Objects Notifications....224
Notification Types for Objects....224
Configuring Events Notification....229

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 719

Creating Notification Rules for Data Events....235

CRUD Operations by Using S3 APIs....239
Authentication....239
Supported and Unsupported APIs....239
Supported APIs....240
Unsupported APIs....243
Buckets and Objects Tagging APIs Overview....244
API Operations Supported for Buckets and Objects Tagging....245
S3 Select API Overview....246
Supported SQL Functions....247

Error Responses....252
REST Error Responses....252
List of Error Codes....252

Integration with Backup Applications....255

Troubleshooting Objects....256
Shutting Down Objects VMs....256
Starting the Objects VMs....258
Detection of Slow Connections....259
Prism Element Clusters or Subnets Not Listed in the User Interface....259
Object Stores Not Listed While Creating a Replication Rule....260
Manually Updating the DNS Server for an Objects Cluster....260

Copyright....262

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 720

NUTANIX OBJECTS OVERVIEW

Nutanix Objects™ (Objects) is a software-defined Object Store Service. This service is designed with an Amazon Web Services Simple Storage Service (AWS S3) compatible REST API interface capable of handling petabytes of unstructured and machine-generated data. Objects addresses storage-related use cases for backup, and long-term retention, and data storage for your cloud-native applications by using standard S3 APIs. You no longer have to introduce an external, separately managed storage solution.

Objects is deployed and managed as part of the Nutanix Enterprise Cloud OS. It enables users of the Nutanix platform to store and manage unstructured data on top of a highly scalable hyper-converged architecture. In comparison to cloud-hosted solutions, this on-premises model offers more consistent control over the costs associated with storing objects, along with more transparency about the location of those objects.

You can manage objects by using Prism Central or the S3-compatible REST APIs after an administrator has authorized the applications and users to access buckets accordingly.

For more information about Objects architecture, refer to *Nutanix Bible*.

Salient Features of Objects

The salient features of Objects are as follows:

Write-Once-Read-Many (WORM)

Nutanix Objects enables you to create WORM buckets to prevent anyone (including an administrator) from modifying or deleting data while the policy is active. WORM policies help you comply with strict regulations often mandated by the healthcare, financial, and government sectors. You can apply WORM policies to any bucket to prevent any updates to the data until the WORM policy expires. Nutanix provides a 24-hour grace period for letting you test the WORM policy. The bucket creator can undo the applied policy within the allowed grace period of 24 hours. After the grace period, no one can delete the policy or reduce the retention period. The option to extend the retention period is available. You must enable versioning on a WORM bucket so that you can update an object. The updated object gets stored as a new version. Versioning ensures that older versions of the object get retained, and the data never gets overwritten. For more information, see WORM Bucket on page 139.

Immutability

Retrieved data must be the same as originally written. This means that you can retrieve the stored object (and its associated metadata) in the future without any modification. If you enabled WORM, the object remains unchanged and is also undeletable.

Object Versioning

When you enable object versioning, uploading multiple copies of the same object creates multiple versions. You can use the versioning feature to protect data from accidental overwrite or deletion or as an option for reverting to a previous state. You can also disable object versioning on a bucket at any time and set the objects in the bucket to expire after a specified time. By default, there is no limit on the number of versions for an object, considering the storage space is available. For more information, see Object Versioning on page 127.

Data Life Cycle Management

You can use age-based data retention policies to enforce compliance with strict data retention regulations that dictate the time to store specific data. For example, HIPAA regulation mandates you to retain medical data for six years from the creation date. You can set a data retention policy to delete all data created in a specific bucket six years after its creation date.

Note: The WORM policy supersedes any set retention policy.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 721

You can set retention policies at the bucket level where objects in a bucket expire after a certain amount of time you specify. If you do no set retention policies, the only limit to how many versions can be maintained depends on the storage space. For more information, see Lifecycle Policies on page 128.

Multipart Upload

Multipart upload allows you to reduce slow upload times by breaking large pieces of data into chunks. Then, the system can handle the data separately to increase upload speeds if you upload them simultaneously. You can also use multipart uploads to prevent losing progress during an upload. For example, if there is a connectivity loss, most applications retry only the unsuccessful chunk. Hence, you do not have to upload the entire object again. For more information, see Supported APIs on page 240.

Data-at-Rest Encryption with Native Key Management

Nutanix Objects provides a FIPS 140-2 compliant data-at-rest encryption solution. To deliver this capability, Objects uses the underlying AOS encryption capability. You can set encryption at an entire cluster level, always encrypting all data. With the native key management, the Nutanix cluster manages the keys, so the solution requires no additional device management or third-party costs.

Identity and Access Management

Native IAM functionality ensures that you have access only to the buckets and objects you created and granted access permissions. Each user gets a pair of access and secret keys that can be used by their applications to access Nutanix Objects. You can also generate access and secret keys for an Active Directory group. Administrators can revoke and regenerate keys at any time. For more information, see Directory Configuration and Access Key Generation on page 106.

Multi-protocol Access

Objects allows you to create buckets using both S3 and NFS protocols. NFS protocol support is natively implemented over Objects and build on the same foundation that powers the S3 protocol. For more information, see Use Cases and Recommendations for NFS on Objects on page 8, NFS-S3 Interoperability on page 8, Limitations of NFS on page 59, Creating and Configuring an NFS Bucket on page 120, and Creating and Configuring an S3 Bucket on page 118.

Usage of Objects

Following are examples of solutions you can implement by using Objects:

- **Backup** –

  You can integrate Objects with the backup applications such as Commvault, HYCU, Veeam, and Veritas. You can create backups to protect your data with a simple, scalable, and cost-effective active archive solution. You can start with small storage and scale to petabytes of storage to deliver great performance. Objects supports the multipart upload API with which you can reduce slow upload times by breaking data into chunks and upload documents, images, and videos to the global namespace.

- **Long-term Retention** –

  You can use Objects for long-term data retention. Built-in object versioning provides storage protection and searches your data without the problem of tape systems. Versioning maintains previous copies of the object to avoid data loss from overwrites or deletes.

  Some organizations, especially in the health, legal, and government sectors, require to comply with the strict regulations mandating requirements such as the minimum period for which data must be available or who can alter data. Nutanix Objects allows you to store data over a long period with features designed to comply with such strict regulations. For example, WORM buckets prevent anyone (including an administrator) from modifying or deleting data while the policy is active.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 722

- **DevOps** –

  Easy application access to your data in a global namespace using simple PUT and GET commands makes Objects the perfect fit for your dev-ops data. Nutanix Objects offers broad support for most programming environments, and you can access it using standard internet networking infrastructures, such as HTTP and HTTPS protocols. With Nutanix Objects, you can easily access the objects with S3-compatible HTTP REST API requests from different locations. The bucket-level metrics allow you to track resource utilization with ease. Also, Identity and Access Management (IAM) support enable secure access to Objects resource and services.

  DevOps and IT ops can use the S3-compatible interface for cross-geo, cross-team collaboration, and agile development.

  Consider the following scenario. Joe and Adam work together on the same team as developers for an image processing application called XYZ. Joe, residing in New York, develops code for the data creation and storage of XYZ. Adam, residing in Seattle, performs the testing of XYZ. Several buckets dedicated to the application XYZ are stored in the Nutanix Objects store instance deployed in the New York office. After completing the programming for the latest feature, Joe stores the latest version of XYZ in a bucket. Adam can use GET request automation-scripts to pull the latest version of the code and store the latest test results into another bucket using PUT requests.

  Thus, the team works more efficiently and quickly. Also, it demonstrates the immutable capabilities of object storage, where Joe's data remains unchanged while Adam performs testing.

Use Cases and Recommendations for NFS on Objects

Use Cases

NFS protocol support provides multiprotocol access (NFS 3.0, S3) to data stored within Objects buckets. NFS protocol support is natively implemented over Objects and builds on the same foundation that powers the S3 protocol.

NFS access over Objects is ideally suited for large-scale, read-heavy workloads with sequential accesses where data is ingested once and minimally or never modified later. Some ideal uses are:

- **Backup applications** – use Objects as a large-scale NFS repository for backups while you migrate the underlying storage to Objects.
- **Analytics** – use Objects multiprotocol access for in place analytics as you ingest data through object or S3 interface and access through file or NFS interfaces that analytic systems require.

Recommendations

Nutanix recommends the following:

- Not to use NFS access over Objects for use cases that require modification to data including file edits and renames. For example, end user computing, home shares, app data that is frequently modified like presentations or CAD files.
- To have up to 100 subdirectories within a directory and a total of up to 100 million objects within a NFS bucket.
- To use `nconnect=1` mount option for NFS buckets.

NFS-S3 Interoperability

This section explains how objects in the S3 namespace get mapped to files and directories in the NFS namespace and vice-versa.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 723

NFS to S3

- All the files and symbolic links created in the NFS namespace appears in the S3 namespace as objects.
- Any directory created from the NFS namespace will not appear in the S3 namespace as S3 protocol does not have any notion of directories.
- Any S3 operation like ObjectHead, ObjectGet or ObjectDelete on the directories fails with the error message `NfsDirectoryOperationNotAllowed (Operation prohibited on an NFS directory)`. Therefore, a file present inside directories and subdirectories appears as a single object in the S3 namespace as shown in the following table:

Table 1: NFS to S3

NFS	S3

• dir1/
  • dir2/
  • file
	dir1/dir2/file

S3 to NFS

- Objects created from the S3 protocol appears as files and directories in the NFS namespace based on the object name. If the object name contains a directory-like hierarchy, then the object is stored in a hierarchical namespace as identified its name.

  Following table shows an example where an object `a/b/c` created from S3 protocol appears in the NFS namespace as `a/`directory which contains the subdirectory `b/` which in turn contains the file `c`.

Table 2: S3 to NFS

S3	NFS

a/b/c	• a/
	  • b/
	  • c

Note:

- These implicit directories are created when an object containing directory hierarchy is accessed from the NFS namespace.
- The implicit directories continue to exist in the NFS namespace after the object containing directory hierarchy has been deleted.
- Folders created from the Objects Browser also appears as a directory in the NFS namespace.

For more information about the Limitations of NFS on Objects, refer to Limitations of NFS on page 59.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 724

Advantages of Objects

Following are the advantages of object storage with Nutanix Objects:

No Silos

Nutanix provides file services (Files) and block services (Volumes) as part of the Acropolis Distributed Storage Fabric (DSF). You can also add Nutanix Objects to the solution, thus allowing block, file, and object storage solutions to coexist with no silos. You can deploy and manage these features in a single environment.

Security-First Approach

Nutanix integrates security into every step of its solution stack from the early stages of development. For example, the stack conforms to Security Technical Implementation Guides (STIGs), which maintain a security baseline configuration based on common standards established by the National Institute of Standards and Technology (NIST). STIGs use machine-readable code to automate self-healing and compliance with the security standards for AOS and AHV. Nutanix also complies with *SEA 17a-4*, which specifies requirements for data retention and accessibility. Nutanix Objects also supports Data-at-Rest Encryption.

Capacity Optimization

Nutanix Objects leverages data-capacity optimization technologies such as compression and erasure coding (EC-X) in the background. In addition to compression savings, EC-X increases the usable storage capacity in a cluster with no overhead to the active path write.

In a cluster with the redundancy factor 2, two copies of the data get replicated among all nodes for resilience. Checksums of the data are stored with the metadata to ensure validity if corruption occurs. Therefore, the cluster (redundancy factor 2) uses half of its raw storage capacity to store copies of its data. EC-X performs the OR operation on these copies of data to compute a parity block. The original data blocks and the parity form an erasure code strip. This process reduces the number of actual data copies needed to protect the environment from a single node failure.

Due to the computational overhead of calculating parity during write operations, EC-X is suitable for workloads with infrequent write operations such as Objects with WORM policies enabled.

Suppose you have three data blocks (A, B, and C) stored in a four-node cluster, with each data block distributed across three nodes. Without EC-X, you may have the original three blocks of data plus three more copies of those blocks, which sum up to a total of six blocks of data. With EC-X enabled, you can reduce the storage footprint to four blocks of data that include the original three blocks of data plus their parity. These blocks are present in different nodes. If a node fails, the system can reconstruct the data from the data blocks and parity data present on the available nodes. Example: If the node hosting block B fails, the system can reconstruct its data from blocks A, C, and P (parity).

Additionally, when the disks are not getting used heavily, the system regularly performs background checksum validations and data restoration to maximize protection against data corruption. These techniques (combined with a high tolerance for disk and node failures in a self-healing and distributed system) form a resilient and reliable enterprise object-storage platform.

Ease of Use and Simple Management

Nutanix Objects is compatible with HTTP S3 REST APIs for object and bucket storage. Objects supports all the necessary methods (including `GET`, `PUT`, `POST`, `DELETE`, and `LIST`) to perform basic object operations.

Nutanix Objects inherits the simplicity of use and management of Prism Central and provides the managing, monitoring, and reporting capabilities that are simple to administer.

For example, Prism Central automatically provides checks for interoperability and compatibility during a software update task. Alerts inform users about specific conditions, such as object storage components hitting capacity thresholds and reduced High Availability (HA). The Prism GUI reports

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 725

on the size of the object store, the number of buckets and objects, average throughput, latency, and the number of GET and PUT operations.

Cost

With Nutanix Objects, the cost to store a large amount of unstructured data is less compared to traditional storage solutions. Compared to public cloud providers, Nutanix Objects does not charge for data ingress or egress.

Objects Architecture

Nutanix Objects integrates with the solution stack through services that run inside the Prism Central VM and manage all the other components and services of object storage.

The Nutanix cluster deploys VMs to handle the multiple components that provide the object storage API and lookups for the objects. These components run as containerized services in a Kubernetes cluster. Objects follows a modular and scale-out design where each component focuses on a single core function, thus allowing you to scale out any component independently to match the workload demands.

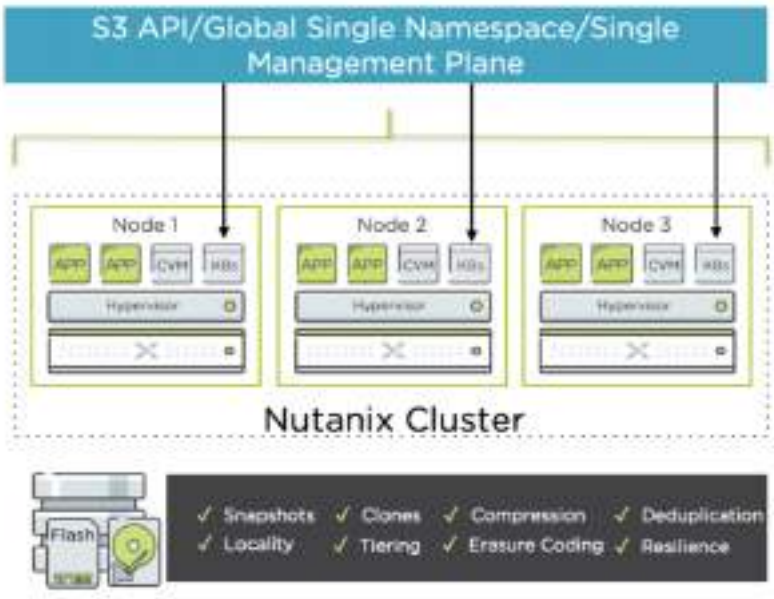


Figure 1: S3-Compatible Objects Storage Integrated with Nutanix

When you make GET and PUT requests to your object storage endpoint, you first hit the front-end adapter, a native, built-in load balancer that manages the S3 REST API calls and directs them to the right worker VM.

The worker VM runs different services that include the following:

- An object controller service, which supervises the data management layer that interfaces with AOS and coordinates with the metadata service.
- A metadata service that manages the metadata and serves as a general key-value store that also handles partitioning and region mapping.
- A life cycle management service that controls life cycle, audits, and background maintenance activities.
- An identity and access management service that handles user authentication for accessing buckets.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 726

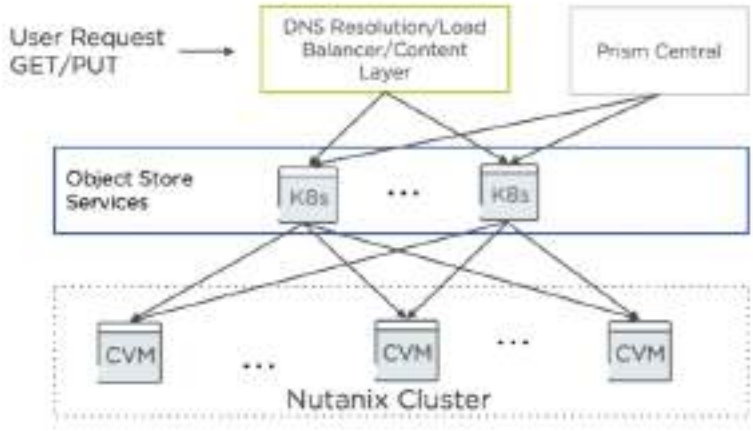


Figure 2: Objects Layered Architecture

Terminology Reference

Following are the terms that you frequently encounter when you are using Objects:

Table 3: Terminology Reference

Terminology	Description
Bucket	An organizational unit exposed to the users and contains the objects. A deployment may have one or more buckets.
Object	Object represents the data uploaded by the user or application. The actual unit (blob) of storage and the item interfaced by using the API (GET or PUT).
S3	The term used to describe the Amazon Web Services (AWS) interface. This term is now used synonymously for an object service. S3 is also used to describe the object API which you use to interact with an object store.
Storage Network	A VLAN required for communication between Objects services.
Public Network	A VLAN used to access the object store endpoints externally.
Microservices Platform (MSP)	A platform based on Kubernetes where all the Objects microservices run.
AHV IPAM	IP Address Management (IPAM) is a feature of AHV that allows it to assign IP addresses automatically to VMs by using DHCP. You can configure each virtual network with a specific IP address subnet, associated domain settings, and groups of IP address pools available for assignment to VMs.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 727

Terminology	Description
Worker VMs	Virtual machines created during object store deployment that host various containerized Objects services. Also, Worker VMs are referred to as Objects nodes.
Objects Browser	A User Interface (UI) that allows the users to directly launch the object store instance in a web browser and perform bucket and object level operations.

Objects Workflow

This section describes the basic workflow of Objects. The subsequent sections provide detailed information about each step.

About this task

Following is the Objects workflow:

Procedure

1. Enable Objects from Prism Central. Refer to Enabling Objects on page 14.
2. Deploy object store on a desired cluster. Refer to Object Store Service Deployment on page 70.
3. Generate the access keys. Refer to Generating Access Key for API Users on page 110.
4. Set up the Secure Sockets Layer (SSL) certificates for the object store. Refer to Setting up SSL Certificate for an Object Store on page 96.
5. Access the object store endpoints from the third-party clients or Objects Browser. Refer to Access Objects Endpoints on page 81 and Objects Browser on page 163.
6. Create buckets using either S3 or NFS protocol. Refer to Bucket Creation, Operations, and Bucket Policy Configuration on page 118.
7. Upload objects and perform object operations using Objects Browser or S3 APIs. Refer to Supported Operations on page 167 and Supported APIs on page 240.
8. Expand the object store if the storage is getting full. Refer to Expanding Storage for an Object Store on page 84.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 728

ENABLING OBJECTS

To create an object store, you first need to enable Objects in Prism Central then add a license in Prism Element or Prism Central depending on the versions in use. With the new PC experience, users with Objects Admin role cannot enable Objects service. Objects service can only be enabled by Super Admin or Prism Admin users.

Before you begin

A non-admin user can enable objects only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions:

- Cluster Admin
- User Admin

> **Note:** Administrators and non-admin users are Prism Central users with the following roles:
>
> - Administrator—A Super Admin or a Prism Admin in Prism Central.
> - Non-admin user—A Prism Central user without any administrator privileges.
>
> For more information about the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.

About this task

To enable Objects in Prism Central, do the following:

Procedure

1. Log on to Prism Central as an administrator.
2. Select **Admin Center** in the Application Switcher.
3. Click **Market place** in the navigation bar.
4. In the Nutanix Apps section, click **Get** for the Objects app.

Figure 3: Objects in Nutanix Marketplace

5. On the app details page, click **Deploy**.

> **Note:** It takes 4-5 minutes to complete the deployment.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 729

6. Select **Objects** in the Application Switcher.
   A welcome page appears with a prerequisites details to create an object store.

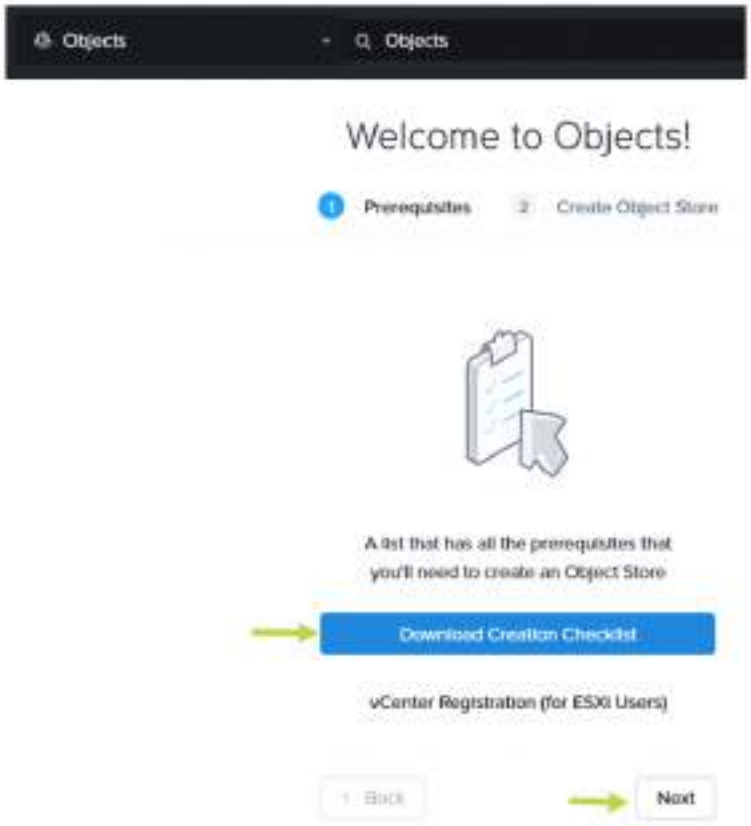


Figure 4: Objects Prerequisites

7. Click **Download Creation Checklist** to download the list of prerequisites for deploying an object store.

> **Note:** Enabling of Object Store Services is performed only once.

> **Note:** After you enable Objects, ensure that you perform LCM inventory and upgrade the MSP and Objects Manager to the latest versions before you start with deployment. For more information, see Objects LCM Upgrades on page 26.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 730

8. (Only for ESXi clusters) Click **vCenter Registration** before deploying object store on an ESXi cluster.

   To deploy object stores on the ESXi clusters, you need to provide the vCenter credentials and configure the IPAM for the ESXi networks. For more information, refer to Managing vCenter for Object Service on page 50.

   Note: A non-admin user can perform vCenter Registration only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions:

   - Create Object Store
   - View Object Store

   Administrators and non-admin users are Prism Central users with the following roles:

   - Administrator—A Super Admin or a Prism Admin in Prism Central.
   - Non-admin user—A Prism Central user without any administrator privileges.

   For more information about the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.

9. Click **Next**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 731

10. Click **Create Object Store** to start creating the first object store.
    For more information about creating the object store, refer to Creating or Deploying an Object Store (Prism Central) on page 70.

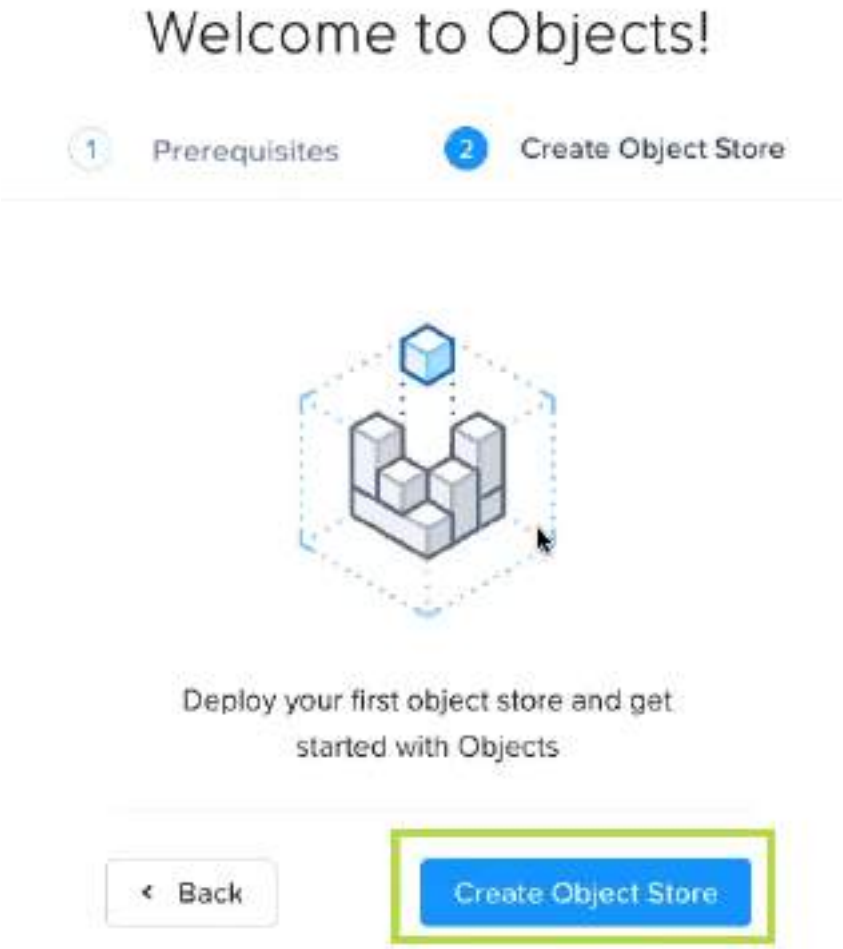


Figure 5: Objects Pre-configuration

What to do next

After deployment, the Objects app appears on the **My Apps** page. You can also select **Objects** in the Application Switcher to access and use the app.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 732

FINDING OBJECTS VERSION

You can find the installed versions of Objects Manager and Objects Service from Prism Central.

About this task

To find the version of Objects, do the following:

Procedure

1. Log on to Prism Central.
2. On the Application Switcher, go to **Admin Center** > **LCM** > **Inventory**.

Figure 6: Objects Pre-configuration

3. Click **Perform Inventory**.
   The **Installed Versions** list displays the version of Objects Manager and Objects Service.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 733

OBJECTS SECURITY HARDENING INSTRUCTIONS

This chapter describes the security hardening instructions for Nutanix Objects.

Before performing Objects hardening configurations, ensure that Prism Central and Prism Element are hardened. See Security Management Using Prism Element (PE) and Security Management Using Prism Central (PC) in the *Nutanix Security Guide*.

Networking

- Ensure only Objects S3 endpoint is exposed to users.
- Prism Central and Prism Element access is protected by a firewall and is not open to end users.
- Objects storage network is only accessible to Prism Element and Prism Central, and this network should be protected by a firewall.

  > **Note:** Use storage network only for Objects deployment. Do not use this storage network for deploying any workload or any other application.

- For the Objects Replication, open the required ports between source and destination Objects cluster IP addresses only. All other access should be protected.

Firewall Rules

Firewall rules must be configured to protect the Objects infrastructure. See the URL and Port Requirements section in the Objects User Guide.

List of networks:

- Nutanix Objects Storage Network (NOSN)
- Nutanix Objects Public Network (NOPN)
- Internet connection (IC)
- Other services (OS)
- Prism Central (PC)
- Prism Element(PE)

Flow Rules

If Flow is enabled on a setup, rules can be configured as security policies (app policy) manually or automatically instead of external firewall.

For more information about configuring the security policy when Flow is enabled, see Protecting Objects Network with Flow (Microsegmentation) on page 21.

If flow is not enabled, same rules can be applied through external firewall.

Inbound traffic allowlist:

- CVM IP addresses (including secondary/segmented)
- PC IP address
- Pod network range, usually 10.100.0.0/16

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 734

- All IP addresses such as 0.0.0.0/0 for port TCP 80 and 443.

  Note: It is recommended to not even allow port 80.

Outbound traffic allowlist:

- CVM IP addresses (including secondary/segmented)
- PC IP address
- Pod network range, usually 10.100.0.0/16
- All IP addresses such as 0.0.0.0/0 for port TCP 53, 7100, 5553 and UDP 53, 123

Objects Bucket Settings

- Disable HTTP port on the network firewall to restrict Objects S3 endpoint access over HTTP protocol.
- Enable Write-Once-Read-Many (WORM) for buckets with sensitive data.

  Objects enables you to create WORM buckets to prevent anyone (including an administrator) from modifying or deleting data while the policy is active. See WORM Bucket.
- Enable Objects versioning.

  When object versioning is enabled, uploading new data to the same object creates new versions. See Creating and Configuring an S3 Bucket on page 118.

  Note: In order to prevent storage consumption from growing unbounded, set up a lifecycle policy to expire old versions and markers with an appropriate interval. See Rules for Lifecycle Policy When Object Versioning is Enabled on page 129.
- Enable Data-at-Rest Encryption with Native Key Management.

  Nutanix Objects provides a FIPS 140-2 compliant data-at-rest encryption solution. To deliver this capability, Objects use the underlying AOS encryption capability. You can set encryption at an entire cluster level, always encrypting all data. See Data-at-Rest Encryption in the *Nutanix Security Guide*.
- Enable Identity and Access Management.

  Review and delete unused or extra access keys for buckets.
- Configure replication.

  Configure replication on buckets to keep at least one copy as backup. See Creating Replication Rules between Buckets.
- Set up SSL Certificate.

  Upload Trusted CA certificate to an Objects cluster to ensure secure communication between Objects S3 endpoint and end users. See Setting up SSL Certificate for an Object Store.
- On Prism Central, Objects user and PC admin user is a root or administrator as they can perform all the operations on the buckets as well as generate new API keys.

  - Prism Central supports role-based access control (RBAC) that allows you to configure and provide customized access to the users based on their assigned roles for the objects entities.
  - Configure RBAC policies to provide Objects access to PC users and use those user credentials to perform operations on Objects from PC. See Role-based Access Control for Objects.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 735

- Configure notifications.

  It enables you to send the completed events logs to the configured endpoints in your Objects instance. See Configuring Events Notification.

- Ensure that the tiering endpoint credentials are protected and not shared anywhere.

  Note: Never save your credentials in plain text form on your computer. Securely store your credentials in encrypted form by using credential storage applications.

Protecting Objects Network with Flow (Microsegmentation)

This section describes steps to protect Objects Network with Flow.

About this task

To protect Objects Network with Flow, do the following:

Procedure

1. Enable Flow micro-segmentation.

   For more information about enabling Flow microsegmentation, see Enabling Microsegmentation in the *Flow Microsegmentation Guide*.

2. Update the **AppType** category to **Objects_security**.

   See Modifying a Category in the *Prism Self Service Administration Guide*.

Figure 7: Update AppType

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 736

3. Assign the newly created category to Objects cluster VMs.
   See Assigning a Category in the *Prism Self Service Administration Guide*.

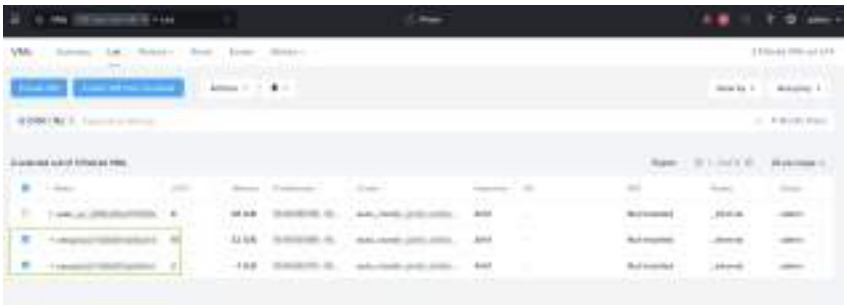


Figure 8: Select VMs to Assign Category

Figure 9: Assign Category

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 737

4. Create an Application Security Policy on *AppType:Objects_security* with a relatable name like Objects_security_policy, and add the following data to **Inbounds** and **Outbounds**.
   See Application Security Policy Configuration in the *Flow Microsegmentation Guide*.
   Inbounds:

   - CVM IP addresses (including secondary/segmented)
   - PC IP address
   - Pod network range, usually 10.100.0.0/16
   - All IP addresses such as 0.0.0.0/0 for port TCP 443.

   Outbound:

   - CVM IP addresses (including secondary/segmented)
   - PC IP address
   - Pod network range, usually 10.100.0.0/16
   - All IP addresses such as 0.0.0.0/0 for port TCP 53, 7100, 5553 and UDP 53, 123

Figure 10: Create Security Policy

Figure 11: Add Inbound OutBound Data

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 738

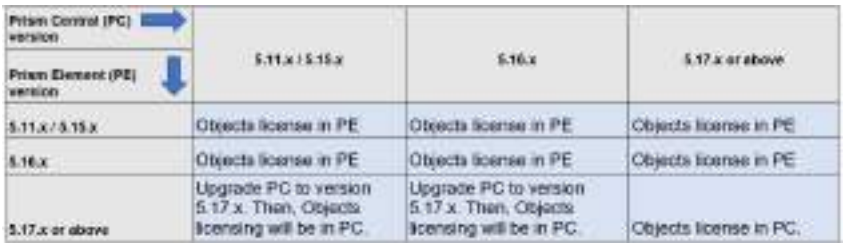
Figure 12: Review Security Policy

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 739

OBJECTS LICENSE MANAGEMENT

Nutanix provides licenses that you can apply manually to help ensure access to all the features. This feature enables you to administer your environment based on your current and future needs. With the introduction of a multi-cluster feature in Objects, you can now manage (add, verify, and monitor) Objects license from the Prism Central, not from the Prism Element.

Refer to the following image to understand the licensing matrix.



Prism Central (PC) version → / Prism Element (PE) version ↓	5.11.x / 5.15.x	5.16.x	5.17.x or above
5.11.x / 5.15.x	Objects license in PE	Objects license in PE	Objects license in PE
5.16.x	Objects license in PE	Objects license in PE	Objects license in PE
5.17.x or above	Upgrade PC to version 5.17.x. Then, Objects licensing will be in PC.	Upgrade PC to version 5.17.x. Then, Objects licensing will be in PC.	Objects license in PC.

Figure 13: Licensing Matrix

Note: Up to 1 TB Objects storage is free for all users.

Types of Licenses

Nutanix provides the following two types of Objects licenses.

- **Objects (For AOS)**: This license allows you to deploy Objects on clusters with AOS licenses.
- **Objects (Dedicated)**: This license is used when deploying an Objects-only cluster without AOS licenses.

Adding Licenses to Prism Central

You can add the Objects license to Prism Central manually. For more information, see Manage Licenses Manually section in the *Nutanix Licensing Guide*.

You can view the Objects usage information in Prism Central. For more information, see Displaying License Features and Details section in the *Nutanix Licensing Guide*.

Open Source Software Usage

For more information about Objects open source licensing details, see latest Objects Release Notes.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 740

OBJECTS LCM UPGRADES

Objects version upgrades by using the Life Cycle Management (LCM) feature. You can perform LCM upgrades through Prism Central (PC). Objects is a part of the PC upgrades module in LCM. LCM upgrades the following components of Objects: *Objects Manager* and *Objects Services*.

Objects Manager

Objects Manager is a containerized service running on PC VM. The Objects Manager is primarily responsible for taking input from a user for deploying the object store, validating the user inputs, managing certificates, deploying the Objects Services, and serving as an interface between PC, and backing-up object store. A single Objects Manager can manage one or more object stores. In the case of a scale-out PC, the Objects Manager service runs on each of the PC nodes and provides high availability.

> **Note:** During an upgrade of the Objects Manager, no disruption happens to the Objects IO. However, the user interface will not be available for a short period of time for statistics and management.

For more information about updating Objects Manager, refer to Upgrading Objects Manager on page 28.

Objects Service

Objects Service provides the object store interface and is responsible for storing and retrieving objects. The objects and metadata for the Objects are stored on the selected Prism Element clusters. The various services that perform the task are containerized and run on the Kubernetes platform. Each Objects Service instance provides a single global namespace. During deployment of the Objects Service, the required number of VMs are created for running the Kubernetes pods and the load balancer.

> **Note:** During an upgrade of the Objects Services, disruption to the IO is expected as each of the internal services gets upgraded. The upgrade process can take 15 to 30 minutes.

For more information on updating Objects Services, refer to Upgrading Objects Service on page 29.

> **Note:**
>
> - Upgrades should be in the following order:
>
> 1. Prism Central
> 2. Prism Element
> 3. MSP Controller. For more information refer to MSP.
> 4. Objects Manager
> 5. Objects Service
>
> - If Objects is not enabled and you upgrade the Prism Central, then the Objects Manager will be upgraded automatically. However, if Objects is enabled, then you have to upgrade the Objects Manager manually.

First-Time Objects Users

You must perform the following tasks to install and update Objects in your environment.

1. Perform an inventory and upgrade to a compatible version of Prism Central by using the Life Cycle Management (LCM) feature in Prism Central, refer to the *Life Cycle Management Guide*.
2. Enable Objects, refer to Enabling Objects on page 14.
3. In LCM, perform inventory and update Objects to an available GA version.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 741

Microservices Platform (MSP)

Microservices Platform (MSP) is a platform based on Kubernetes where all the Objects microservices run.

The lifecycle of MSP is controlled by a service running on Prism Central called MSP Controller. You need to upgrade the MSP Controller before upgrading the Objects Manager and Objects Service. The first object store cluster deployed on the Prism Central is the primary MSP or the primary object store. Rest all the service MSPs are the secondary MSPs or the secondary object stores.

> **Note:** The primary object store cluster hosts all the common services such as IAM, and you cannot delete the primary cluster without deleting the secondary cluster. This note is applicable only when IAM-HA feature is not enabled. For more information, see the Objects IAM-High Availability Overview on page 106 section.

Finding the MSP Version

About this task

Run the following command on Prism Central VM to find the MSP version:

Procedure

1. Log on to Prism Central VM.
2. Run the following command:
   ```
   admin@pcvm$ mspctl controller version
   ```

   > **Note:** If `mspctl controller version` command does not work, use `mspctl controller_version` command as you might be using an older version of MSP (below 2.2.0).

Finding the Primary and Secondary MSP Clusters

About this task

Run the following command on Prism Central VM to find the primary and secondary MSP clusters:

Procedure

1. Log on to Prism Central VM.
2. Run the following command:
   ```
   admin@pcvm$ mspctl cluster list
   ```

   > **Note:** If the *cluster_type* value is `primary_msp`, then the cluster is a primary MSP cluster. Other clusters are secondary.

   > **Note:** If `mspctl cluster list` command does not work, use `mspctl cluster_list` command as you might be using an older version of MSP (below 2.2.0).

Upgrading MSP Controller

You can upgrade the MSP Controller from the LCM page in Prism Central.

About this task

> **Note:**
>
> - For Objects deployment, it is recommended to upgrade to the latest MSP controller version.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 742

- Ensure that you have MSP version 1.0.8 to:
  - upgrade to MSP 2.2.1.
  - allow Objects to be visible for an upgrade in the dark-side mode.

To upgrade the MSP controller, do the following:

Procedure

1. Log on to Prism Central.
2. On the Application Switcher, go to **Admin Center** > **LCM** to open the LCM page.
3. Click **Inventory**, and then click **Perform Inventory**.
   The table lists all the updated modules.
4. Click **Updates** > **Software**.
5. Select the **MSP** check box, and then click **Update**.
6. Click **Apply Updates** to finish the update process.
   The MSP Controller is upgraded.

Upgrading Objects Manager

You need to upgrade MSP before upgrading the Objects Manager.

About this task

Note: Objects Manager upgrade will be disabled when there is at least one unresolved Objects Service upgrade failure.

To upgrade Objects Manager, do the following:

Procedure

1. Log on to Prism Central.

   For more information, refer to Enabling Objects on page 14.
2. In the Application Switcher, go to **Admin Center** > **LCM** to open the LCM page.
3. Click **Inventory**.
4. Click **Perform Inventory**.

   Note: It takes 10 to 15 minutes to list all the updated modules.

   The table lists all the updated modules.
5. If a new Objects Manager version is available, then select the **Objects Manager** check box, and then click **Update**.

   If multiple versions of Objects Manager are available, then select the latest version. You can also select MSP, Objects Manager, and Objects services, and upgrade them together. When multiple options for upgrade are selected, the upgrade happens serially and not in parallel.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 743

6. Click **Apply Updates** to finish the update process.
   Objects Manager is updated to the latest version.

   > **Note:** The update process takes about 10 to 15 minutes to complete.

7. Click **Inventory** > **Perform Inventory** to verify the latest version.

Upgrading Objects Service

You can upgrade the Objects Service after the Objects Manager is upgraded.

About this task

> **Note:** Objects Service is available for upgrade only after deployment.

To upgrade Objects Service, do the following:

Procedure

1. Log on to Prism Central.
2. In the Application Switcher, go to **Admin Center** > **LCM** to open the LCM page.
3. Click **Inventory**.
4. Click **Perform Inventory**.

   > **Note:** It takes 10 to 15 minutes to list all the updated modules.

   The table lists all the updated modules.
5. Click **Updates** > **Software**.
6. Select the **Objects Service** instance check box, and then click **Update**.

   Multiple Object Service instances will be listed separately. You can either select all of the instances and upgrade them together, or select and upgrade the instances individually. You can also select MSP, Objects Manager, and Objects services, and upgrade them together. When multiple options for upgrade are selected, the upgrade happens serially and not in parallel.
7. Click **Apply Updates** to finish the update process.
   Objects Service is updated to the latest version.

   > **Note:** The update process takes about 15 to 30 minutes for each Object Service instance to complete.

8. Click **Inventory** > **Perform Inventory** to verify the latest version.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 744

ROLE-BASED ACCESS CONTROL FOR OBJECTS

Prism Central supports role-based access control (RBAC) that allows you to configure and provide customized access to the users based on their assigned roles for the objects entities.

The access policies and permissions are user-based policies and applies only to the actions performed on the Prism Central web console. These policies and permissions do not apply to the actions performed on Objects Browser or any S3 compatible client application even if the same users have Prism Central access and Objects Browser access.

From the Prism Central roles dashboard, you can define and assign the following additional roles to users or user groups:

- A set of predefined built-in roles (system roles)
- Additional custom roles

Objects support the following built-in roles (system roles) that are defined by default:

- Objects Admin—permissions required to create and manage object stores.
- Objects Viewer—permissions required to perform read-only operations on object stores.

> **Note:** For more information on Role Based Access Control, see:
>
> - *Controlling User Access (RBAC)* in the *Security Guide*.
> - *Built-in Role Management* in the *Security Guide*
> - *Operations Management* in the *Prism Central Guide*.

Prerequisites for Configuring Role-based Access Control for Objects

Make sure that your system meets the following requirements before you start to configure role-based access control for objects.

- Prism Central version pc.2021.9 or later
- Objects Manager version 3.4 or later
- Objects Service version 3.4 or later (recommended version)
- Microservices Infrastructure is enabled in Prism Central

> **Note:** For information on enabling Microservices Infrastructure, see *Enabling Microservices Infrastructure* in the *Prism Central Guide*.

Only administrators (Super Admin or a Prism Admin in Prism Central) can create roles and access control policies for objects. For more information about the built-in roles in Prism Central, see *Built-in Role Management* in the *Security Guide*.

> **Note:** To view the Prism Central version, log on to the Prism Central web console. In the Application Switcher, click **Infrastructure**. In the left navigation bar, select **Prism Central Settings** > **Prism Central Management**. The Prism Central version is listed in the **Prism Central Summary** section.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 745

Role-Based Access Control Workflows for Objects

Role-based access control (RBAC) allows users to configure and provide different levels of access to the users based on the role of the user within an organization.

You can create the following roles and assign them to the users based on your requirements:

- Full administrator
- View-only administrator
- Buckets administrator
- Infra administrator
- Custom

> **Note:** For more information on role-based access control, see:
>
> - *Built-in Role Management* in the *Security Guide*
> - *Controlling User Access (RBAC)* in the *Security Guide*.
> - *Operations Management* in the *Prism Central Guide*.

Objects Permissions

Administrators can use the Prism Central RBAC feature to create access control policies and attach it to objects users. A non-admin user can perform object-related tasks only after an administrator creates an access control policy on a role in Prism Central for the non-admin user.

The administrators and non-admin users are Prism Central users with the following roles:

- Administrator—A Super Admin or a Prism Admin in Prism Central.
- Non-admin user—A Prism Central user without any administrator privileges.

> **Note:** For more information on the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*

The following table lists the permissions that an administrator can grant to a non-admin user to perform various objects tasks. These permissions allow the users to perform the following tasks:

Table 4: Objects Permissions

Permission	Tasks Users Can Perform
Add Multicluster	Add Prism Element clusters to expand the storage.
Create Endpoint	Create remote endpoints for tiering.
Create Object Store	Create object stores.
Create Quota Policy	Create quota policies for objects.
Delete Object Store	Remove object stores.
Delete Quota Policy	Remove the quota policies created by the respective user for objects.
Download Certificate	Download the CA-signed certificates for an object store.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 746

Permission	Tasks Users Can Perform
Edit Buckets	Edit the buckets in an object store.
Regenerate Self Signed Certificate	Regenerate self-signed certificates for an object store.
Replace Certificates	Replace certificates for an object store.
Scale Out	Add more resources to an existing object store cluster.
Set Capacity	Add additional storage capacity to an existing object store cluster.
Set Notification Endpoint	Add the notification endpoints.
Update Endpoint	Update the existing tiering endpoints.
Update Multicluster	Remove or modify the existing expanded storage (Prism Element cluster).
Update Quota Policy	Update the quota policies.
View Buckets	View the buckets in an object store.
View Endpoint	View the existing tiering endpoints.
View Multicluster	View the Prism Element clusters added for expanded storage.
View Notification Endpoint	View the notification endpoints.
View Object Store	View the object stores.
View Quota Policy	View the quota policies.

Creating Full Administrator Role for Objects

You can create full access administrator policy for users or user groups, and grant full access rights to all operations on Objects instances using role-based access control (RBAC) from the Prism Central web console.

About this task

To create a full access policy for Objects instances, do the following:

Note:

- Only users with administrator privileges create a full access policy for Objects instances.
- It might take some time (around five minutes, or so) for the changes made to the policy to be effective.

Procedure

1. Log on to the Prism Central web console as an Admin user.
2. In the Application Switcher, select **Admin Center** > **IAM** > **Roles**.
3. Select the Objects Admin role, and then click **Manage Assignment**.
   The **Role Assignment** page appears.
4. Click **Add New** to create a new role.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 747

5. From the **Select Users or Groups** section, select the required Active Directory group from the pull-down list, and then select one or more users, or user groups using the **Search User** field.

   Note: You can only add users who are part of an Active Directory group.

6. From the **Entities** section, select object store as the **Entity Type**, and then select the following:

   - Individual Entity
   - Select **All Objects** or enter the name of the Objects instance on which you need to grant custom permissions for the user.

7. Click **Save**.
   An administrator user with full access is created.

Creating View-only Administrator Role for Objects

You can create a view-only administrator role for users or user groups and grant complete access to read-only operations on Objects instances using role-based access control (RBAC) from the Prism Central web console.

About this task

Note: Only users with administrator privileges can do this task.

To create a view-only admin access policy for Objects instances, do the following:

Procedure

1. Log on to the Prism Central web console as an Admin user.
2. In the Application Switcher, select **Admin Center** > **IAM** > **Roles**.
3. Select the Objects Viewer role, and then click **Manage Assignment**.
   The **Role Assignment** page appears.
4. Click **Add New** to create a new role.
5. From the **Select Users or Groups** section, select the required Active Directory group from the pull-down list, and then select a user or user groups using the **Search User** field.

   Note: You can add only those users who are part of a Windows Active Directory group.

6. From the **Entities** section, select object store as **Entity Type**, and then select the following:

   - **Individual Entity**
   - Select **All Objects** or enter the name of the objects instance on which you need to grant read-only access to the user.

7. Click **Save**.
   A view-only administrator access control policy for one or more users or user groups is created.

Creating Bucket Administrator Role for Objects

You can create a bucket administrator policy to manage all bucket activities on objects instances using role-based access control (RBAC) from the Prism Central web console.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 748

About this task

> **Note:** Users with only administrator privileges can do this task.

To create a buckets admin policy, do the following:

Procedure

1. Log on to the Prism Central web console as an Admin user.
2. In the Application Switcher, select **Admin Center** > **IAM** > **Roles**.
3. Click **Create Role**.
   The **Roles** page appears.
4. Enter the following details on the **Roles** page:
   a. **Role Name**: Enter a name for the role.
   b. **Description**: Enter a brief description of the role.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 749

5. From the **Object Store** section, click **Change** next to the **Set Custom Permissions** option.
   The **Custom Object Store Permissions** window appears.

   Note: You can also enter *Object Store* in **Filter Entities** to go to the object store section.

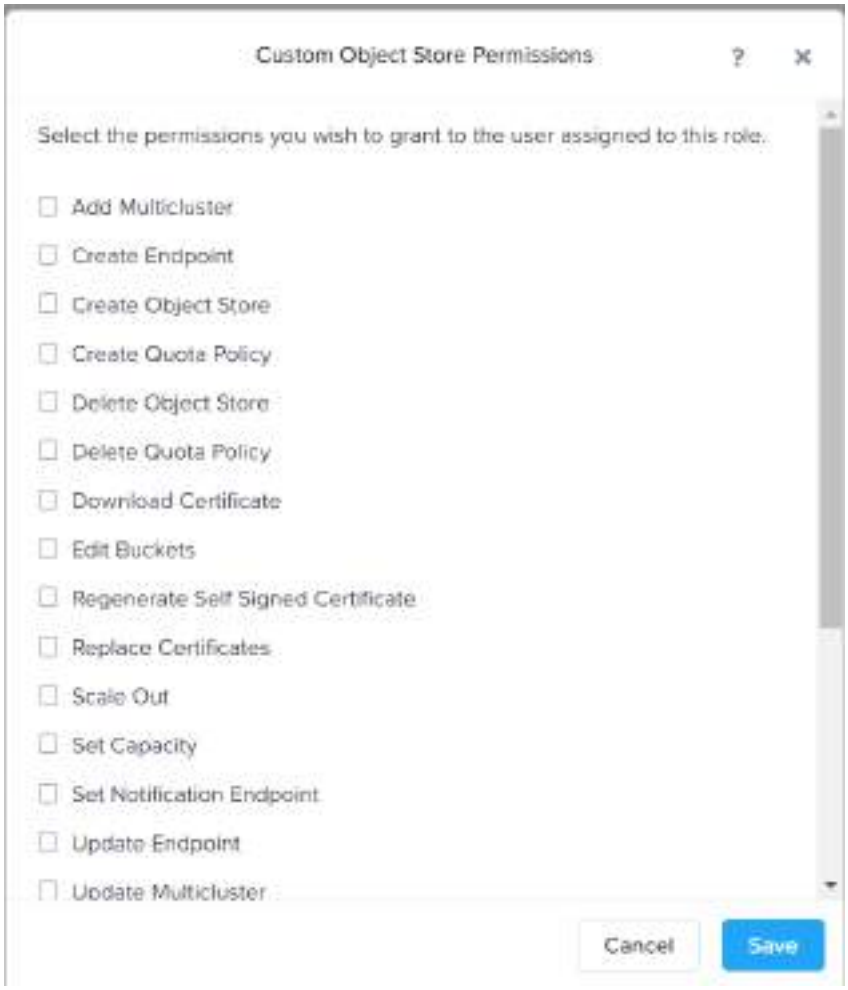


Figure 14: Custom Object Store Permissions

6. Select the following permissions from the list and click **Save**:

   - Edit Buckets
   - View Buckets
   - View Object Store

   Note:

   - When you select certain permissions, other additional permissions might automatically get added to the permission list. Read the on-screen instructions to understand the additional permissions that are automatically granted to the new custom role.
   - Users with Edit Bucket permission can perform bucket operations, such as create, update, and delete on the buckets available in the object stores that are assigned to the respective users.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 750

7. Click the newly created role, and click **Manage Assignment**.
   The **Role Assignment** page appears.
8. Click **Add New** to assign the role to more users or user groups.
9. From the **Select Users or Groups** section, select the Windows AD group, and then select the user or user groups using the **Search User** field.

   Note:

   - You can add only those users who are part of an Active Directory group.
   - When permission is granted to a role, the specific permission is not always inherited to the access control policy that is created with that role. This role needs to be assigned to a specific Objects instance.

10. From the **Entities** section, select object store as the **Entity Type**, and then select the following:

    - Individual Entity
    - Select All Objects or enter the name of the Objects instance on which you need to grant custom permissions for the user.

11. Click **Save**.
    The Buckets Admin access control policy is saved and listed on the **Roles** page. The user now has access to perform bucket management tasks (create, update, and delete buckets) on all buckets in that objects instance.

    Note: Certain actions on buckets might need additional permissions to be assigned to the custom role. For example, to set a lifecycle policy based on tiering on a bucket, see Tiering section for the required permissions.

Creating Infra Administrator Role for Objects

An administrator can provide access to users or to user groups to manage all the existing objects instances without providing any write access to buckets on the objects instances, from the Prism Central web console.

About this task

Note: Users with only administrator privileges can perform this task.

To create infra administrator access control policy, do the following:

Procedure

1. Log on to the Prism Central web console as an Admin user.
2. In the Application Switcher, select **Admin Center** > **IAM** > **Roles**.
3. Click **Create Role**.
   The **Roles** page appears.
4. Enter the following details on the **Roles** page:

   a. **Role Name**: Enter a name for the role.

   b. **Description**: Enter a brief description of the role.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 751

5. From the object Store section, select **Set Custom Permissions** and click **Change**.
   The **Custom Object Store Permissions** window appears.

   > **Note:** You can also enter *Object Store* in **Filter Entities** to go to the **Object Store** section.

6. Select the following permissions from the list and click **Save**:
   Add Multicluster, Create Quota Policy, Delete Quota Policy, Download Certificate, Regenerate Self Signed Certificate, Replace Certificates, Scale Out, Set Capacity, Set Notification Endpoint, Update Multicluster, Update Quota Policy, View Buckets, Edit Buckets, View Multicluster, View Notification Endpoint, View Object Store, and View Quota Policy.

   > **Note:** When you select certain permissions, other additional permissions might automatically get added to the permission list. Read the on-screen instructions to understand the additional permissions that are automatically granted to the new custom role.

7. Click the newly created role, and click **Manage Assignment**.
   The **Role Assignment** page appears.

8. Click **Add New** to assign the role to users or user groups.

9. From the **Select Users or Groups** section, select the Windows AD group, and then select the users or user groups using the **Search User** field.

   > **Note:**
   >
   > - You can add only those users who are part of an Active Directory group.
   > - When permission is granted to a role, the specific permission is not always inherited to the access control policy that is created with that role. This role needs to be assigned to a specific Objects instance.

10. From the **Entities** section, select object store as the **Entity Type**, and then select the following:

    - Individual Entity
    - Select **All Objects** or enter the name of the objects instance on which you need to grant custom permissions for the user.

      > **Note:** When permission is granted to a role, the specific permission is not always inherited to the access control policy that is created with that role. This role needs to be assigned to a specific Objects instance.

11. Click **Save**.
    The Infra Administration access control policy is saved and listed on the **Roles** page. The user now has access to manage existing objects instances. However, the user cannot perform any bucket update operations, create any objects instances, or delete any objects instances.

Creating a Custom Role for Objects

An administrator can create custom roles and provide access to users or to user groups from the Prism Central web console.

About this task

> **Note:** Only users with administrator privileges can do this task.

For information on creating a custom role, see *Creating a Custom Role* in the *Security Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 752

To create a custom access control policy (custom role), do the following:

Procedure

1. Log on to the Prism Central web console as an Admin user.
2. In the Application Switcher, select **Admin Center** > **IAM** > **Roles**.
3. Click **Create Role**.
   The **Roles** page appears.
4. Enter the following details on the **Roles** page:
   a. **Role Name**: Enter a name for the role.
   b. **Description**: Enter a brief description of the role.
5. From the Object Store section, select **Set Custom Permissions** and click **Change**.
   The **Custom Object Store Permissions** window appears.

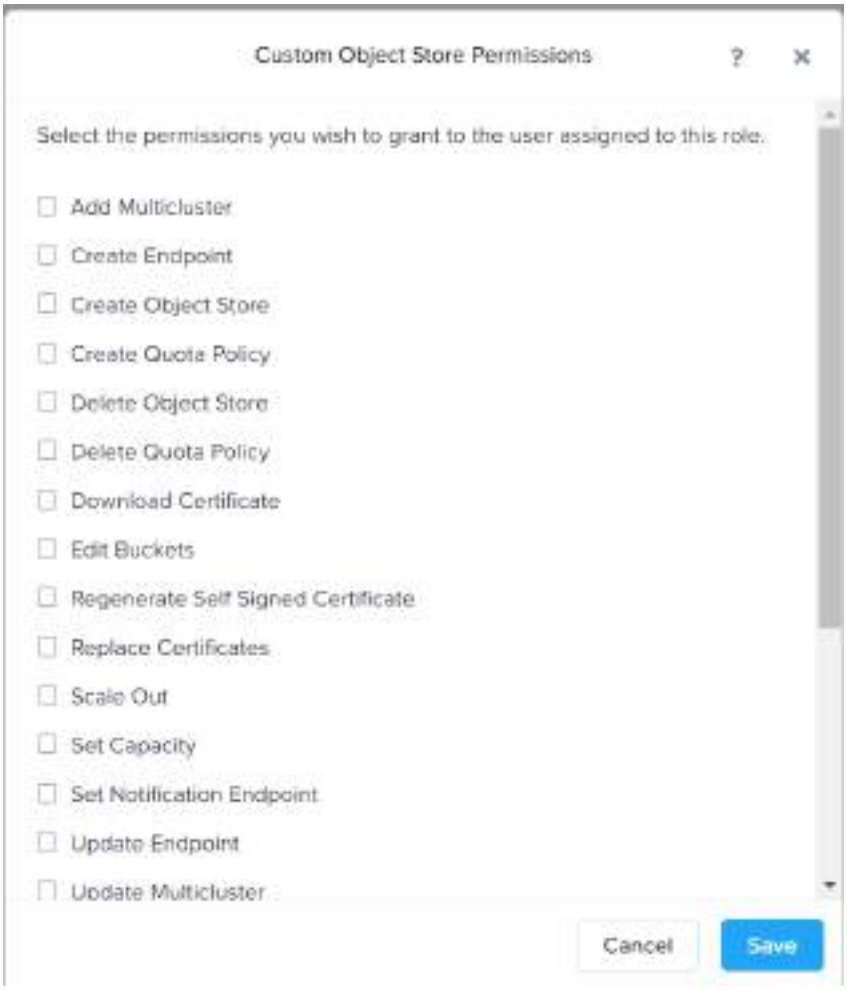


Figure 15: Custom Object Store Permissions Window

Note: You can also enter *Object Store* in **Filter Entities** to go to the **Object Store** section.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 753

6. Select the required permissions and click **Save**.

   Note: When you select certain permissions, other additional permissions might automatically get added to the permission list. Read the on-screen instructions to understand the additional permissions that are automatically granted to the new custom role.

7. Select the newly created role, and then click **Manage Assignment**.
   The **Role Assignment** page appears.

8. Click **Add New** to assign the role to users or user groups.

Figure 16: Role Assignment Window

9. From the **Select Users or Groups** section, select the required Active Directory group from the pull-down list, and then select one or more users or user groups using the **Search User** field.

   Note:

   - You can add only those users who are part of an Active Directory group.
   - When permission is granted to a role, the specific permission is not always inherited to the access control policy that is created with that role. This role needs to be assigned to a specific Objects instance.

10. From the **Entities** section, select object store as the **Entity Type**, and then select the following:

    - **Individual Entity**
    - Select **All Objects** or enter the name of the Objects instance on which you need to grant custom permissions for the user.

      Note: When permission is granted to a role, the specific permission is not always inherited to the access control policy that is created with that role. This role needs to be assigned to a specific Objects instance.

11. Click **Save**.
    The custom access control policy is saved and listed in the **Roles** page. The user now has access to manage existing Objects instances granted to him in the policy.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 754

DEPLOYMENT AND NETWORK PREREQUISITES

Ensure that you have met the deployment prerequisites and configured the network for **AHV** or **ESXi** before proceeding for an object store deployment.

Deployment Prerequisites - AHV and ESXi

Before deploying Object Store Services on AHV or ESXi, review this section carefully to ensure you have met the prerequisites. This section combines prerequisites for sites with internet access (online) and dark site (offline) deployments. Unless specified, the requirements are for both online and dark site (offline) deployments.

General Requirements

Ensure that your environment conforms to the following requirements before running Objects:

> **Note:** ESXi is supported only with Objects 3.0 or later versions.

- The hypervisor can be AHV or ESXi.
- Prism Element version 5.11.2 or later and Prism Central version 5.17.1 or later running in your environment.
- Recommended browser: Google Chrome
- Minimum of one node in a cluster running AHV or ESXi.

  > **Note:** Objects use no more than 12 vCPUs for each AHV or ESXi node.

- Ensure that no AHV or ESXi host or Prism Element or Prism Central upgrade is in progress while deploying Objects.
- Ensure that the object store domain should be dedicated for the object store deployment.

  For example, if the top level domain is `mycompany.com`, then the object store domain can be a sub domain such as `objectstore.mycompany.com`.
- Recommended that proxy should be able to reach the guest VM.
- Recommended to enable Pulse (only for site with Internet access).
- For an online installation, it is recommended to have a high speed and stable Internet connection.

  > **Note:** Image download times out after 90 minutes and the deployment fails.

- Recommended to upgrade to the latest version of the MSP controller for deployment in a dark site. Refer to Microservices Platform (MSP) on page 27.
- Ensure that the LCM web server is accessible from the Prism Element on which Objects is to be deployed in a dark site.
- Ensure that the LCM web server is accessible through the proxy, if set on Prism Central for the dark site deployment.
- Allow Prism Central and Prism Element to access the web server through port 80 for dark site deployment.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 755

- Ensure to upgrade to MSP 2.0 or later versions and Objects 3.0 or later versions for expanding the object store cluster.
- Ensure to upgrade to Objects 2.1 or later versions for scaling out the object store cluster.

Network Requirements

Ensure to configure the following network requirements before running Objects:

- Configure Domain Name Servers (DNS) on both Prism Element and Prism Central.
- Configure Network Time Protocol (NTP) servers on both Prism Element and Prism Central.
- Set up the Virtual IP address and the data services IP address on the Prism Element where you plan to deploy Objects. Also, ensure that you set the DSIP on the PE cluster where the Prism Central is deployed.
- Ensure that the communication between Objects (Storage or Public network) and Prism Central must be direct and not through a proxy server.
- **AHV**: Ensure VLANs that are required internally for Object Store Services and externally for accessing the object store endpoints are configured on Prism Element correctly. Follow the guidelines provided in the Network Configuration on page 42 section.

  ESXi: Refer to ESXi Prerequisites.
- Ensure that you have an Internet connectivity for both Prism Element and Prism Central for online deployment. If you do not have Internet, refer to Deploying Object Store at a Dark Site (Offline Deployment) on page 98.

Prerequisites - ESXi

Before you start deploying Object Store Services on ESXi clusters, review this section carefully to ensure you have met the prerequisites. This section combines prerequisites for both sites with internet access (online) and dark site (offline) deployments.

Network Prerequisites

Ensure to configure the following network requirements before running Objects:

- Ensure that the ESXi network to be used for Objects deployment is available on all ESXi hosts.
  - If the network is configured using the standard vSwitch, ensure that all hosts have the network with the same name and VLAN.
  - If the network is configured using the Distributed Virtual Switch (DVS), ensure that all hosts are part of DVS.
- Ensure that you meet the Objects ESXi IPAM requirements. For more information, see ESXi Configuration on page 47.
- Ensure that only nodes belonging to a single Prism Element (PE) get added to an ESX cluster in vCenter.
- Ensure the VMware NSX network is present on all hosts of both the primary and secondary ESXi Metro Storage Clusters.

vCenter and ESXi Prerequisites

Ensure that the ESXi cluster complies with the following settings:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 756

- ESXi clusters must be registered to a vCenter.
- Ensure that Distributed Resource Scheduler (DRS) and High Availability (HA) solutions are enabled on the cluster. For more information, see the *Create a Cluster* topic in the *VMware vSphere Product Documentation*.
- Ensure that the AOS cluster where you are deploying the object stores is mapped to a single ESXi cluster.
- Supported ESXi hypervisors versions are 6.5 or above.
- Objects version 3.0 and MSP 2.0 and later versions are supported.
- The minimum supported version of NSX-T is 2.4. Refer to KB article 000008545.

Prism Central VM (PCVM) Prerequisites

Ensure that the PCVM complies with the following:

- Ensure that PCVM is hosted and registered on the Prism Element (PE). It is required to provision Volume from the hosted PE to the MSP controller for image conversion.
- Ensure that the vCenter IP address is allowed in the proxy configuration and vCenter is connected to Prism Central.

  Worker VMs, Prism Central, and Prism Element must have a direct connection with the vCenter and not through a proxy server.

Network Configuration

The Nutanix Objects architecture uses two networks - **Objects Storage Network** (internal) and **Objects Public Network** (external).

Objects Storage Network is a virtual network used for internal communication between the components of an object store. **Objects Public Network** is a virtual network used by external clients to access the Object Store.

Note:

- You can have two virtual networks, each for Objects Storage Network and Objects Public Network, but it is not mandatory. You can have the Objects Storage Network and the Objects Public Network on the same virtual network. However, it is recommended to have the Objects Storage Network and the Objects Public Network on different virtual networks for production deployments.
- It is recommended that the Objects Storage Network should be same as the CVM or the Hypervisor network. A single network enables the traffic between Objects and CVM to flow within the same network, hence avoiding cross-network hop which tends to be network constrained in some deployments. The traffic that flows between Objects and CVM is a function of the capability of the underlying AOS and is going to be significant in a dedicated objects deployment.
- If you want to use different networks for Objects Storage Network and CVM network, ensure that the network bandwidth between the top-of-rack switch and the L3 device is fast enough to avoid network congestions. Alternatively, you can enable L3 functionality on the top-of-rack switch.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 757

LACP and Link Aggregation

We recommend you configure link aggregation with LACP and balance-tcp. Objects is a network-heavy workload and requires a high network bandwidth. You can achieve a faster network by aggregating multiple physical links into one logical network interface that can be used for all traffic.

You require LACP and link aggregation to take full advantage of the bandwidth provided by multiple links. In Open vSwitch (OVS), it is accomplished through dynamic link aggregation with LACP and load balancing using balance-tcp.

For more information about how to enable, disable, and verify LACP in AHV, see Enabling LACP and LAG (AHV Only) in the AHV Networking Guide.

On ESXi based Objects deployments, you can also use the vSphere Distributed Switch with *Route based on physical NIC load (LBT)*.

AHV Configuration

You can configure and manage virtual networks through Prism Element and use these virtual networks to deploy an object store through Prism Central.

Once you have successfully added these virtual networks (with AHV IPAM enabled) in Prism Element for AHV, you can use these virtual networks to deploy an object store through Prism Central. For more information about network configurations and enabling AHV IPAM, refer to Network Configuration for VM Interfaces in *Prism Web Console Guide*.

The following section describes the Objects Storage (internal) and Objects Public (external) networks in more detail:

Objects Storage Network

An object store uses this private virtual network to communicate between services. The number of IP addresses required for deploying your Objects store instance varies according to the deployment size. For more information, see the *IP Address Consumption* section.

Requirements of a virtual network used for an object store:

- AHV IPAM must be enabled.
- Sufficient IP addresses must be available in the IPAM DHCP Pool. Refer to *IP Address Consumption - Based on Deployment Size*
- Two static IP addresses outside the DHCP pool are required for each object store. Later while deploying the object store from Prism Central, use the static IP addresses for the Objects Storage Network configuration based on the object store storage and resource requirements.

> **Note:** Objects internal services use the `10.100.0.0/16` and `10.200.0.0/16` subnets therefore the subnet used for internal interface IP addresses cannot conflict with either of these subnets.

Objects Public Network

An object store uses this virtual network (with AHV IPAM enabled) to allow access from external clients.

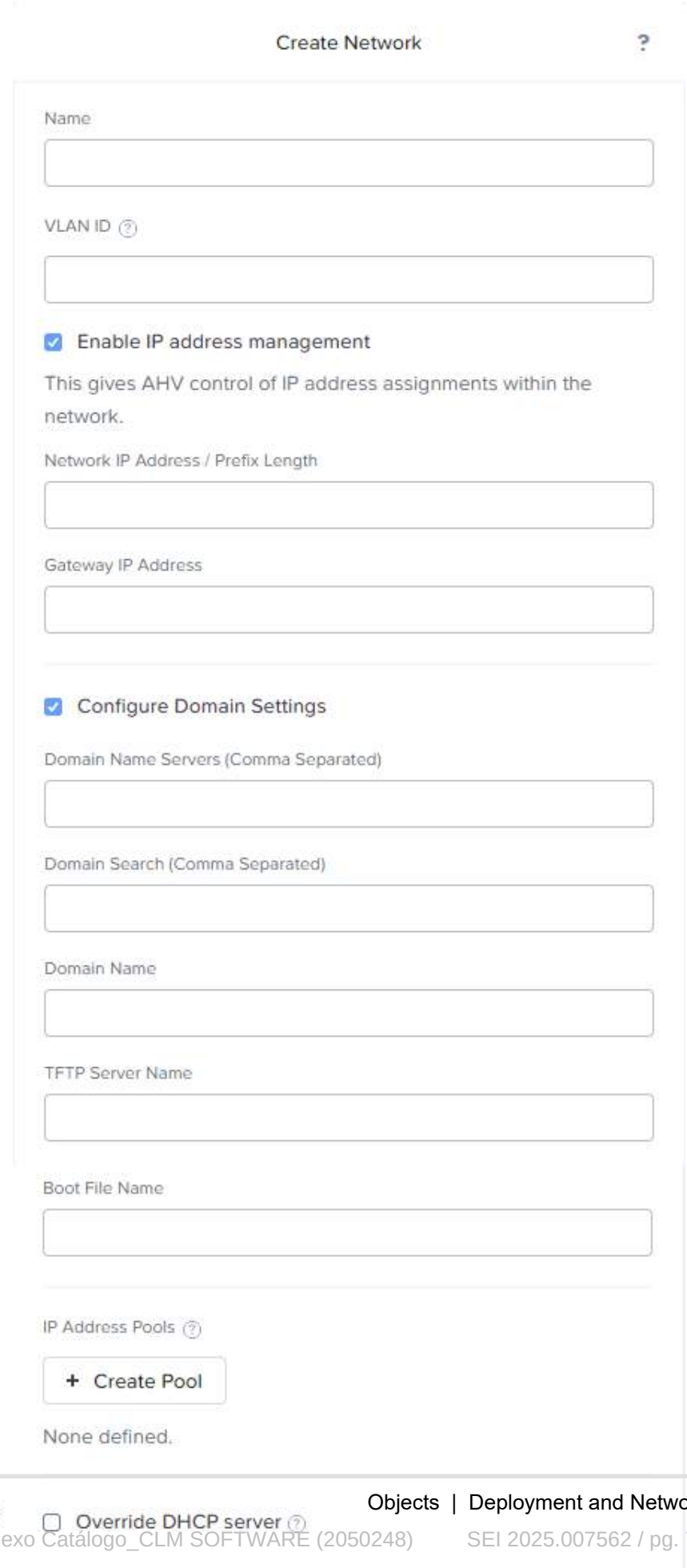
Requirements of a virtual network to access an object store externally:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 758

- The virtual network must have AHV IPAM enabled.

  While configuring the virtual network, make sure you specify details such as VLAN ID, Network IP Address/Prefix Length, Gateway IP address, and DNS Servers.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 759



Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 760

- While deploying an object store from Prism Central, use up to four static IP addresses for the Objects public network configuration based on the object store storage and resource requirements.

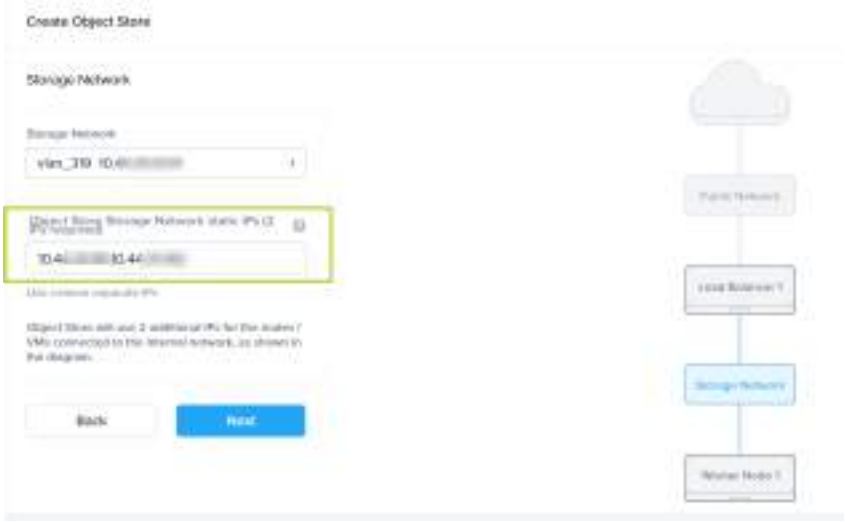


Figure 18: Network Configuration - Objects Storage IP addresses

Figure 19: Network Configuration - Objects Public IP addresses

Note: You can have two virtual networks, each for Objects Storage Network and Objects Public Network, but it is not mandatory. You can have the Objects Storage Network and the Objects Public Network on the same virtual network. However, it is recommended to have the Objects Storage Network and the Objects Public Network on different virtual networks for production deployments.

Note: All the IP addresses may not get used during the deployment. The number of IP addresses used depends on the size of your deployment. The unused IP addresses get reserved for future usage.

You can view a list of deployed object stores, and the general and networking details of the object stores. For example, you can view the Objects Public IP addresses for your deployment. For more information, see Viewing Object Store Deployments on page 78.

IP Address Consumption

This section describes the IP address consumption based on the deployment size.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 761

Objects Public Network

Up to four static IP addresses are required for exposing the Objects S3 Endpoint based on the selected worker nodes. The client connects to these IP addresses for all the S3 requests. Object supports a maximum of four public IP addresses for each Object Store.

Objects Storage Network

The IP address consumption for the Objects Storage Network is as follows:

- From the DHCP pool
  - Each Worker VM requires one IP address.
  - One IP address for each load balancer for communications with Objects workers.
  - Two IP addresses for High Availability of internal MSP services.
- Outside DHCP Pool - Two static IP addresses are required for MSP DNS and API servers.

Number of Worker Nodes	AHV Managed Networks					
	Objects Storage Network					Objects Public Network
	From DHCP Pool				Outside DHCP Pool	Number of static IP addresses required for load balancers for communication with external S3 clients
	Number of IP addresses required for Worker VMs	Number of IP addresses required for the Load Balancer VMs to communicate with Worker VMs	Number of IP addresses for HA of internal MSP services	Number of IP addresses required for IPAM DHCP Server	Number of Static IP addresses required for MSP DNS and API Server	
1	1	1	2	1	2	1
2	2	1	2	1	2	1
3	3	2	2	1	2	2
4	4	3	2	1	2	3
5	5	4	2	1	2	4
N	N	4	2	1	2	4

Figure 20: IP Address Consumption - Based on Deployment Size

ESXi Configuration

For ESXi clusters, you can perform the Objects ESXi IPAM configuration.

You can do the Objects ESXi IPAM configuration from the **Objects service** > **vCenter Management** available in the Prism Central web console. For more information, see Managing vCenter for Object Service on page 50.

Objects requires you to add the IPAM range for the ESXi networks that you want to use for object store deployment.

Objects uses these ESXi networks for two purposes:

- To deploy Objects VMs that host the various Objects services (also referred to as **Objects Storage Network**).
- To deploy load balancer VMs that provide object store endpoint to the S3 clients (also referred to as **Objects Public Network**).

The following section describes the Objects Storage (internal) and Objects Public (external) networks in more detail:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 762

Objects Storage Network

An object store uses this private virtual network to communicate between services. The number of static IP addresses required for deploying your Objects store instance varies according to the deployment size. For more information, see the *IP Address Consumption* section.

Requirements of a virtual network used for an Object Store:

- Add the IPAM range for the ESXi networks in the **vCenter Management** page.
- Sufficient IP addresses must be available. Refer to *IP Address Consumption - Based on Deployment Size*
- Subnet, Gateway, and DNS IP address to be used for the ESXi network. The provided values must be valid.

> **Note:** Objects internal services use the `10.100.0.0/16` and `10.200.0.0/16` subnets therefore the subnet used for internal interface IP addresses cannot conflict with either of these subnets.

Objects Public Network

An object store uses this virtual network to allow access from external clients.

Requirements of a virtual network to access an object store externally:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 763

- Up to four static IP addresses that can either be part of or outside the IPAM range. Later while deploying the object store from Prism Central, use the static IP addresses for the Objects Public Network configuration based on the object store storage and resource requirements.

Note: If the **Objects Public Network** is different from the **Objects Storage Network**, then only subnet and Gateway values are needed. IPAM range and DNS IP address values are optional.

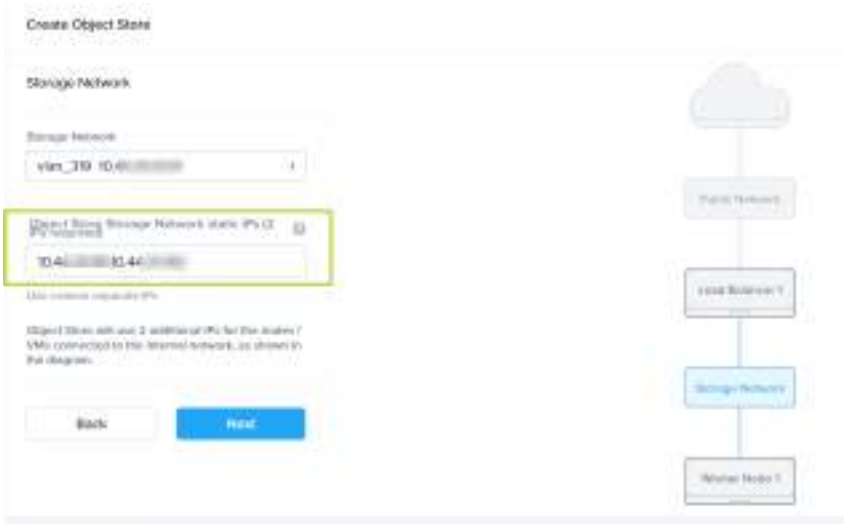


Figure 21: Network Configuration - Objects Storage IP addresses

Figure 22: Network Configuration - Objects Public IP addresses

Note: You can have two virtual networks, each for Objects Storage Network and Objects Public Network, but it is not mandatory. You can have the Objects Storage Network and the Objects Public Network on the same virtual network. However, it is recommended to have the Objects Storage Network and the Objects Public Network on different virtual networks for production deployments.

Note: All the IP addresses may not get used during the deployment. The number of IP addresses used depends on the size of your deployment. The unused IP addresses get reserved for future usage.

You can view a list of deployed object stores, and the general and networking details of the object stores. For example, you can view the Objects Public IP addresses for your deployment. For more information, see Viewing Object Store Deployments on page 78.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 764

IP Address Consumption

This section describes the IP address consumption based on the deployment size.

Objects Public Network

Up to four static IP addresses are required for exposing the Objects S3 Endpoint based on the selected worker nodes. The client connects to these IP addresses for all S3 requests. Object supports a maximum of four public IP addresses for each Object Store.

> **Note:** The IP addresses can be within or outside the range of the IPAM network.

Objects Storage Network

The IP addresses get consumed from the IPAM range configured for the ESXi networks as follows:

- Each Worker VM requires one IP address.
- One IP address for each load balancer for communications with Objects workers.
- Two IP addresses for High Availability of internal MSP services.
- Two static IP addresses required for MSP DNS and API servers.

Number of Worker Nodes	Objects Storage Network					Objects Public Network
	Objects ESXi IPAM Range Configured for the ESXi Network					*Number of static IP addresses required for load balancers for communication with external S3 clients
	Number of IP addresses required for Worker VMs	Number of IP addresses required for the Load Balancer VMs to communicate with Worker VMs	Number of IP addresses for HA of internal MSP services	Number of IP addresses required for IPAM DHCP Server	Number of Static IP addresses required for MSP DNS and API Server	
1	1	1	2	1	2	1
2	2	1	2	1	2	1
3	3	2	2	1	2	2
4	4	3	2	1	2	3
5	5	4	2	1	2	4
N	N	4	2	1	2	4

* Public access IP addresses can be within or outside the range of the IPAM Network

Figure 23: IP Address Consumption - Based on Deployment Size

Managing vCenter for Object Service

To deploy Object Stores on ESXi clusters, you need to provide the vCenter credentials and configure the IPAM for ESXi networks.

About this task

For AHV clusters, IPAM is configured in the Prism Element. For ESXi clusters, you can perform the IPAM configuration from the Objects > vCenter Management available in the Prism Central web console.

Managing vCenter for object service consists of two steps.

- Add the vCenter IP address and login credentials in the Object service within the Prism Central to create a trust relationship. Nutanix does not store the login credentials after the connection is established between the vCenter and Prism Central.
- Add IPAM for one or more ESXi networks.

  When deploying the object store instance, you need to define the Objects Storage Network and Object Public Network. You can use these pre-configured networks for Objects internal and public access.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 765

To register the vCenter in the Prism Central, do the following:

Procedure

1. Log on to the source Prism Central web console, and click the **Entity** menu > **Services** > **Objects**.
2. Click **vCenter Management**.
3. Click **Add vCenter**.

Figure 24: vCenter Management Page

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 766

4. In the **vCenter** page, enter the IP address and login credentials of the vCenter.

   The details you enter are used to generate a certificate and build a trust relationship between the vCenter and Prism Central.

   Note: Nutanix does not store the login credentials after the connection is established between the vCenter and Prism Central.

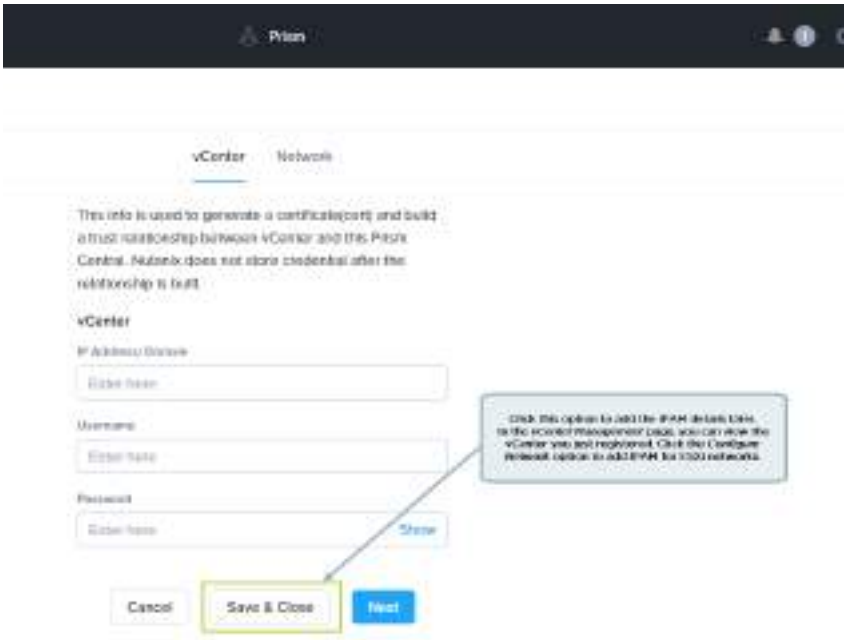


Figure 25: Register vCenter

   Note: For a user with non-administrator privileges to perform vCenter Registration, the administrator must create an access control policy for the non-administrator user on a role that must have the following minimum permissions:

   - Create Object Store
   - View Object Store

5. Click **Next** to add IPAM for the ESXi network.

   Else, click **Save & Close** to add the IPAM details later. In the **vCenter Management** page, you can click **Configure Network** in the **Actions** column to proceed with adding the IPAM for ESXi networks.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 767

6. Click **Add Network**.
   The **Add Network** page appears.

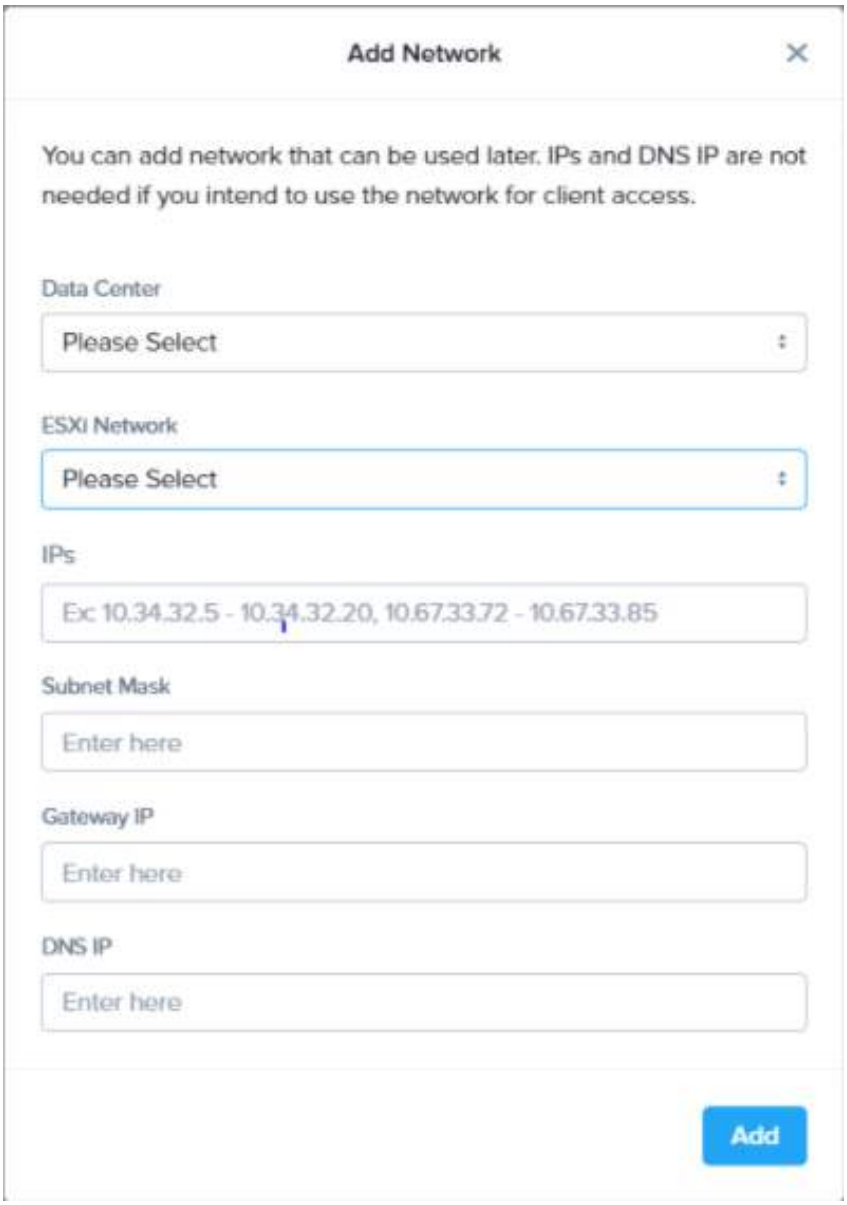


Figure 26: Add IPAM for ESXi Network

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 768

7. In the **Add Network** page, do the following:

   a. In the **Data Center**, select the datacenter where your ESXi cluster is located.

      The **ESXi Network** drop-down will get populated with a list of supported ESXi networks belonging to the data center.

   b. In the **ESXi Network**, select the ESXi network you want to use for deployment.

   c. Enter the IP address range, subnet mask, Gateway IP address, and DNS IP address.

      The IP address range you provide will be used for the Objects Storage Network. The IP address range and DNS IP address are optional if the IPAM will be used only for the Objects Pubic Network.

   d. Click **Add** to complete your IPAM configuration.

      If you want to add more networks, click **Add Network** on the **Configure** page and enter the details.

      > **Note:** It is recommended to use separate networks for the Objects Storage Network and Objects Public Network.

   e. Click **Update** to close the **Configure** page.

      In the **vCenter Management** page, in the **Network** column, you can view the count of IPAM.

      In the **Actions** column, you can click the **Delete** option to delete the vCenter.

      > **Note:** Even if you delete a vCenter, the IPAM details would still be available. If you add the deleted vCenter again, the IPAM details previously added gets recovered.

What to do next

You can start with the deployment of the object store on the ESXi clusters. For more information, see Object Store Service Deployment.

Shared Versus Single Network

You can configure Objects to use a single network for all services or separate the subnets used for internal communications and client communications.

You can have two virtual networks, each for Objects Storage Network and Objects Public Network, but it is not mandatory. You can have the Objects Storage Network and the Objects Public Network on the same virtual network. However, it is recommended to have the Objects Storage Network and the Objects Public Network on different virtual networks for production deployments.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 769

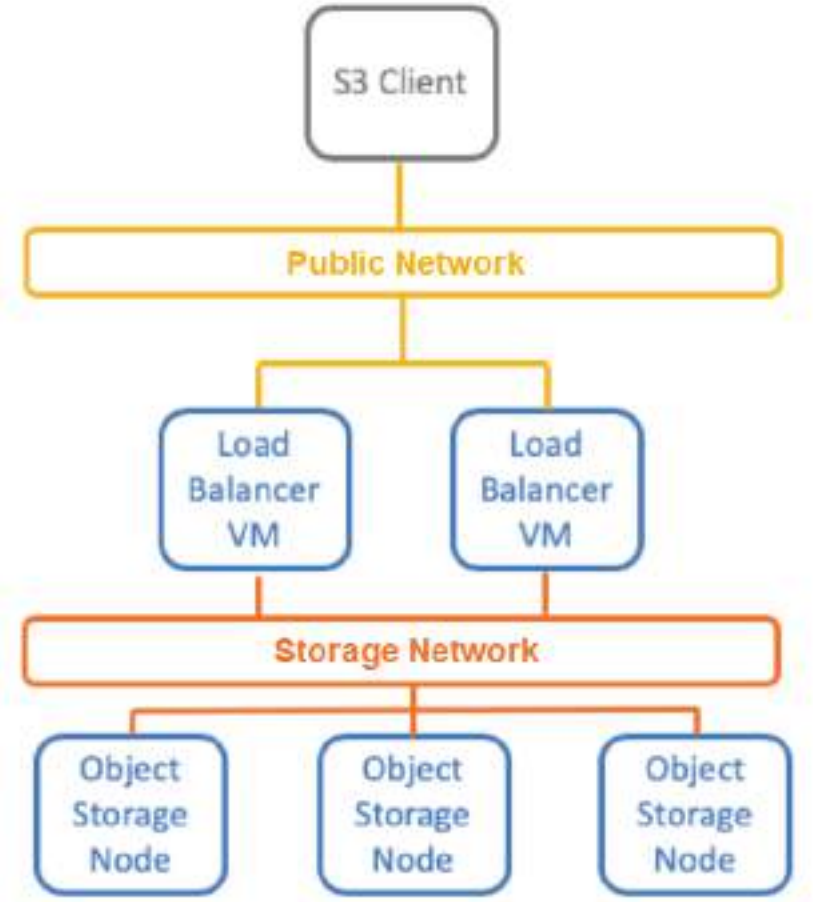


Figure 27: Objects Network Architecture - Using Two Separate Networks (Storage and Public)

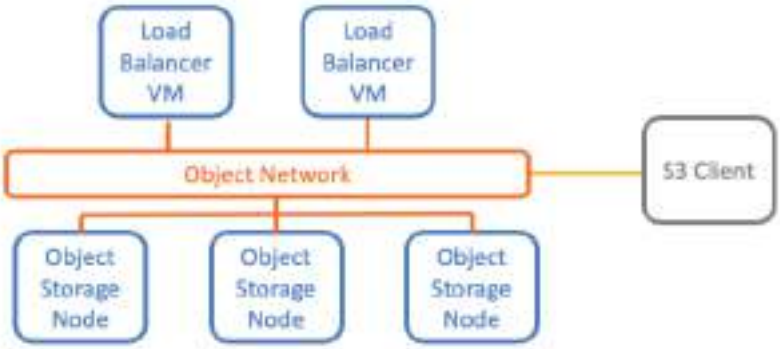


Figure 28: Objects Network Architecture - Using One Network (Storage and Public)

URL and Port Requirements

This section describes the URL and port requirements for Objects instance deployment.

URL Requirements

The following URLs are used by the Objects server:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 770

- Prism Central and Prism Element must have access to the following:
  - `download.nutanix.com`
  - `docker.io`
  - `api.ecr.us-west-2.amazonaws.com`
  - `prod-us-west-2-starport-layer-bucket.s3.us-west-2.amazonaws.com`
- Gold image is downloaded from *download.nutanix.com*.
- `.quay.io` and `.cloudfront.net`

> **Note:** URLs are not required for the dark site deployment.

Port Requirements

Refer to the Port Reference Guide for the required ports for your Objects deployment.

> **Note:** Internal network IP ranges such as 10.100.x.x and 10.200.x.x could be seen on the firewall if the inter MSP VM traffic passes through the firewall.

Refer to the following diagrams to understand Objects network architecture for IAM-HA enabled and disabled clusters. For more information about Objects IAM-HA, see Objects IAM-High Availability Overview on page 106.

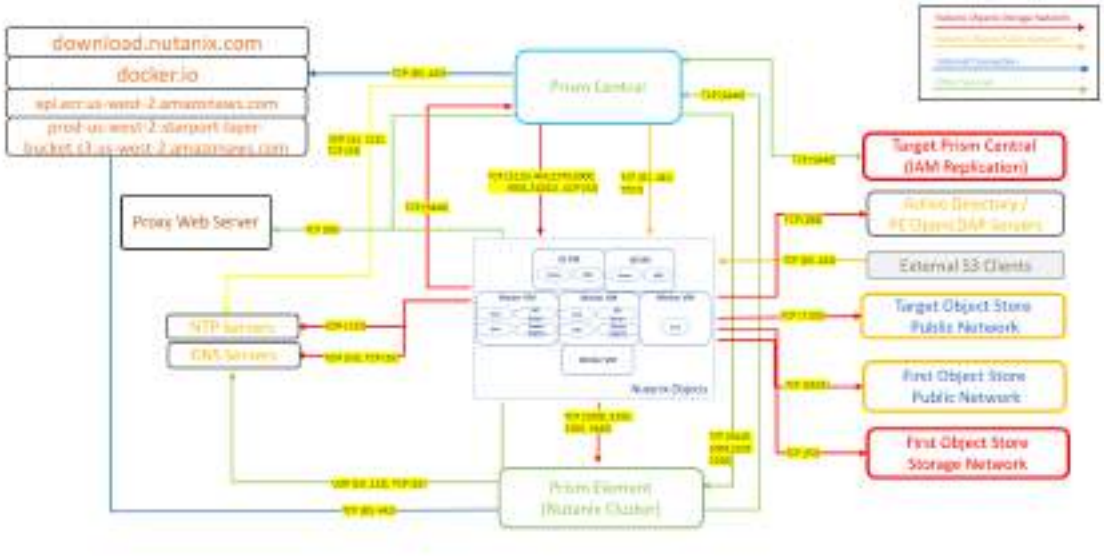


Figure 29: IAM-HA Disabled Objects Network Diagram with Ports (AHV)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 771

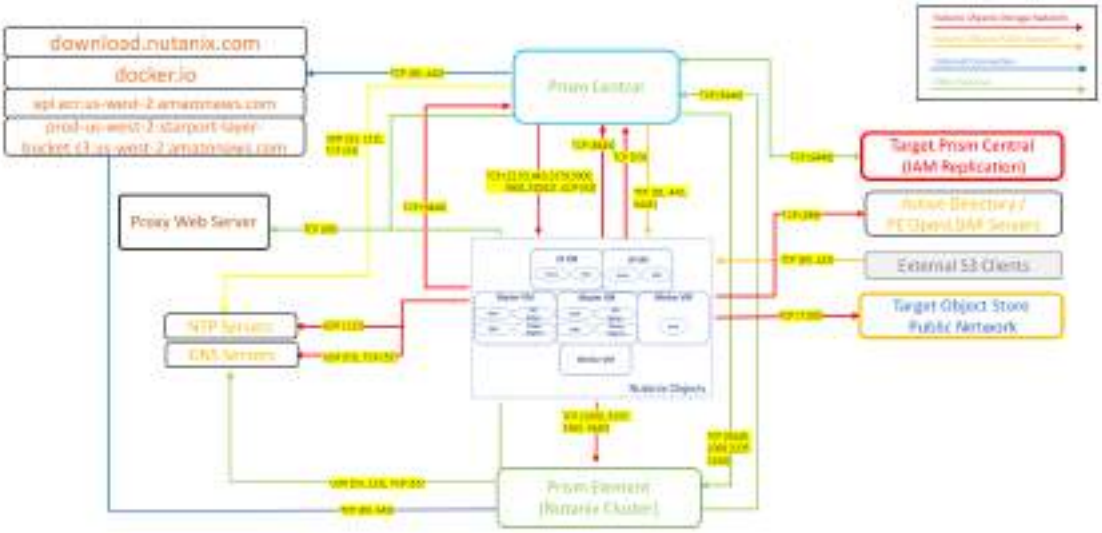


Figure 30: IAM-HA Enabled Objects Network Diagram with Ports (AHV)

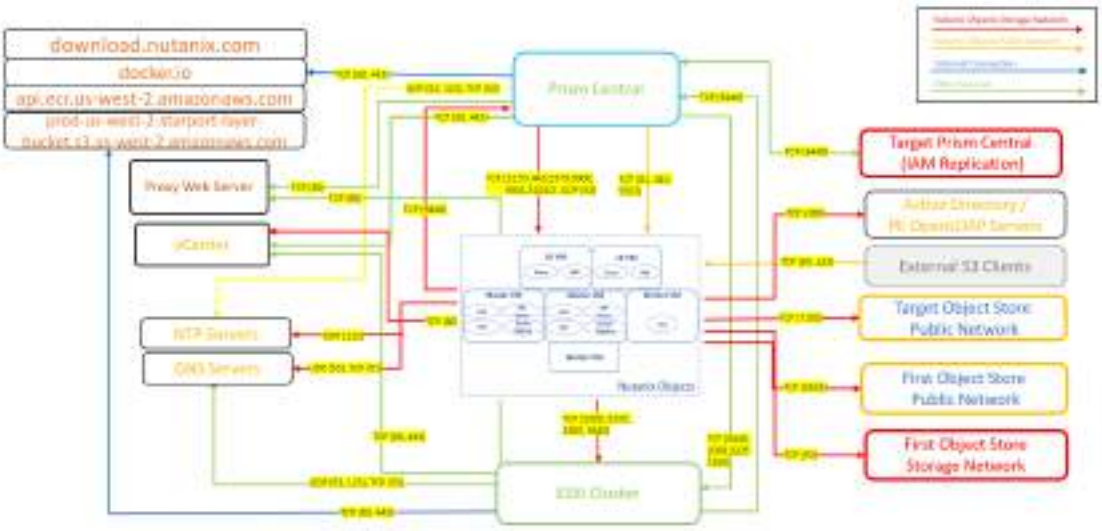


Figure 31: IAM-HA Disabled Objects Network Diagram with Ports (ESXi)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 772

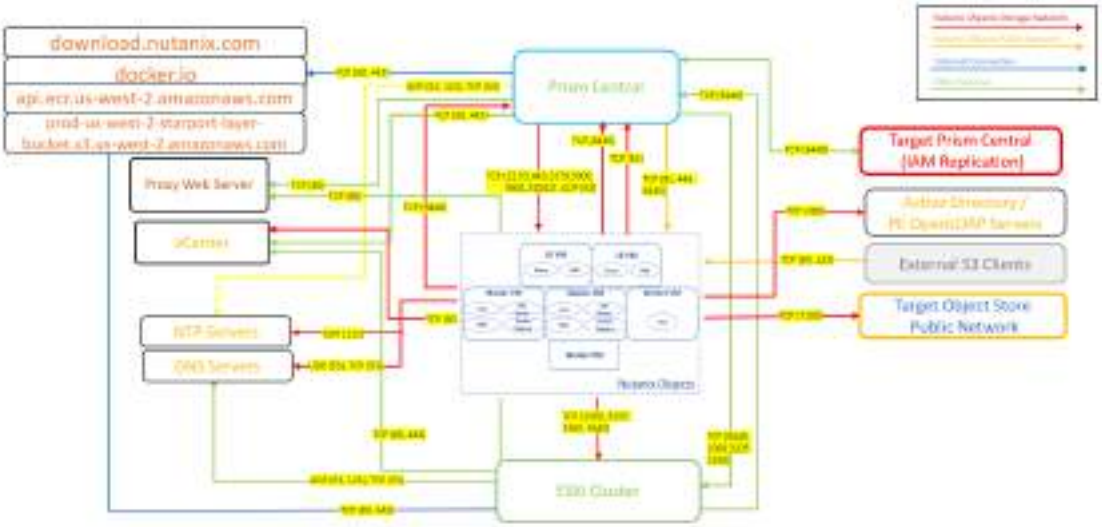


Figure 32: IAM-HA Enabled Objects Network Diagram with Ports (ESXi)

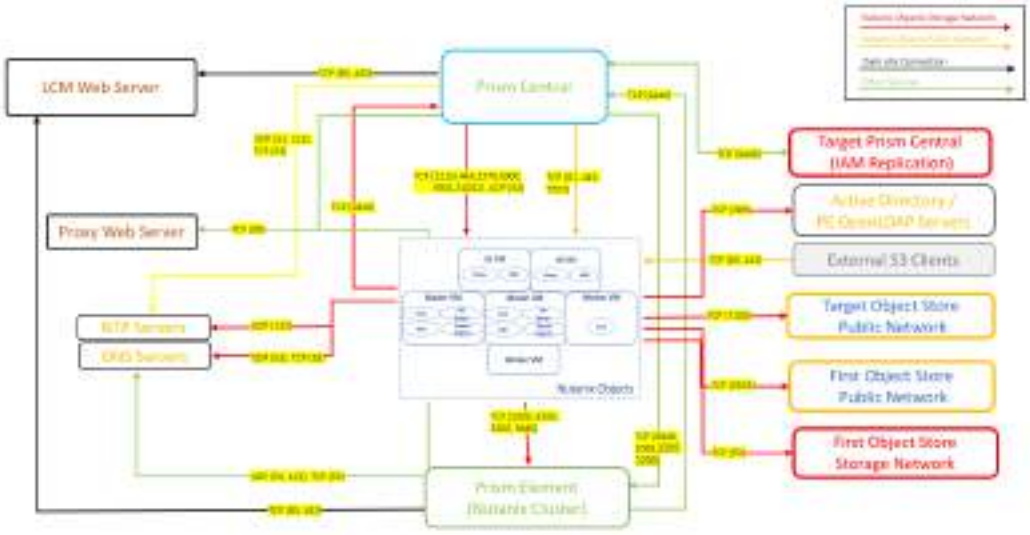


Figure 33: IAM-HA Disabled Objects Network Diagram with Ports (Dark Site)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 773

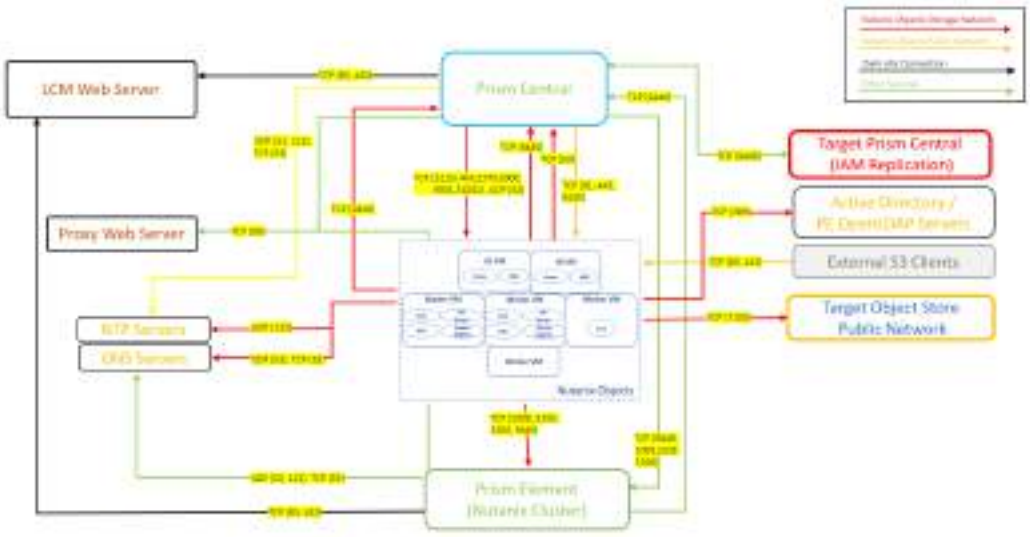


Figure 34: IAM-HA Enabled Objects Network Diagram with Ports (Dark Site)

Limitations

The following section lists the limitations for Objects.

System Limitations

- Once an object store gets deployed, you cannot change the Data Services, Controller VM, Microservices Platform (MSP), and Prism Central IP addresses.
- Prism Central and Prism Element de-registration and reregistration is not supported.

Limitations of NFS

This section lists the limitations of multiprotocol access.

- NFS adapter in Objects does not support Windows NFS client.
- You can enable NFS access only at the time of bucket creation.
- NFS-enabled buckets are exposed as NFS shares, which can be mounted by the NFS clients.
- You can perform update (only multiprotocol access configurations), delete, and share actions on NFS buckets.

  Note: You can delete NFS-enabled buckets only if it does not have any object and any directory explicitly created from the NFS protocol.

- You cannot enable other S3 bucket features, such as Lifecycle Policies, Versioning, WORM, Replication, Static Website, CORS, and Notifications on NFS-enabled buckets.
- You can only create symbolic links through NFS. Hard links are not supported.
- You can rename files and links; however, you cannot rename a directory. After renaming, the file handle of the renamed file changes.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 774

- In addition to the S3 object naming convention, the following are some cases, which are not allowed for an object name in the NFS-enabled bucket:
  - Object name cannot be **.** or **..**
  - Object name cannot start with **/**,**./** or **../**
  - Object name cannot contain **//**, **/./** or **/../** pattern.
  - Object names cannot end with **/.** or **/..**
  - If an object name contains a directory hierarchy, then each component in the object name separated by **/** cannot be more than 255 bytes in length.
- Objects with **/** as suffix or objects-browser-created folders, which will appear as directories in the NFS namespace cannot be deleted from the NFS protocol.
- If the objects are created from the S3 protocol in such a way that they end up creating a conflict in the object and directory name, then only the file will be visible in the NFS namespace and the directory will get hidden. Only on renaming or removing the file to some other name, the directory will become visible again.

  For example, suppose we create two objects `dir1/dir2/file` and `dir1/dir2` from the S3 protocol. As we can see, `dir2` is a directory as well as a file, so it creates a conflict. Now, while traversing this namespace from NFS protocol, once we are inside `dir1/` directory, only the object `dir2` would be visible and not the subdirectory `dir2/`. So, it is recommended to not use conflicting names for objects while creating them from the S3 protocol.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 775

FEDERATION OVERVIEW

In the context of a single Objects instance, *namespace* is a set of unique buckets hosted by that instance. Federation provides a way to create a single namespace across multiple individual Objects instances. One federation instance corresponds to one such namespace.

A federated namespace can span across multiple Objects instances that potentially reside in different geographical locations.

Each Objects instance has a default local namespace that is independent of any other Objects instance. In addition, an Objects instance can join multiple federated namespaces by becoming a member of each federation.

Any Objects instance that joins a federation as a member can contribute to the federated namespace. A federated namespace can be accessed from any of the members using the Federation FQDN in the **Host** field of the HTTP requests.

Federated namespace supports the following properties:

- Federated namespace enforces unique bucket names within the namespace.

  For example, if a client creates a bucket `foo` in a federated namespace, then another client that later tries creating the bucket `foo` would fail with error message `BucketAlreadyExists` or `BucketAlreadyOwnedByYou`.

- All clients, irrespective of which federation member they choose to access the federated namespace from, see the same consistent list of buckets.
- Any buckets and objects that are part of the federated namespace can be accessed from any of the members.

A federation instance is supported in the backend using a subset of the federation members, called **Core Members**. Core members, together, run a distributed consensus service in the backend to provide fault tolerance for the federated namespace.

Figure 35: Federation

Prerequisites - Federated Namespace

Before creating a Federated namespace, review this section carefully to ensure you have met the prerequisites.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 776

- You must have at least one object store instance managed by a single or multiple Prism Central instances.
- For Objects 4.0, it is necessary to upgrade Prism Central and Prism Element to compatible versions, with a minimum required Prism Central version of 2022.9.
- Objects Manager on all Prism Central instances must be upgraded to compatible versions.
- Established AZ pairing between Prism Central instances.
- Setup IAM replication across Prism Central instances.

> **Note:** IAM pairing works only when both Prism Centrals have either IAM-HA enabled or disabled.

To create federated namespace, refer to Creating Federated Namespace on page 62.

Creating Federated Namespace

Nutanix federation namespace is a mechanism that enables multiple independent systems to share a common namespace or naming system. This allows different systems to refer to the same resources using the same names, even if those resources are located in different systems and locations.

Before you begin

To create a federated namespace, do the following:

Procedure

1. Log on to the Prism Central web console, in Application Switcher, select **Objects** > **Federated Namespaces**.
2. Click **Federated Namespaces**.

Figure 36: Federated Namespace

> **Note:**
>
> - Ensure SSL are updated with the federation FQDN for individual object stores that will be part of the corresponding federated namespace.
> - Ensure your DNS is configured to map the federation FQDN to the object store public IP addresses so that applications can access the federation namespace.
> - The Federation FQDN should not be a subdomain of the Prism Central domain.
>
> .

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 777

3. Click **Create Federated NameSpace**.

   After clicking **Get Started** on the prerequisites pop-up window that provides the necessary details, you will be directed to a new window for creating a federated namespace.

Figure 37: Create Federated Namespace

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 778

4. Update the fields as indicated:

   - **Name:** Enter the name of federated namespace.

     The federation name must meet the following guidelines.

     - Must be unique across all existing federations.
     - Must start with a letter.
     - Can have alphanumeric or hyphen characters. Hyphen can only be used in the middle of the name.
     - Must not contain special characters.
     - Must be a minimum of 1 and a maximum of 16 characters long.
   - **Domain:** Enter the domain.
   - The federation domain must meet the following guidelines:

     - It must contain at least one dot.
     - It may contain either alphanumeric or hyphen characters.
     - It must not start or stop with a hyphen or a dot.
     - When selecting a federation fully qualified domain name (FQDN), it's important to avoid using a subdomain that belongs to any of the MSP subdomains that are connected to the Prism Central web console.
   - **Object Stores:** Select and add at least one object store instance. It is recommended to have at least three instances from different clusters to set up federation. You can select all the required object store instances that run the federation services.

     > **Note:** Once you select the Object stores, the visual representation on the right changes accordingly.

   - **Federation core member:**

     A federation instance is supported in the backend using a subset of the federation members, called **Core Members**. Core members, together, run a distributed consensus service in the backend to provide fault tolerance for the federated namespace.

     You can select and designate core members from the list of Object stores.

   - > **Note:** To ensure higher fault tolerance in case of cluster failure, you can add 1, 3, or 5 core members from the same or different clusters.

   - **Federation members:** All object stores participating in the federation are called federation members.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 779

5. Click **Setup**.
   The federation setup is ready.

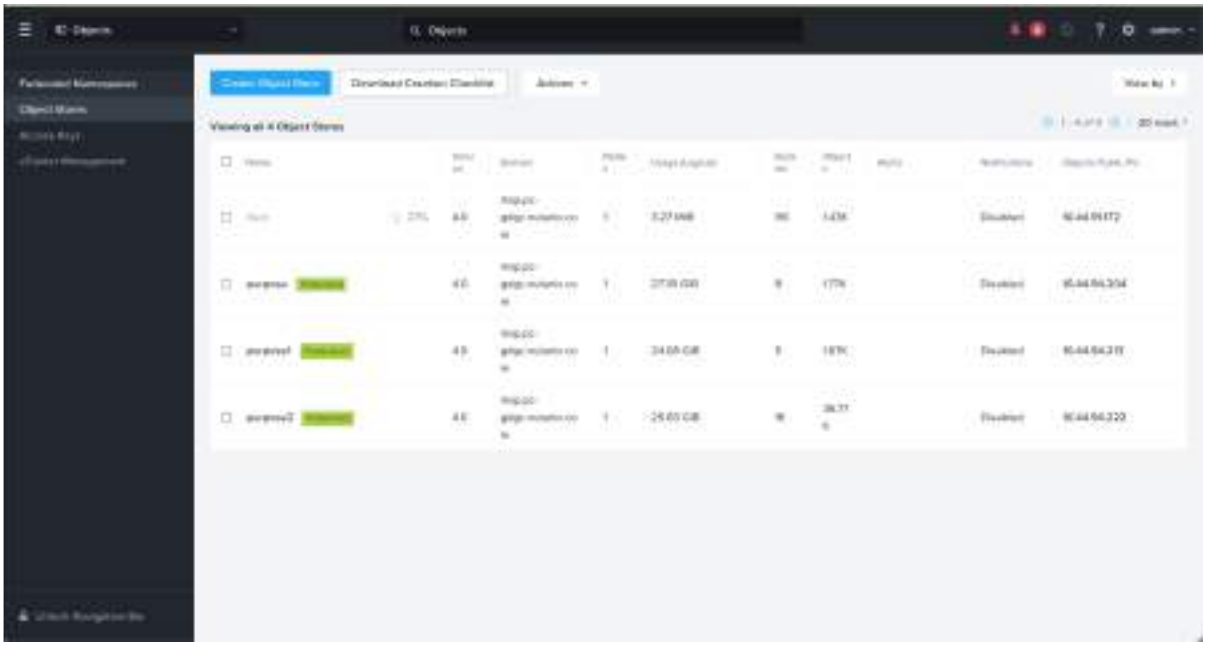


Figure 38: Federation Setup

What to do next

After creating a federated namespace, you can view and perform operations on the namespace. For more information, refer to Viewing Federated Namespaces on page 66 section.

Managing Federated Namespace

After creating a federated namespace, you can view details and manage the object stores.

About this task

To manage and add object store do the following:

Procedure

1. Log on to the Prism Central web console.
2. In Application Switcher, select **Objects** > **Federated Namespaces**.
   A list of existing Federated Namespaces appears.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 780

3. Select a **Namespace**, and click **Manage Namespace** .
   The Federated Namespace opens in a new window.

Figure 39: Federated Namespace

4. To remove an object store, first select an object store, and then click **Remove Object Store**.
   The object store is removed.

5. Click **Add Object Store** to add an object store to the existing federation.
   The Add Object Store window appears. Select and add the required object stores.

   Note:

   - You can add between 1 and 20 object stores.
   - Core members cannot be added to a federation.
   - A core member cannot be removed.
   - When selecting a member that should be added to a federation during creation or later, you should filter out the unhealthy object store instances, to ensure the federation **add_member** operation does not fail at a later stage.

6. Click **Delete Federation** to delete the federation.
   Navigates back to the list of existing federations. You cannot access the deleted federation.

What to do next

You can view the object store and check if they are part of the local namespace or federated namespace, see Viewing Object Store Summary on page 81.

Viewing Federated Namespaces

You can click any Federated Namespace to view all the details of the Summary and Object stores.

The following table lists and defines the fields used in Summary and Object stores:

Table 5: Summary

Term	Description
Name	Displays the name of the object store.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 781

Term	Description
Domain	Displays the domain of the object store.
FQDN(s)	Displays a complete address to access the Federation.
Object Stores	Displays the number of object stores.
Buckets	Displays the number of buckets in an object store.
Object Browser	Displays a link to access the federated namespace.

Table 6: Object Stores

Term	Description
Name	Name of the Object store
Buckets	Number of buckets for the particular Object store
Objects	Number of Objects for that particular Object store
Capacity Usage (logical)	Displays the object storage capacity usage.
Version	Displays the version of Objects in which the object store was created.
Public IPs	Displays the public IP addresses of Object store. These are presented as links that can be used to launch the Objects Browser.
PC Location	Displays the location of the Object store.

Deleting Federated Namespace

You can delete an existing Federated Namespace.

About this task

Note:

- A healthy federation can be deleted
- Bulk deletion is not allowed.
- If a federation service fails to start, it can be deleted.

To delete a federated namespace, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In Application Switcher, select **ObjectsFederated Namespaces**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 782

3. Select the required **Federated Namespace** to delete.

> **Note:** Clear out all the objects and buckets stored in the selected Object store.

The federated namespace opens in a new window.

Figure 40: Federated Namespace

4. Click **Delete Federation**.
   The federated namespace is deleted.

What to do next

You can view the different error messages in federated namespace, see Errors in Federated Namespace on page 68.

Errors in Federated Namespace

When an error occurs while creating a federated namespace, the description lists the type of error.

Following are the different types of error seen in a federated namespace.

Table 7: Errors

Error type	Description	Steps to recover
Addition Failure	Inability to add a new object store to an existing federation.	1. Check the object store. 2. Get back the object store to a healthy state.
Backend Unreachable	When services of some of the object stores that are a part of the federation are down.	1. Check the object store. 2. Get back the object store to a healthy state.
Creation Failed	When the service cannot be created.	1. Check the object store. 2. Get back the object store to a healthy state.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 783

Error type	Description	Steps to recover
Deletion Failure	Inability to delete an object store as it is hosting buckets or objects.	1. Check the object store. 2. Clear out all the objects and buckets stored in the selected object store.
Transport error	When core members are unreachable.	1. Check the object store. 2. Get back the services to a healthy state.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 784

OBJECT STORE SERVICE DEPLOYMENT

Objects is a highly available and distributed Object Store Service which can store petabytes of data.

To start using Objects, you need to deploy the Object Store Service. Refer to Creating or Deploying an Object Store (Prism Central) on page 70. You can also perform offline deployment (site without Internet access) of an object store. Refer to Deploying Object Store at a Dark Site (Offline Deployment) on page 98.

You can deploy multiple Objects instance on a single Prism Element registered to a Prism Central, or you can register multiple Prism Elements to one Prism Central and deploy as many object stores on each of these Prism Elements provided you have sufficient storage.

You can do the following operations after deploying an Objects instance:

1. Configure the directory and generate the access key. Refer to Directory Configuration and Access Key Generation on page 106.
2. Create buckets within the object store. Refer to Creating and Configuring an S3 Bucket on page 118
3. Upload objects and meta-data to the buckets by using the S3 APIs. Refer to Supported APIs on page 240.

Note:

- After registering Prism Element to Prism Central, wait for 10 minutes before starting the deployment.
- Parallel Object Store Service deployments are not supported.
- If your deployment fails due to precheck failures, you can resume the deployment after fixing the configuration.
- For objects containers, the EC delay will be reduced from 7 days to 3 days for old and new deployments.

Object Store Instance Naming Conventions

The name of an object store must conform to the following rules:

- Be unique across all existing object store names in Objects.
- Begin with a letter, and end with a letter or number.
- Can contain alphanumeric or hyphen characters.
- Not contain any special character other than a hyphen.
- Minimum of 1 and a maximum of 16 characters long.

Note: You cannot change the name after creating the object store.

Creating or Deploying an Object Store (Prism Central)

Before creating a bucket and uploading objects, you must deploy an object store. You can deploy multiple Object Store Services on a single Prism Element registered to a Prism Central, or you can deploy multiple object stores on each Prism Element accessible from Prism Central provided you have sufficient storage.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 785

Before you begin

Make sure you satisfy the deployment prerequisites before starting the deployment. Refer to Deployment Prerequisites - AHV and ESXi on page 40.

A non-admin user can create or deploy an object store only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions and the non-admin user must be assigned to specific objects instances:

- Create Object Store
- View Cluster
- View Subnet (only for AHV)

> **Note:** Administrators and non-admin users are Prism Central users with the following roles:
>
> - Administrator—A Super Admin or a Prism Admin in Prism Central.
> - Non-admin user—A Prism Central user without any administrator privileges.
>
> For more information on the built-in roles in Prism Central, see *Built-in Role Management* in the *Security Guide*.

In addition to the above permissions, the user must also have:

- View Cluster access to the Prism Element on which the Objects instance will be deployed
- View Subnet access to the managed networks that will be used for deployment if the Prism Element runs on AHV

> **Note:** When you create an access control policy, select Cluster as the Entity type, and select Individual Entity, and then select All Clusters or the particular cluster on which you need to deploy the object store.

The user, who creates an Objects instance, gets full access to that Object instance automatically. This full access can be later revoked or modified by the administrator user.

About this task

> **Note:**
>
> - You cannot deploy a single Object Store Service across multiple Prism Elements.
> - If you exit by clicking **X** while creating an object store, the entered input and the pre-checks status are not saved.
> - Deployment can take a minimum of 30 minutes.
> - A new container with `msp-<uuid>` is created for Objects deployment on ESXi. This container will be used for downloading VM images for MSP workers.
> - DNS configuration has to be manually added on the client side to resolve Objects FQDN to Objects Public IP address.
> - If CMSP is enabled, you cannot input the domain name for the object store deployment. The CMSP domain is used as the object store domain. If you want to use a different domain, add FQDNs to those domains for the object store. See Managing FQDN and SSL Certificate on page 93.

To create an object store, do the following:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 786

Procedure

1. Log on to Prism Central.
2. In the Application Switcher, click **Objects**.
3. Click **Create Object Store**.
4. In the **Create Object Store: Prerequisites** window, click **Continue** if you fulfil the prerequisites for AHV or ESXi.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 787

5. On the **Object Store Details** section, do the following, and then click **Next**:

Figure 41: Object Store Details

- You can view the summary of the object store by clicking **Show Summary** on the right pane.
- You can hover over the help icon to get more information about the respective fields.
- The diagram updates automatically with the required worker nodes, load balancers, and resources required for the number of the worker nodes selected.
- Active components will be highlighted in the diagram.

a. **Object Store Name**: Enter the name of the object store you want to create.
For guidelines on choosing a compliant name, refer to Object Store Naming Conventions.

b. **Domain**: Enter the domain name.

> **Note:** This domain name is the default domain name for all the object store in that cluster.

Domain naming conventions:

- Must contain at least one dot.
- Can contain either alphanumeric, hyphen, or underscore characters.
- Cannot start or end with a hyphen or underscore or dot.

c. **Cluster**: Select the cluster where the object store will be deployed.

d. **Worker Nodes**: Add the number of worker nodes.

> **Note:**
>
> - The configured worker nodes cannot exceed the worker nodes of the cluster.
> - Resources cannot be reduced once added.
> - Actual performance depends on a variety of factors.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 788

- Each VM is assigned 10 vCPUs and a DHCP IP address.
- A minimum of 10vCPUs and 32 GiB of memory is required.
- Each click on plus for Worker Nodes add 10vCPUs and 32 GiB of memory.
- vCPU and memory are linked. vCPU has to be in multiple of 10 and memory in multiple of 32.

6. On the **Storage Network** section, do the following, and then click **Next**:

Figure 42: Storage Network Details

a. **Storage Network**: Select Objects storage network that is used for the internal communication between the components of an object store.

   For more information on the IP address requirements according to the deployment size, see Network Configuration.

b. (Only for AHV) **Object Store Storage Network Static IPs (2 IPs required)** : Enter two storage network IP addresses separated by a comma.

   - These storage network IP addresses are within the Objects Storage Network.
   - Object store will use two additional IP addresses for the nodes or VMs connected to the internal network.

   Note: For ESXi, these two internal IP addresses are not required and selected automatically from the IPAM range configured for ESXi networks.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 789

7. On the **Public Network** section, do the following and then click **Save & Continue**:

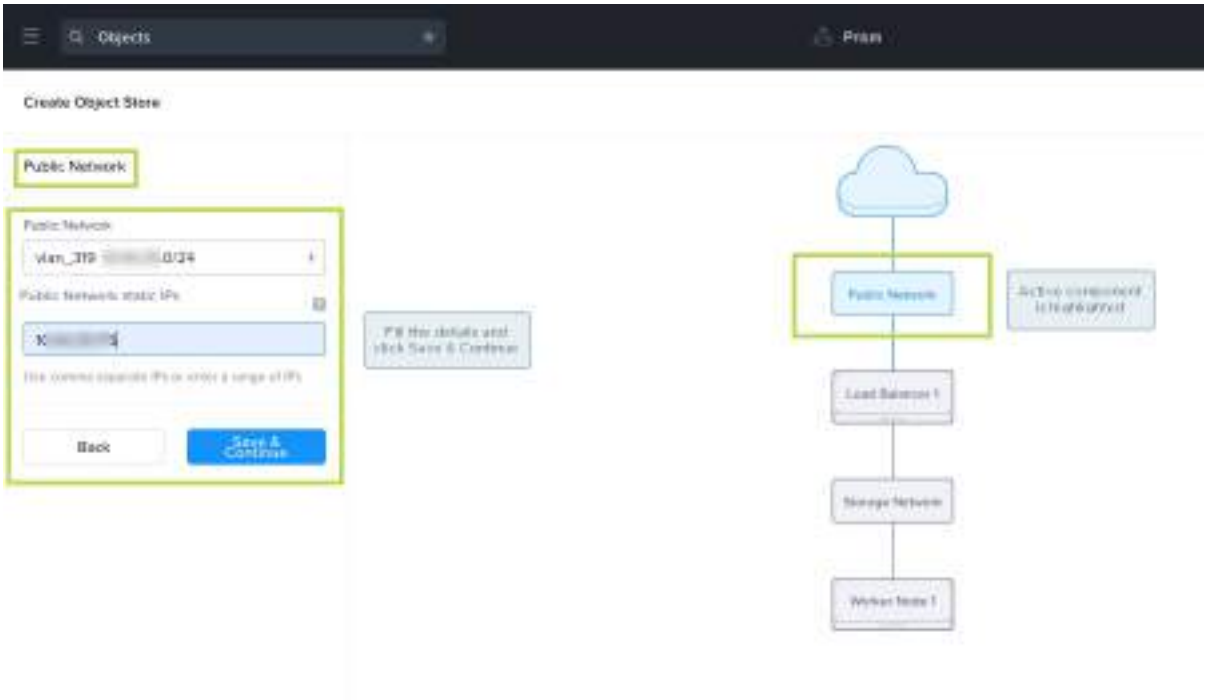


Figure 43: Public Network Details

a. **Public Network**: Select Objects public network that is used to allow access to the Object Store from the external clients.

   This VLAN should have up to four IP addresses in the usable IP address range. This network can be the same as the Storage Network. For more information, see Shared Versus Single Network on page 54.

b. In the **Public Network Static IPs**: Enter the public access IP addresses (one for each load balancer) separated by a comma or as an IP address range.

   For example, if one Load Balancer is used, then only one IP address is required. Also, you can enter the IP addresses in a range, `10.2.3.1-10.2.3.4`, or separated by a comma `10.2.3.1, 10.2.3.2, 10.2.3.3, 10.2.3.4`

   AHV - These IP addresses are within the Objects Public Network and used to access the object store.

   ESXi - The public access IP addresses can be within or outside the range of the IPAM network.

   For more information about network configurations, refer to Network Configuration on page 42.

You can click **Save for Later** if you wish to continue with the deployment later. The object store will be saved in the list of object stores. Select the object store, and then click **Actions** > **Complete Deployment** to complete the deployment.

Pre-checks starts before the deployment begins. A list of checks performed is displayed in the UI. Also, a VM image named *predeployment_port_vm*, and two VMs named *predeployment_objects_public* and *predeployment_objects_storage* are created.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 790

Figure 44: Pre-deployment checks status and report

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 791

8.

Note: All pre-checks must pass to start the deployment.

Depending upon the pre-check result, do the following:

» If the pre-checks are passed, click **Download Report** to download the report, and then click **Create Object Store** to start with the object store deployment.

The report contains the name of the check, status, and message.

» If the pre-checks fail, an error message is displayed in the UI. Click **Download Report** to download the report. A `Fail` status is displayed next to the check name with a message. The object store is saved and you can complete the deployment after fixing the failed checks.

Once the pre-checks are passed, you can view the status of the object store deployment.

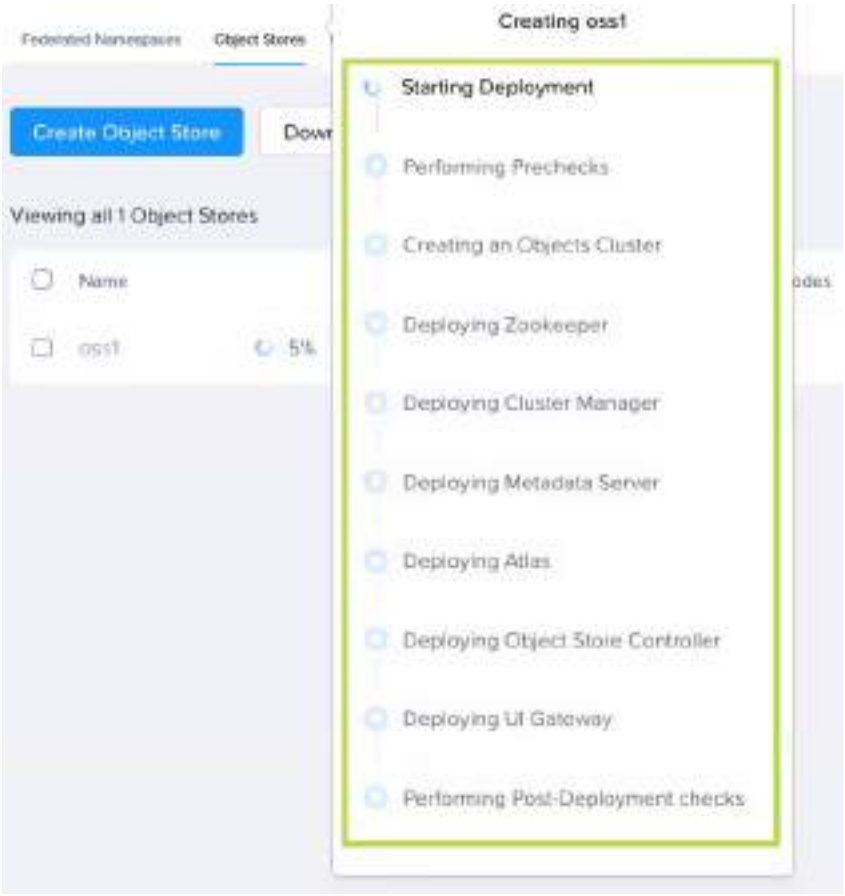


Figure 45: Deployment Steps

You can view the deployment progress in percentage and each step in the grid by hovering over the loading icon.

Note: Use an encrypted cluster for encrypting the bucket.

Warning: Do not delete MSP VMs (created with a prefix in Objects deployment) from the vCenter or Prism Central. There are no checks to identify the deletion of MSP VMs. You can identify the MSP VMs by their name. The naming conventions are as follows:

- MSP Worker VM: *`deployment_name`*`-XXXXXX-default-N`

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 792

- Load Balancer MSP VM: *deployment_name*-XXXXXX-XXXXXXXXXX-envoy-N

What to do next

After deploying the object store, you can perform the following:

- Configure directory and generate access key. Refer to Directory Configuration and Access Key Generation on page 106.
- Access the endpoint provided as part of Client Access Network (S3 Endpoints) by using HTTP or HTTPS. Refer to Access Objects Endpoints on page 81.
- Create and configure buckets. Refer to Creating and Configuring an S3 Bucket on page 118.
- Create objects using S3 APIs. Refer to Supported S3 APIs
- Expand the object store storage. Refer to Expanding Storage for an Object Store on page 84
- Scale out an object store. Refer to Scaling Out an Object Store on page 88
- Share buckets. Refer to Sharing a Bucket on page 151.

Viewing Object Store Deployments

You can view a list of deployed object stores, and the general and networking details of the object stores.

Before you begin

A non-admin user can view an object store only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have minimum permission to view an object store and the non-admin user must be assigned to specific Objects instances.

Note: Administrators and non-admin users are Prism Central users with the following roles:

- Administrator—A Super Admin or a Prism Admin in Prism Central.
- Non-admin user—A Prism Central user without any administrator privileges.

For more information about the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.

About this task

To view the object store, do the following:

Procedure

1. Log on to the Prism Central web console.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 793

2. In the Application Switcher, click **Objects**.

Figure 46: Object Stores List View

A list of existing object stores appears. The following steps describe the fields that appear in the object store table. You can click on the name of an object store to open the object store in a new window. You

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 794

can click **View By** to view the **General**, **Usage**, or **Networking** details of an object store. A dash (-) is displayed in the field when a value is not available or applicable.

General view:

- **Name**: Displays the name of the object store. A *Federated* tag is displayed next to the federated object stores.
- **Version**: Displays the version of Objects in which the object store was created.
- **Domain**: Displays the domain of the object store.
- **Nodes**: Displays the number of nodes of the object store.
- **Usage (Logical)**: Displays the object store usage in GiB or TiB.
- **Buckets**: Displays the number of buckets in an object store.
- **Objects**: Displays the number of objects in an object store.
- **Alerts**: Displays the alerts for a particular object store.

  For more information, refer to Viewing Alerts on page 218.
- **Notifications**: Displays notifications if any.
- **Objects Public IPs**: Displays the endpoints or the IP addresses used by the client.

  You can access these endpoints by using HTTP and HTTPS protocols. For more information, refer to Access Objects Endpoints on page 81.

Networking view:

- **Name**: Displays the name of the object store.
- **Cluster**: Displays the cluster in which the object store is deployed.
- **Objects Public Network**: Displays the VLAN required for accessing object store endpoints externally.
- **Objects Public IPs**: Displays the public IP address of Objects. This is used to access the Objects Browser.
- **Objects Storage Network**: Displays the VLAN required internally for deploying Object Store Services on Prism Element.
- **Storage Network Static IPs**: Displays the internal configured IP addresses.

Usage view:

- **Name**: Displays the name of the object store.
- **Usage (Logical)**: Displays the cluster in which object store is deployed.
- **Local Usage**: Displays the amount of data stored locally in the Objects cluster.
- **Tiered Usage**: Displays the amount of data tiered out and stored remotely based on lifecycle policies.
- **Licensed Usage**: Displays the usage from a single object store accounted against the licensed capacity. It is calculated as (Local Usage + Tiered Usage).

  Note: Data tiered to another Objects endpoint is not included.

For information about Network Configurations, refer to Network Configuration on page 42.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 795

What to do next

You can view the summary of an object store and perform various object store operations, see Viewing Object Store Summary on page 81.

Access Objects Endpoints

Objects endpoints are the entry point to Objects. You can access these endpoints by using the HTTP or HTTPS protocols through any third-party clients which support S3 APIs.

Accessing Buckets and Objects within an Object Store Instance

Objects supports path-style and virtual hosted-style bucket access.

- **Path-Style Access**: The path-style syntax requires that you use the endpoint when attempting to access a bucket, and the request specifies a bucket by using the first slash-delimited component of the Request-URI path.

  For example, if you have a bucket with the bucket name as **bucket-name** and the object name as **example.jpg**, and you want to use the path-style syntax. Following is the correct request:

  ```
  PUT /bucket-name/example.jpg HTTP/1.1
  Host: object-store-name.domain-name
  ```

- **Virtual Hosted-Style Access**: The virtual hosted-style syntax is used to address a bucket in a REST API call by using the HTTP Host header. This method requires the bucket name to be DNS-compliant.

  For example, if you have a bucket with the bucket name as **bucket-name** and the object name as **example.jpg**, and you want to use the virtual hosted style. Following is the correct request:

  ```
  PUT /example.jpg HTTP/1.1
  Host: bucket-name.object-store-name.domain-name
  ```

  For virtual hosted-style access, allow the Objects FQDN in the DNS server with the wild card allowlist. For example, the following are the expected DNS entries for the Objects endpoint.

  ```
  objects.subdomain.example.com.        IN      A       192.168.5.101
  objects.subdomain.example.com.        IN      A       192.168.5.102
  objects.subdomain.example.com.        IN      A       192.168.5.103
  objects.subdomain.example.com.        IN      A       192.168.5.104
  *.objects.subdomain.example.com.      IN      A       192.168.5.101
  *.objects.subdomain.example.com.      IN      A       192.168.5.102
  *.objects.subdomain.example.com.      IN      A       192.168.5.103
  *.objects.subdomain.example.com.      IN      A       192.168.5.104
  ```

Viewing Object Store Summary

You can view the summary of an object store. The summary comprises of configuration, namespaces, and usage of the object store.

About this task

To view the object store summary, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 796

3. Click the **Object Stores** tab, and then click the name of the object store from the table to view its summary.

Figure 47: Object Stores List View

4. Click the **Summary** tab.

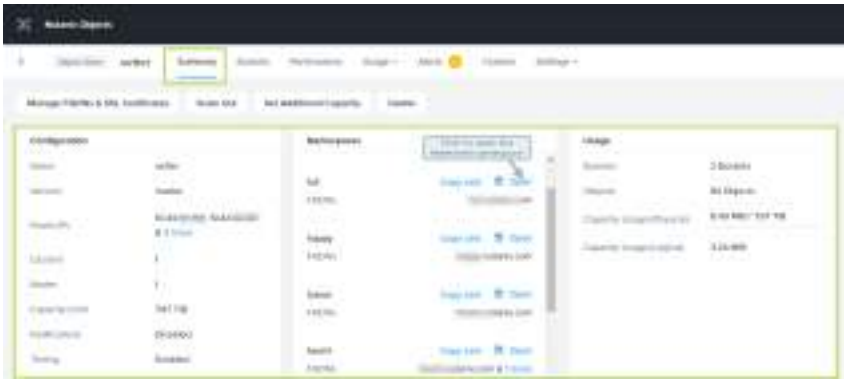


Figure 48: Object Stores Summary View

You can view the object store configurations, federated namespaces, and usage.

What to do next

You can do the following from the object store summary page:

- Managing FQDNs and SSL Certificates, see Managing FQDN and SSL Certificate on page 93.
- Scaling out an object store, see Scaling Out an Object Store on page 88.
- Expanding an object store, see Expanding Storage for an Object Store on page 84.
- Deleting an object store, see Deleting an Object Store on page 82.
- Launching Objects Browser, see Launching the Objects Browser on page 165.

Deleting an Object Store

You can delete both successful and failed object store deployments. However, for deletion of successful deployment, ensure to first delete the objects and buckets within that object store.

Before you begin

A non-admin user can delete an object store only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions and the non-admin user must be assigned to specific objects instances:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 797

- Delete Object Store
- View Object Store

> **Note:** Administrators and non-admin users are Prism Central users with the following roles:
>
> - Administrator—A Super Admin or a Prism Admin in Prism Central.
> - Non-admin user—A Prism Central user without any administrator privileges.
>
> For more information on the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.

About this task

> **Note:**
>
> - Deployments in progress cannot be deleted.
> - You cannot delete the primary cluster without deleting the secondary cluster as the primary object store cluster hosts all the common services. To delete the primary cluster, ensure all the secondary clusters are deleted.
> - Multi-cluster containers are not deleted on secondary Prism Elements if the Objects deployment is not successful.
> - If a failure occurs while replacing an SSL certificate for an object store, you cannot delete that object store deployment; however, you can try replacing the SSL certificate again.
> - Deletion of an object on the local object store may not immediately lead to space reclamation on the AWS S3. Space reclamation happens when all the source objects mapped to the corresponding objects in the AWS S3 get deleted.

To delete an object store deployment, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the Object Stores table, select the object store which you want to delete, and then click **Actions** > **Delete**.

Figure 49: Delete Object Store Window

4. On the confirmation dialog box, click **Delete**.
   A message appears to confirm the object store deletion.

Object Store Expansion

This section describes the expansion options available with object store.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 798

Storage Expansion

If your existing object store storage is less than 85% full or you want to use a different cluster for object store storage, you can expand the storage of your object store cluster by adding new nodes to the existing cluster or by adding additional clusters.

For example, if you have an object store deployed on a 10 TB cluster named *Cluster1* and your storage is almost or less than 8.5 TB full, then you can either add a node to the existing *Cluster1* or add a new cluster or existing clusters (such as *Cluster2* and *Cluster3*) if they have sufficient storage capacity. In this example, *Cluster1* is the existing primary cluster on which the object store was initially deployed and hosts the worker VMs for the object store. *Cluster2* and *Cluster3* are secondary clusters that are later added for capacity expansion.

Scale-Out (Compute and Memory Expansion)

Scaling out an object store enables you to add more resources to an existing object store cluster. You can scale out the CPU count and memory, and optionally, add more storage in addition to the current usage. Scale out uses an extra 10 vCPUs and 32 GiB memory for the newly added node.

Expanding Storage for an Object Store

Before you begin

Following are the requirements to add a new cluster to an existing object store.

- Ensure to upgrade to MSP 1.0.5 and Objects 2.0 before expanding the object store cluster.
- Ensure that the new clusters are registered to the same Prism Central cluster where the object store is deployed.
- Primary and secondary clusters should have versions greater than AOS 5.11.2.
- Up to 4 secondary clusters are supported.
- VMware ESXi and Nutanix AHV clusters are supported. Microsoft Hyper-V cluster is not supported.
- Data services IP address must be configured in each secondary cluster.
- Firewall must be running on the CVMs in the cluster.
- Maximum latency required for adding secondary clusters is less than 5 milliseconds.

Note:

- You cannot add secondary clusters if the primary cluster is full. You should add the secondary clusters before the primary storage reaches 80% of the total capacity.
- When you add a secondary cluster to an empty object store (with no objects) and if suddenly the secondary cluster becomes unreachable, then an alert will not be displayed for that Prism Element and that cluster will not be shown in the user interface. However, once you start adding objects to that object store, an alert will be raised and the unreachable cluster will be marked in the user interface in a minute.

Caution: Primary clusters cannot be removed once successfully added to an object store.

A non-admin user can expand storage for an object store only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions and the non-admin user must be assigned to specific objects instances:

- View Multicluster

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 799

- Add Multicluster
- Update Multicluster
- View Cluster
- View Object Store

> **Note:** Administrators and non-admin users are Prism Central users with the following roles:
>
> - Administrator—A Super Admin or a Prism Admin in Prism Central.
> - Non-admin user—A Prism Central user without any administrator privileges.
>
> For more information about the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.

In addition to the above permissions, the user must have View Cluster permission on the Prism Element that needs to be added to the Object store.

Update Multicluster is needed only to update the capacity or to delete an added cluster.

About this task

To expand the object store storage, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. Click the **Object Stores** tab, and then click the name of the object store for which you want to expand the storage.

Figure 50: Object Stores List View

The object store opens on a new window.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 800

4. Click **Clusters**.

Figure 51: Object Store Clusters List

> **Note:** You can expand your object store cluster by adding one secondary cluster at a time.

The table lists the Usage, Max Usable and Free Capacity of the cluster. All the capacities listed are physical capacities, not logical.

- **Usage (Physical)**: Physical capacity used by this object store on the cluster.
- **Max Usable (Physical)**: Maximum physical capacity on the cluster can be used by this object store. This is calculated as the total physical capacity of the cluster * any limit set for this cluster - capacity used by other workloads. Your available capacity might be less than you planned for as other workloads are taking up the space.
- **Free Capacity (Physical)**: Additional capacity the object store can consume on this cluster within the specified limit. It is possible that there might not be free capacity available for the object store to consume even if current consumed capacity is less than max usable since there may be other workloads consuming capacity from this cluster.

For example, Cluster A is a primary cluster with 10 TB as the total capacity. No hard limit can be set on this cluster as it is a primary cluster. So, the *Max Usable Physical Capacity* of this object store cluster is 10 TB. However, the current object store usage is 5 TB and other workloads usage is 2 TB. So, the additional *Physical Free Capacity* available for the object store is 3 TB. However, in case of Cluster B which is the secondary cluster with total capacity as 15 TB, the hard limit is 50%. So, the *Max Usable Physical Capacity* of this object store cluster is 50 % * 15 TB = 7.5 TB. However, the current object store usage is 2 TB and other workloads usage is 10 TB. So, the additional *Physical Free Capacity* available for the object store should be 5.5 TB, but as the the other workloads consume 2.5 TB of the *Max Usable Physical Capacity* of the object store, so the remaining *Physical Free Capacity* available for the object store is only 3 TB. So, other workloads can consume the *Max Usable Physical Capacity* of the object store; however, an object store cannot go beyond the set limit.

Your primary cluster where the object store is deployed will be displayed in the table and this cluster cannot be removed. You can also view the free and used storage space.

5. Click **Add Clusters**.

> **Note:**
>
> - Once you have added 4 secondary clusters, the **Add Clusters** button will be disabled.
> - When adding a cluster, you cannot remove another cluster or reduce the limit of another cluster; however while removing the cluster or reducing the limit of the cluster, you can add another cluster.

A list of clusters registered to the Prism Central will be displayed. Hypervisor type, total physical capacity and free physical capacity of the clusters will also be displayed. However, the clusters that are already added as secondary clusters to an object store will not be displayed.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 801

6. Once you select the cluster, under **Set up hard limit** section, select the usage limit in percentage, or select **Custom** and enter a custom limit for an object store, and then click **Done**.

   This limits the object store to use a maximum capacity on the selected cluster. If you exceed the limit, an alert is generated.

Figure 52: Setting Up Hard Limit

You can change the limit (increase or decrease) once a secondary cluster is added. Select the cluster, and then click **Update Limit**. You cannot update the limit for the primary cluster. You can also remove

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 802

the secondary clusters once added. Select the cluster, and then click **Remove**. The removed cluster can be added back to the multi-cluster.

Note: Points to note when updating the limit of the secondary clusters or removing the secondary clusters.

- If the secondary cluster is empty, then the removal of that cluster takes up to 3 hours.
- If the secondary cluster has some data, and the storage limit is reduced or the cluster is removed, then starting the data migration process may take up to 7 hours.
- When you reduce the limit of the secondary cluster and if the used capacity of the cluster is less than the updated limit capacity, then no data migration takes place and limit is changed without any delay.
- When adding a cluster, you cannot remove another cluster or reduce the limit of another cluster; however while removing the cluster or reducing the limit of the cluster, you can add another cluster or increase limit of another secondary cluster.
- If you cancel removing the cluster or decreasing the limit, then the last updated limit remains the same and any data migrated to other clusters will not be migrated back to this cluster.
- While reduction of limit for one cluster is ongoing, you can increase the limit of another cluster but cannot decrease.

Figure 53: Setting Up Hard Limit

A new cluster is added to the object store. If any secondary cluster addition fails, you can remove that cluster. You can also see the usage of these clusters in the **Usage** tab. For more information, refer to Viewing Object Store Usage on page 214.

Note: It will take a minute to add a new cluster.

Scaling Out an Object Store

Scaling out an object store enables you to add more resources to an existing object store cluster. You can add a worker node, and optionally, add more storage in addition to the current usage. An additional 10 vCPUs and 32 GiB memory get added for each worker node.

Before you begin

- Make sure that you have at least a three-node cluster for performing scale-out.
- Make sure that physical resources are available.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 803

A non-admin user can scale out an object store only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions and the non-admin user must be assigned to specific objects instances:

- Scale-Out
- View Object Store

> **Note:** Administrators and non-admin users are Prism Central users with the following roles:
>
> - Administrator—A Super Admin or a Prism Admin in Prism Central.
> - Non-admin user—A Prism Central user without any administrator privileges.
>
> For more information about the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.

About this task

> **Note:**
>
> - Objects version lower than Objects 2.1 does not support scale-out. Upgrade Objects to the latest version to use the scale-out feature.
> - You can scale out one node or VM at a time.
> - During scale out of an object store, no disruption happens. You can launch the object store during scale-out.
> - If physical resources (VMs) are deployed, rollback is not supported. However, if the deployment of physical resources fails or if the deployment fails prior to deploying physical resources and your cluster is not scaling, you can roll back. For rolling back scale out of the object store, contact Nutanix Support at http://portal.nutanix.com.

You can perform compute scale out (adding worker nodes) and storage scale out (adding additional storage capacity) for an object store.

To scale out an object store, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 804

3. Click the **Object Stores** tab, and then from the object store table, select the object store that you want to scale out.

Figure 54: Object Store Selection for Scale Out

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 805

4. If you want to add a worker node (compute scale out), do the following:

   a. In the **Actions** list, click **Scale out**.
      The **Compute Scale Out** window appears.

   b. Click **Add Nodes**.

Figure 55: Compute Scale Out

The object store is now scaling out. This process takes about 5 to 10 minutes. You can track step by step deployment progress with scale out workflow progress for the object store.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 806

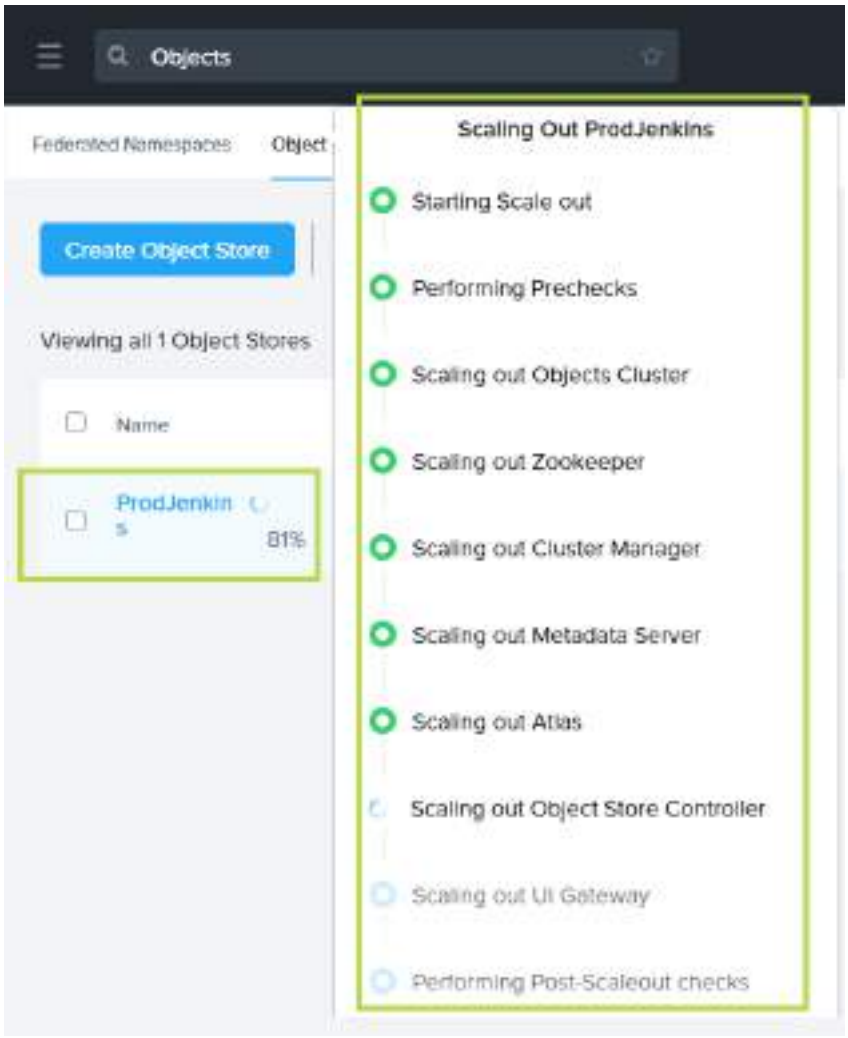


Figure 56: Object Store Scale Out Progress

Once the object store scale out is completed, new node is added to the object store. The object store takes an additional 10 vCPUs and 32 GiB of memory for the worker node.

5. If you want to add more storage to the current usage (storage scale out), do the following:

   a. In the **Actions** list, click **Set Additional Capacity**.
   The **Set Additional Capacity** page appears.

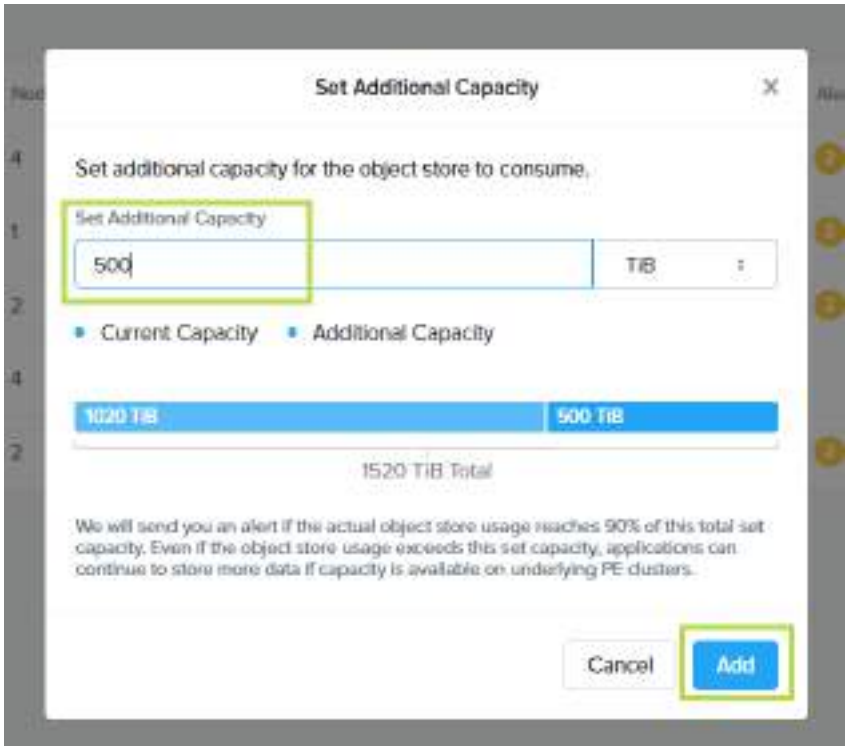


Figure 57: Storage Scale Out

   b. Enter the amount of additional storage you want to add to the current usage and click **Add** to complete.

> **Note:** Objects generates an alert if the logical usage of your object store reaches 90% of the specified value. For more information about alerts, refer to Viewing Alerts.

Managing FQDN and SSL Certificate

You can add multiple FQDNs, download the CA certificate, and set up or replace the SSL certificate for your object store.

A non-admin user can manage FQDN and SSL certificates only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions and the non-admin user must be assigned to specific objects instances:

- Regenerate Self Signed Certificate
- Replace Certificates
- Download Certificate
- View Object Store

> **Note:** Administrators and non-admin users are Prism Central users with the following roles:
>
> - Administrator—A Super Admin or a Prism Admin in Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 808

- Non-admin user—A Prism Central user without any administrator privileges.

For more information on the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.

Adding FQDNs

You can now create multiple FQDNs for an object store. The FQDN used while creating an object store is the default FQDN and rest of the FQDNs are alternate FQDNs.

About this task

To add a FQDN, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. Click the **Object Stores** tab, and then from the object stores table, select the object store for which you want to create a FQDN.
4. Click **Actions** > **Manage FQDNs and SSL Certificates**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 809

5. In the **New FQDN** field, type the FQDN and then click **+FQDN**.
   Guidelines for naming FQDN:

   - Must contain at least two dots.
   - Can contain either alphanumeric, hyphen, or underscore characters.
   - Cannot start or end with a hyphen or underscore or dot.
   - Duplicate domain name is not allowed.
   - A FQDN cannot be at a sub-domain of another FQDN.

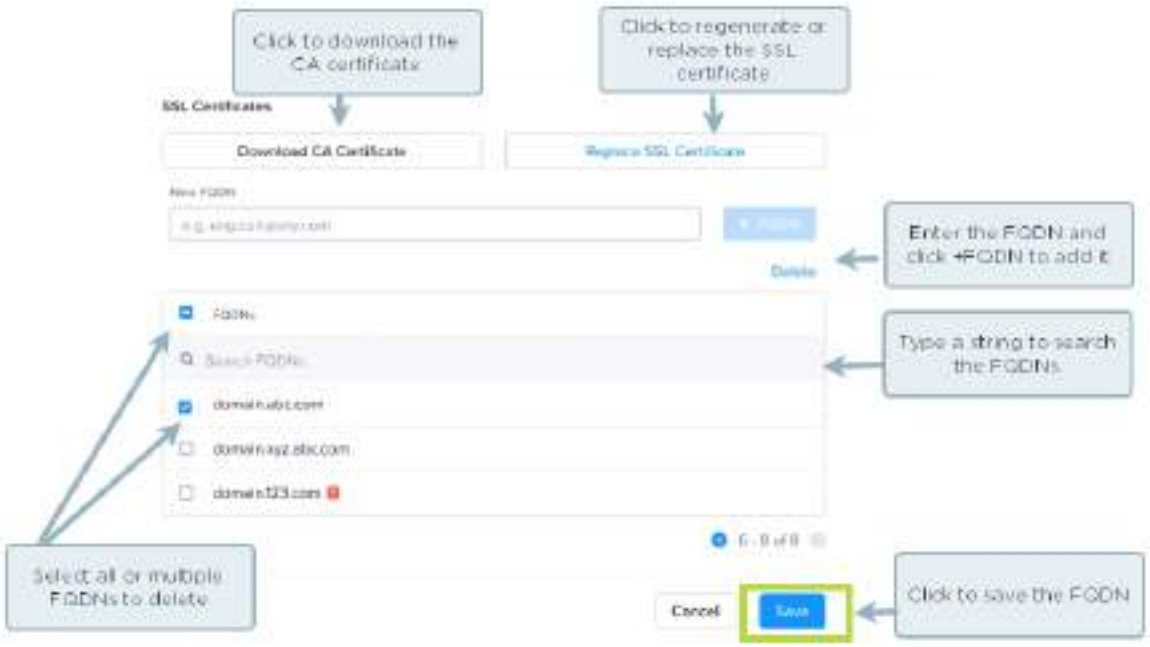


Figure 58: Adding FQDNs

You can select one or more FQDNs, and click **Delete** to delete the FQDNs. However, you cannot delete the default FQDN (the FQDN used while creating an object store).

The new FQDN is listed in the table.

> **Note:** A warning message is shown if the new FQDN is missing in the DNS configuration of the certificate. To add the FQDN to the certificate do either of the following:
>
> - Regenerate the SSL certificate to add all the newly added domains to the certificate.
> - Replace the SSL certificate by importing a CA-signed certificate. Make sure to add all the domains to that certificate.

6. Click **Save**.
   A confirmation dialog box appears to replace the SSL certificate.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 810

7. Click **Yes, Replace**.
   The new FQDN is added and the SSL certificate remains the same.

   Note: The object store will be unreachable for 2-3 minutes and you will not be able to perform any operations on that object store.

What to do next

You can also regenerate or replace the SSL certificate. Refer to Setting up SSL Certificate for an Object Store on page 96.

Setting up SSL Certificate for an Object Store

By default, self-signed Secure Socket Layer (SSL) certificates are generated. If you have strong security requirements, you can replace the default certificate for the object store to securely connect to the object store while you use the HTTPS protocol. You can replace the certificates either by regenerating a self-signed certificate or if you have a Certificate Authority (CA)-signed certificate, then you can import your private key and certificate files. When you replace the existing certificate, it removes the web browser certificate error warnings.

Before you begin

Ensure that you have met the following requirements:

- The private key should be RSA key type with key size 2048- or 4096-bit. Contents of the private key can be in PKCS#1 standard, unencrypted PKCS#8 standard, and PEM format.
- The provided public certificate must be signed by the provided CA.

  Note: If you want the server to return the server certificate and the chain of intermediate certificates, upload the server certificate and the chain of intermediate certificates as a public certificate in a single file.

- The public certificate must have the FQDN of the Object Store Service along with the wild card in either CN or SAN. For example, if the object store name is `objects-2021` and the domain is `companyname.com`, then the FQDN should be *objects-2021.companyname.com*. Then, the certificate must have **.objects-2021.companyname.com*, *objects-2021.companyname.com*.

About this task

To set the SSL certificate, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. Click the **Object Stores** tab, and then from the object stores table, select the object store for which you want to set the certificate.
4. Click **Actions** > **Manage FQDNs and SSL Certificates**.
5. Under SSL Certificates, click **Replace SSL Certificate**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 811

6. In the **Replace SSL Certificate** window, select one of the following:

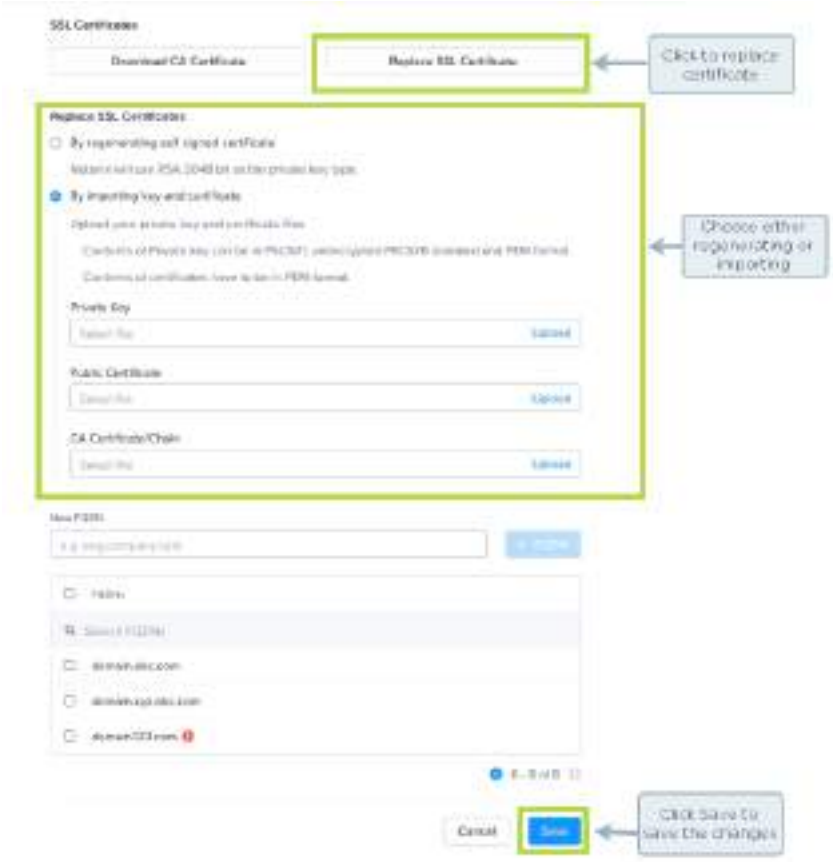


Figure 59: Replacing SSL Certificate

a. **By regenerating self signed certificate**: Uses RSA 2048 bit as the private key type.

A self-signed certificate is a certificate signed by the same entity that verifies the certificate.

a. **By importing key and certificate**: Upload your private key and certificate files.

- **Private Key**: Click **Upload** to upload the private key.

  This key is used to decrypt the message.

- **Public Certificate**: Click **Upload** to upload the public certificate.

  A public key certificate is an electronic document used to prove the ownership of a public key. The certificate includes information about the key, information about the identity of its owner (called the subject), and the digital signature of an entity that has verified the contents of the certificate (called the issuer).

- **CA Certificate/Chain**: Upload the CA certificate.

  A certificate chain is the certificate of a particular CA, plus the certificates of any higher CAs up through the root CA.

You can also add or delete the FQDNs while regenerating or replacing the SSL certificate. Refer to Adding FQDNs on page 94.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 812

7. Click **Save**.
   The default SSL certificate is replaced.

Deploying Object Store on Nutanix Cloud Cluster

Perform the tasks described in this section to get started with NC2 on Objects.

Before you begin

Ensure that you have registered for NC2 on AWS from the My Nutanix portal. See Getting Started with NC2 for more information.

About this task

To deploy an object store on Nutanix Cloud Cluster (NC2), do the following:

Procedure

1. Enable **Objects**.
   See Enabling Objects on page 14.
2. Create an object store using the IP addresses from the subnet created on the Prism Element web console. Select only the required number of IP addresses instead of using all 255.
3. Ensure that the name servers are configured correctly. Copy the name servers from the Prism Element web console and add them to the Prism Central web console.
4. Using the load balancer, log on to Prism Central.
5. You can get the IP address from the subnets created on Prism Element and deploy the **Object Store**.

   Note: You can provide any free IP address in the subnet.
6. Once the OSS deployment is successful, create a load balancer for the Objects endpoint IP address to access the Objects Browser.

Deploying Object Store at a Dark Site (Offline Deployment)

Dark site deployment is a process for deploying Objects at a site without Internet access.

Before you begin

Make sure you satisfy the deployment prerequisites before starting the deployment. Refer to Deployment Prerequisites - AHV and ESXi on page 40.

About this task

To deploy an object store in a dark site, do the following:

Procedure

1. Deploy Prism Central 2023.1.0.1 or later version.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 813

2. Check the Compatibility matrix to find the latest Objects Manager Version from the Support Portal.

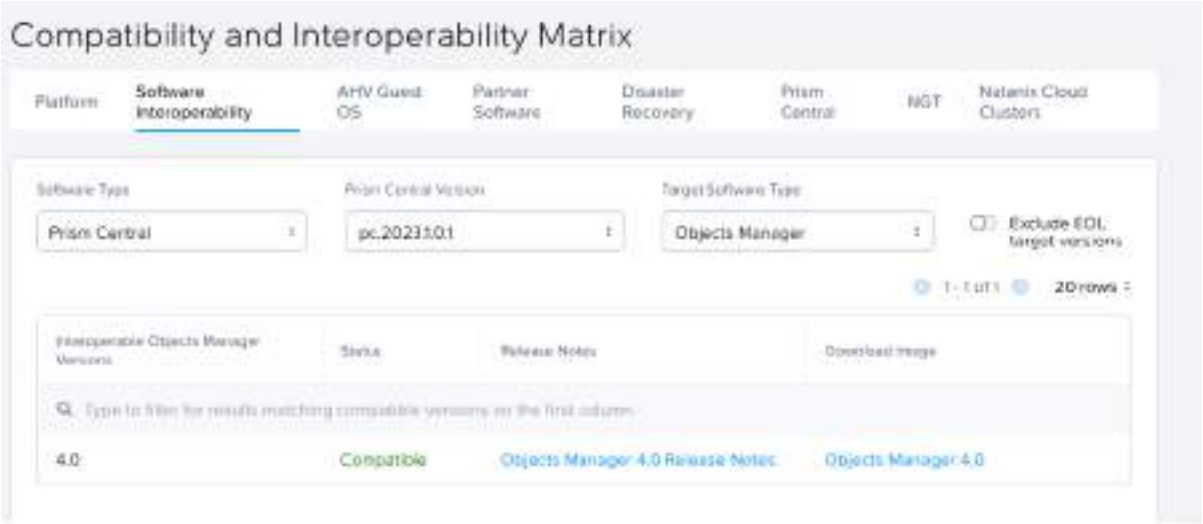


Figure 60: Compatibility Matrix: PC and Objects Manager

3. Download the latest **Objects LCM bundle** from the Support Portal.

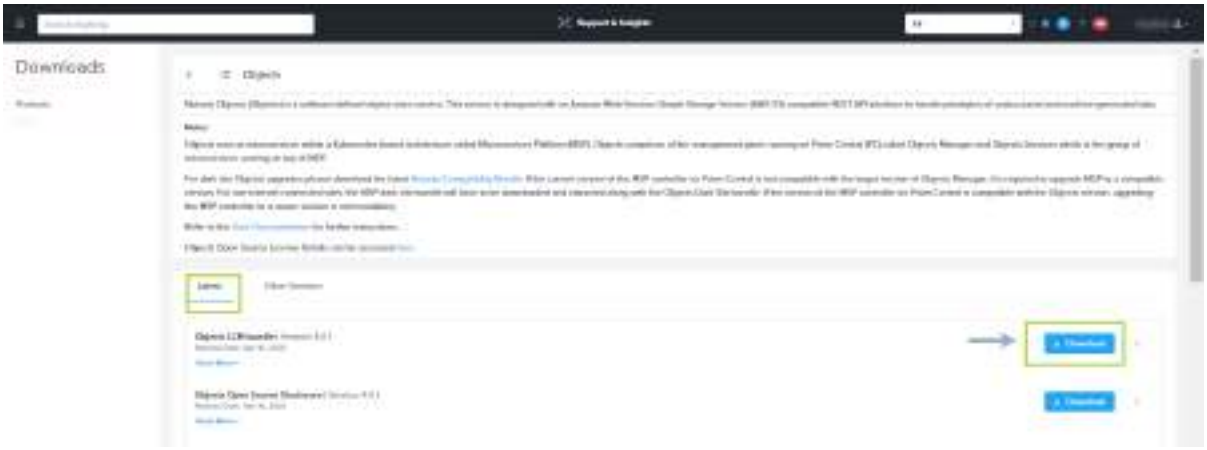


Figure 61: Download Objects LCM Bundle

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 814

4. Check the Compatibility Matrix to find the latest MSP version from the Support Portal.

Figure 62: Compatibility Matrix: Objects Manager and MSP Controller

5. Download the latest MSP dark site bundle from the Support Portal.

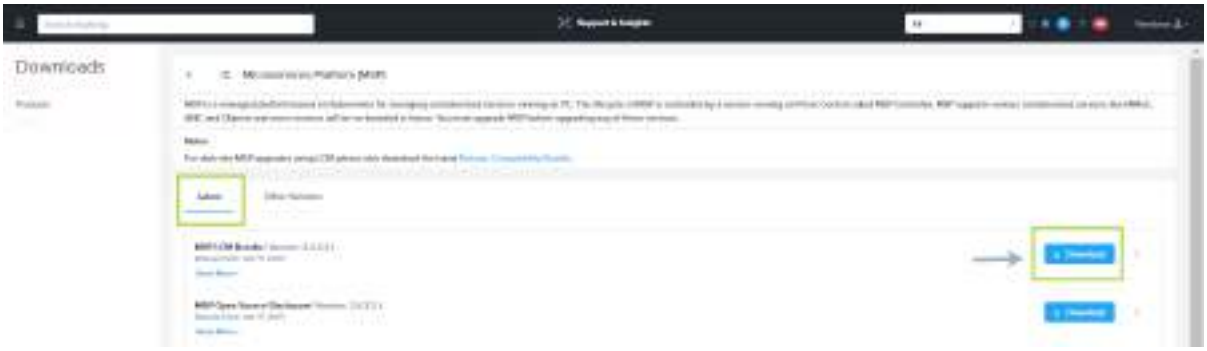


Figure 63: Download MSP LCM Bundle

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 815

6. Download the latest LCM Framework Bundle from the Support Portal.

Figure 64: Download LCM Framework Bundle

7. Set up the Dark Site web server, and copy the latest bundles for Objects, MSP, and LCM to the web server in the folder named `darksite`.

   To view example of setting up a web server, see the *Setting Up a Local Web Server* section in the LCM Dark Site Guide.

8. Run the following commands to untar all the three bundles within the same location (`darksite` folder).

```
tar -xvf lcm_dark_site_bundle_2.6.0.1.36249.tar.gz
```

```
tar -xvf lcm_darksite_msp-2.4.3.2.tar.gz
```

```
 tar -xvf objects-4.0.tar.gz
```

9. Login to the Prism Central and navigate to the **Admin Center** from the application switcher.

   a. Enable the Nutanix Marketplace.

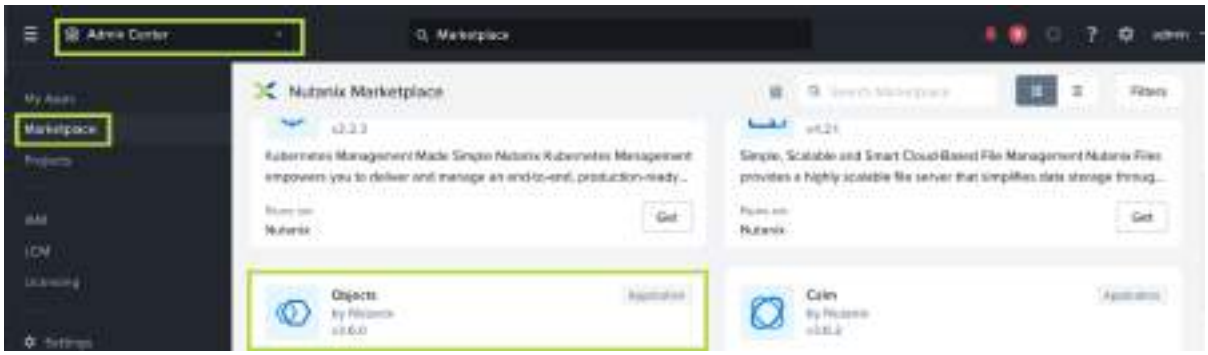


Figure 65: Nutanix Marketplace

   b. Get the Objects application.
   This step enables the Objects Service on the Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 816

10. Once the Objects Service is enabled, navigate to **Objects** from the Application Switcher.

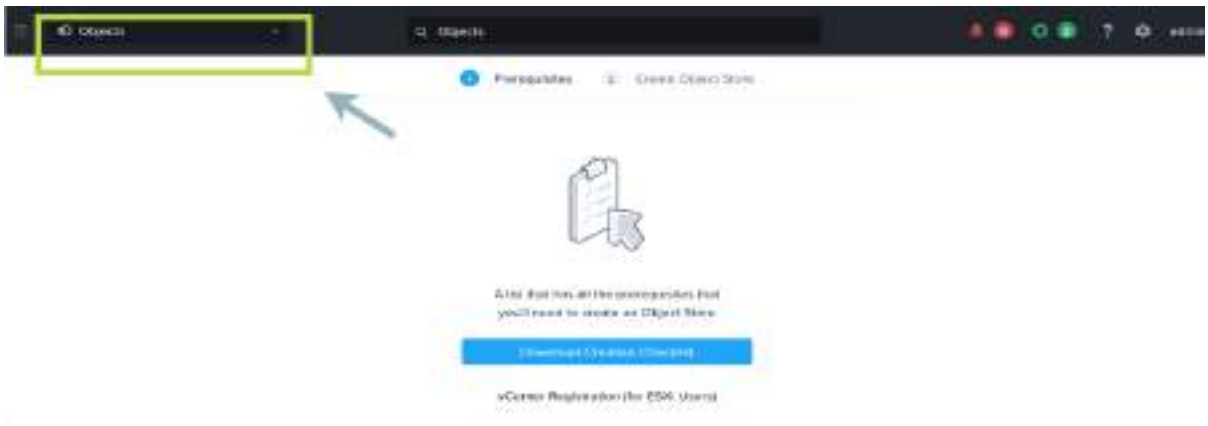


Figure 66: Objects Landing Page

The Objects landing page appears.

11. To configure the dark site server in LCM, do the following:

    a. Navigate to the **Admin Center** from the Application Switcher, and then click **LCM** > **Settings**.

    b. Under Source, select **Dark Site (Local Web Server)** from the drop down, and enter the web server URL from Step 8 where all dark site bundles are untarred .

    For example, `http://`*`IP address of the web server`*`/darksite/`

    `darksite` is the folder where all the bundles are untarred.

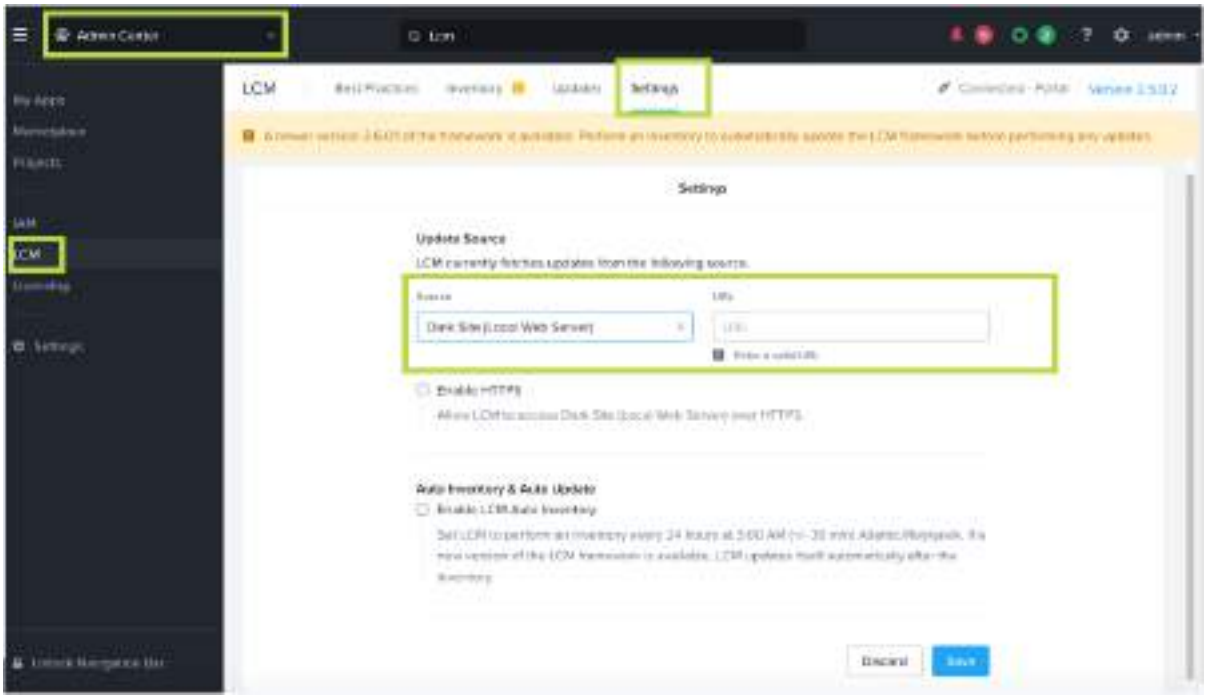


Figure 67: LCM Dark Site Settings

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 817

12. SSH to Prism Central and run the following command to check the AirGap enabled status:

```
nutanix@PCVM~$ mspctl controller airgap get
```

Figure 68: LCM Dark Site Settings

13. Login to the Prism Central UI and navigate to **LCM** > **Inventory**, and then click **Perform Inventory**.

14. Once LCM Inventory completes, upgrade to latest Objects Manager version should be available (if current Objects manager is not the latest).

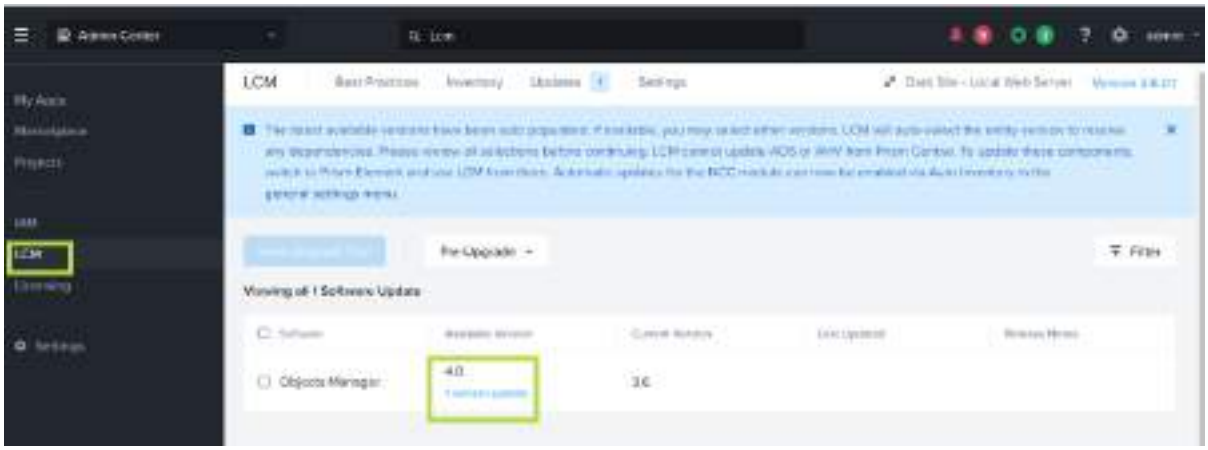


Figure 69: Objects Manager Upgrade

15. Select **Objects Manager**, and click **View Upgrade Plan**, and then click **Apply Updates**.
Once the Objects Manager is upgraded to the latest version, the setup is ready to start the Objects deployment.

16. SSH to Prism Central and run the following command to ensure MSP Controller version on Prism Central is same as shown in Step 4.

```
nutanix@PCVM~$ mspctl controller version
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 818

17. Go to the **Objects** app from the Application switcher, and then click **Create Object Store** to start the deployment.

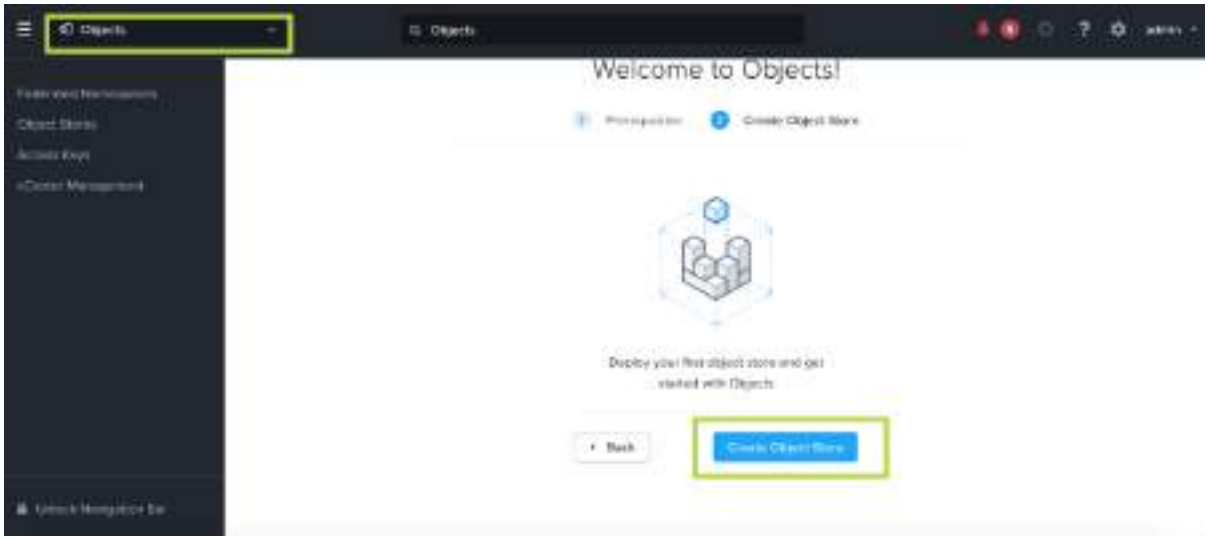


Figure 70: Create Object Store

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 819

TYPES OF OBJECTS USERS

There are two ways to manage Objects.

- **Prism Central**: Prism Central users can access Objects by using the Prism Central web console. These users can create user accounts and perform all the operations except any object-specific operations such as PUT, DELETE, copy, and list objects on any of the buckets (own or others). Prism Central users can also access a bucket by using the S3 APIs. These users can view buckets of all the API users, and can also share buckets of any API user with any other users.

  The following additional types of Prism Central users with varying access levels, as described below, can be defined using role-based access control (RBAC).

  - Objects-only admin - Admin user having access to only Objects service within Prism Central. Within Objects, you can create the following three different users:

    - Full access to Objects service (Objects only—full access)
    - Read-only access to Objects service (Objects only—view access)
    - Restricted access to Objects service (user can customize the access)

  - Prism Central admin role with no access to Objects service at all within Prism Central (No Objects access)

- **API**: S3 API users (IAM users) cannot access Objects by using the Prism Central web console. They access buckets and perform operations only by using the S3 APIs. This includes S3-compatible applications. The API users have unconditional access to their own buckets and limited or no access to buckets of other users based on the shared policy. S3 API users are added using the Objects GUI. For more information, see Generating Access Key for API Users on page 110.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 820

DIRECTORY CONFIGURATION AND ACCESS KEY GENERATION

You can configure the directory, add people, and generate access keys for the people. You can use these directories to search for people who can have access to the service. Only users with an access key can share buckets.

Objects IAM-High Availability Overview

IAM-High Availability (IAM-HA) feature is introduced to ensure the high availability of Objects IAM across data centers. It provides the ability to withstand Prism Central or primary data center failures. Earlier, Objects IAM was deployed only on the first Objects cluster, and the rest of the Objects clusters were dependent on it. IAM-HA ensures that each Objects cluster is operational on its own, without depending on the other Objects clusters. With IAM-HA, any new deployments will use IAMv2 (the same version of IAM as Prism Central).

Prerequisites

The following are the prerequisites for the IAM-HA feature to be enabled automatically:

- Prism Central version should be pc.2023.1.0.2 or later.
- MSP version should be MSP 2.4.3.4 or later.
- No object store (Objects cluster) should be present. Only new object store deployments will have IAM-HA enabled.

  Note: Once IAM-HA is enabled, any new deployments will use IAMv2.

- If existing object stores are present, you should delete all the object stores.

  Note: After you delete all the existing object stores, the IAM-HA feature gets automatically enabled.

- Make sure to open the additional ports needed for the IAM-HA feature. See Port Reference Guide.

Configuring Directories

If IAM-HA is disabled, then you can add directories that Objects can use to search for people who can have access to the service. You can also configure multiple Active Directory servers in the user interface and search across one or more Active Directories. If IAM-HA is enabled, you can only view directories. You cannot configure directories from the Objects UI. You can go to the directory configuration page on Prism Central to configure the directory.

Before you begin

A non-admin user can configure directories only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions:

- View Object Store
- Create an Object Store

  Note: Administrators and non-admin users are Prism Central users with the following roles:

  - Administrator—A Super Admin or a Prism Admin in Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 821

- Non-admin user—A Prism Central user without any administrator privileges.

For more information about the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.

About this task

To configure the directories, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. Click **Access Keys**.

Note:

- If IAM-HA is enabled, you can only view directories. You cannot configure directories from the Objects UI. You can go to the directory configuration page on Prism Central to configure the directory.
- Deletion of the directory is not allowed if a user has been created and access keys are present.

Figure 71: View Directories if IAM-HA is Enabled

4. Click **Configure Directories**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 822

5. Click **+ Add Directory**.

Figure 72: Directory Configuration If IAM-HA is Disabled

If you have already added the directory earlier, you will see a list of directories in this screen, and you can edit or remove the directory from the **Edit** or **Remove** link next to the directory name.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 823

6. In the **Add Directory** window, select any one of the following:

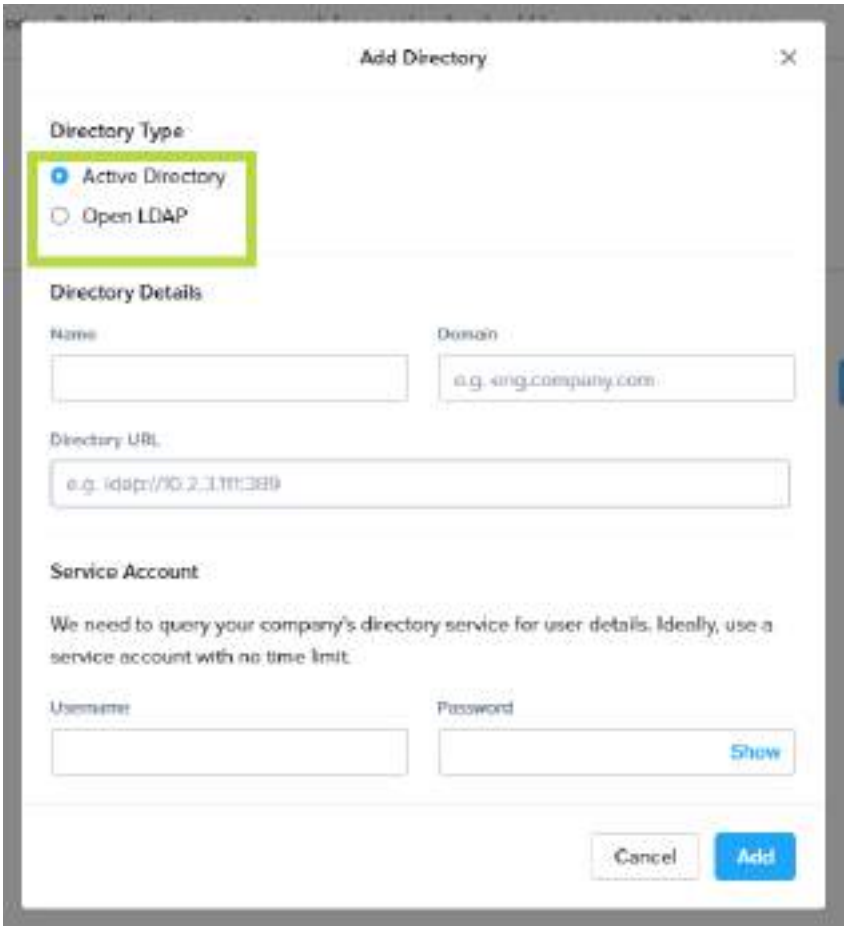


Figure 73: Add Directory Window

a. **Active Directory**: To add a directory through Active Directory, enter the following directory details and service account credentials:

- **Name**: Enter the name of the Active Directory server.
- **Domain**: Enter the domain that represents the top of the Active Directory tree and uses DNS to define its namespace.

  Usually, the domain is the DNS name of the company.
- **Directory URL**: Enter the Active Directory URL with the port to access the Active Directory server.

  For example, `ldap://10.2.3.111:389`
- **Username**: Enter the username for accessing the Active Directory server to retrieve the user details.
- **Password**: Enter the password for accessing the Active Directory server to retrieve the user details.

> **Note:** To access Objects, no expiry should be set on the Active Directory account.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 824

b. **LDAP**: To add a directory through Lightweight Directory Access Protocol (LDAP), enter the following directory details, user and group details hierarchy (or tree under which the user details for generating access keys have to be retrieved), and service account credentials:

- **Name**: Enter the name of the OpenLDAP server.
- **Domain**: Enter the domain that represents the top of the LDAP tree that uses DNS to define its namespace.

  Usually, the domain is the DNS name of the company.
- **Directory URL**: Enter the domain that represents the LDAP URL with port to access OpenLDAP server.

  For example, `ldap://10.2.3.111:389`
- **User Object Class**: Enter the LDAP object class value that defines users in the directory service. When the user is created, this list of user object classes is added to the attributes list of the user.
- **User Search Base**: Enter the location or the search starting point in the LDAP tree, which locates the users.

  For example, OU=people.
- **Username Attribute**: Enter the attribute names that are searched to retrieve users from the LDAP tree.
- **Group Object Class**: Enter the LDAP object class value that defines groups in the directory service to which the users belong.

  When the group is created, this list of group object classes is added to the attribute list of the user.
- **Group Search Base**: Represents the location or the search starting point in the LDAP tree under which groups are located.

  For example, OU=people
- **Group Member Attribute**: Enter the member attribute that specifies the group memberships.
- **Group Member Attribute Value**: Enter the group entries for which the memberships are specified by using the member attribute.

  These member attributes can have member attribute values specifying group membership in Distinguished Names (DNs). Member attribute values are used for group membership resolution.
- **Username**: Enter the username for accessing the openLDAP server to retrieve the user details.
- **Password**: Enter the password for accessing the openLDAP server to retrieve the user details.

> **Note:** To access Objects, no expiry should be set on the LDAP account.

What to do next

You can now generate an access key for the API users. Refer to Generating Access Key for API Users on page 110.

Generating Access Key for API Users

You can add people (users) from the directory or through email address, and generate access key for the users. Only users with access keys can share buckets.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 825

Before you begin

A non-admin user can generate access keys only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions:

- View Object Store
- Create an Object Store

> **Note:** Administrators and non-admin users are Prism Central users with the following roles:
>
> - Administrator—A Super Admin or a Prism Admin in Prism Central.
> - Non-admin user—A Prism Central user without any administrator privileges.
>
> For more information on the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.

About this task

To generate access keys for the users, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. Click **Access Keys**.
4. Click **+ Add People**.

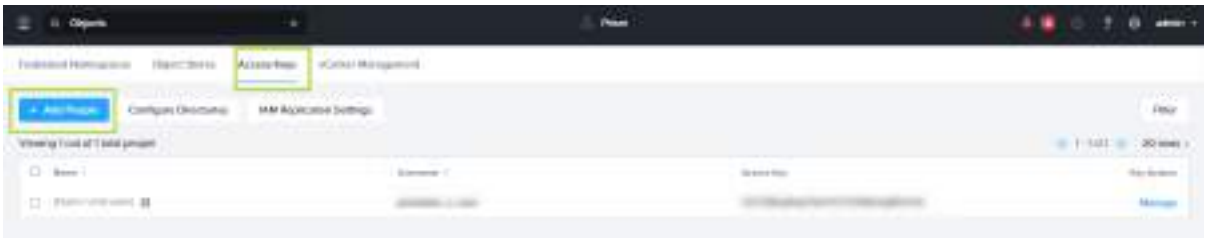


Figure 74: Adding People for Access Key Generation

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 826

5. In the **Add People** window, select any of the following options:

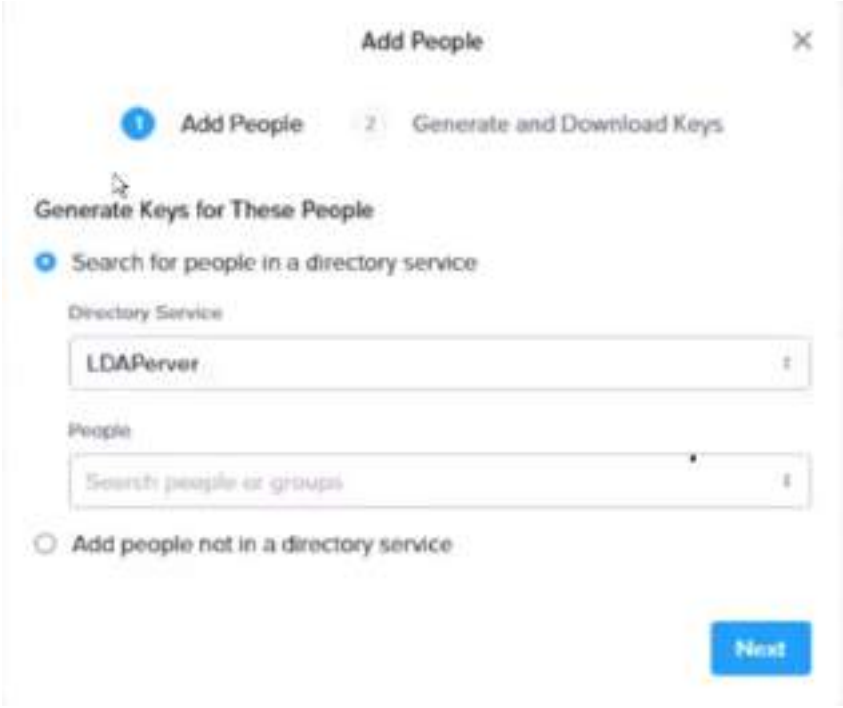


Figure 75: Add People Window: Search in Directory

a. **Search for people in a directory service**: Select to add people from the directory.
For more information about adding a directory, refer to Configuring Directories on page 106.

> **Note:** You can use the Active Directory (AD) group to generate key pairs. Objects IAM generates key pairs for each user as a separate file (inside a single zip file). The administrator can distribute these individual key pair files to the end users.

b. **Add people not in a directory service**: Add the email addresses of the people. Also, you can add a display name for the user.
Adding the display name is optional and can contain up to 255 characters.
Click **+Add** to add multiple users.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 827

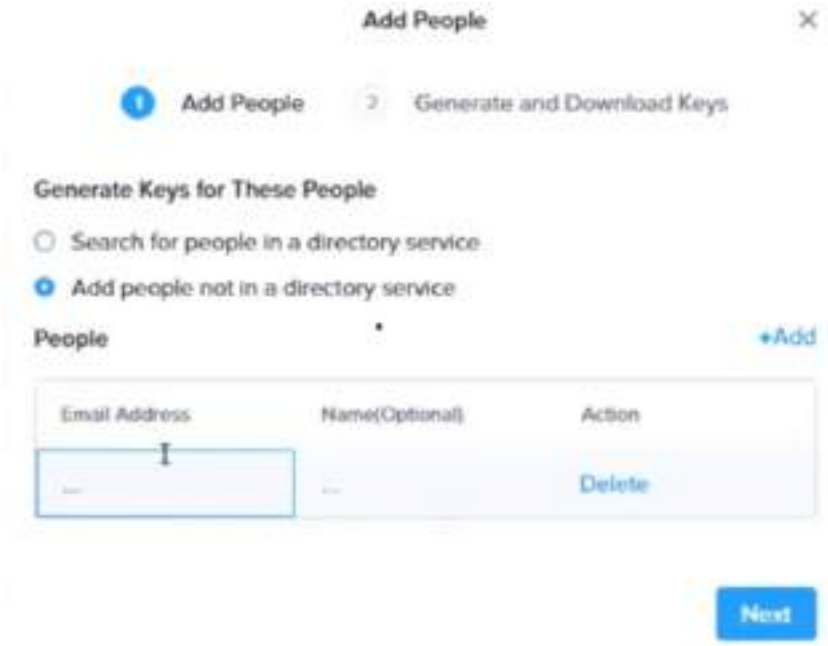


Figure 76: Add People Window: Enter Email Address

6. Click **Next** to open the **Generate and Download Keys** page.
   In this page, you generate and download the access keys. You can also add a tag to the access keys for key management.

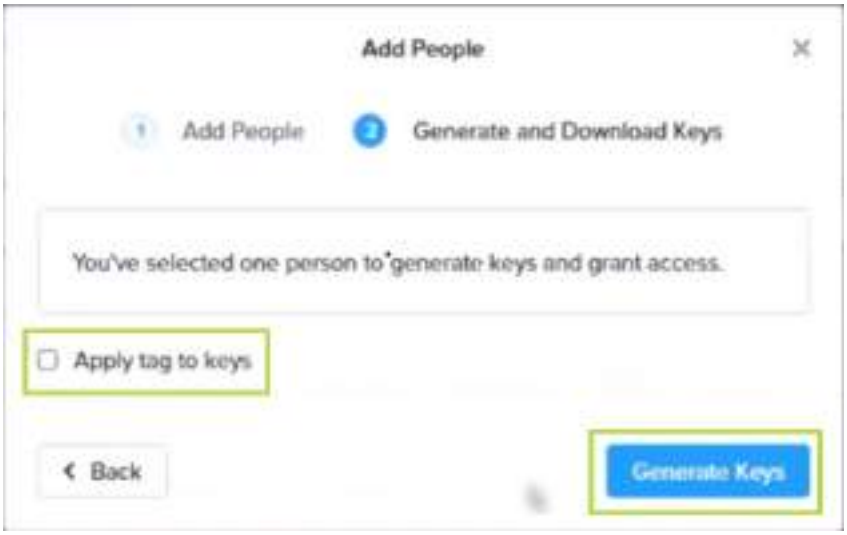


Figure 77: Generate and Download Keys Page

7. (Optional) Select **Apply tag to keys** check box and enter a tag name for the access keys.
   If you added multiple users, the same tag applies to all. The tags can contain up to 255 characters.

> **Note:** You cannot change the tag once added.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 828

8. Click **Generate Keys**.
   The keys are generated for the selected people.

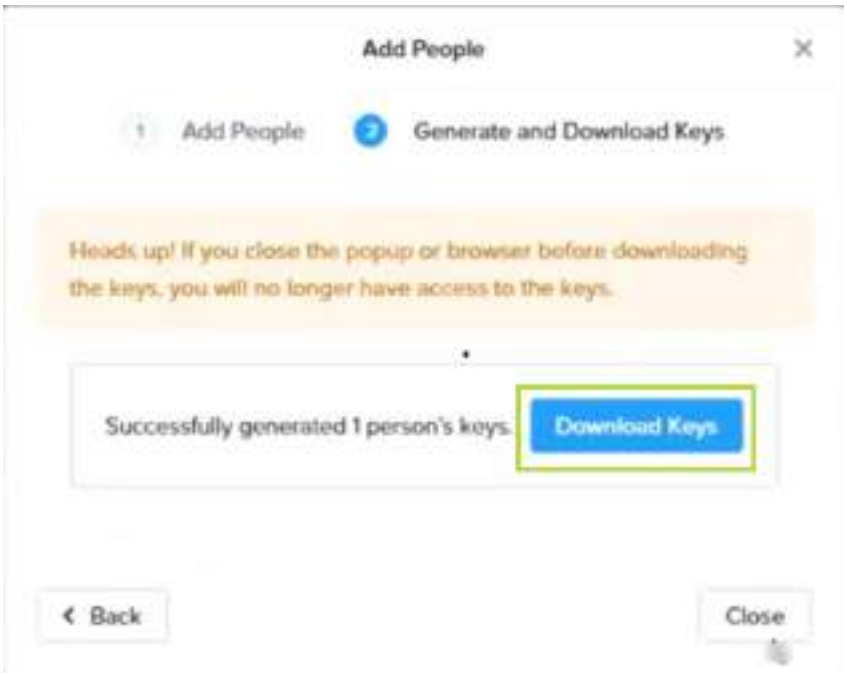


Figure 78: Generate and Download Keys Page

9. To download the keys, click **Download Keys**.
   The keys are downloaded.

> **Caution:** For Google Chrome, Microsoft Edge, and Internet Explorer, you can directly download the keys. For Safari and Firefox, after you click **Download keys**, a new tab opens listing the keys. You must copy and paste the keys at the desired location manually from the tab. You no longer have access to the keys after you close the tab.

Viewing API Users

You can view the list of people who can have access to Objects.

Before you begin

For a user with non-administrator privileges to view API users, the administrator must create an access control policy for the non-administrator user on a role that must have the minimum permission to View Object Store.

About this task

> **Note:** If the IAM-HA feature is enabled, the users with 0 access keys are not displayed on the **Access Keys** page.

To view the list of API users of Objects, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 829

3. Click **Access Keys**.

> **Note:** You can add keys for multiple users, but you cannot delete multiple users at the same time.

The table displays the list of API users.

Managing API Keys

If you lose or forget your access keys, you cannot retrieve the same key. However, you can add the key and get access. You can also delete a key.

Before you begin

A non-admin user can manage API keys only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions:

- View Object Store
- Create an Object Store

> **Note:** Administrators and non-admin users are Prism Central users with the following roles:
>
> - Administrator—A Super Admin or a Prism Admin in Prism Central.
> - Non-admin user—A Prism Central user without any administrator privileges.
>
> For more information on the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.

About this task

To add or delete the access keys, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. Click **Access Keys**.
   The table displays the list of API users.
4. Click **Manage** against a user.

Figure 79: Manage Keys Page

The **Manage Keys** page appears. This page provides you with the option to add or delete access keys.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 830

5. To manage a key, you can do one of the following:

   » **Add Key**: Click this button to generate the access key for the user.

   » **Apply tag to keys**: Select this option if you want to associate a tag with the access key.

   > **Note:** You can add one key at a time and up to five keys for a user.

   » **Delete**: Select the access key and click this button to delete the access key.

   The access key of the user gets deleted and has no access to the object.

   > **Note:**
   >
   > - You can delete one key at a time.
   > - If all keys for a user are deleted, then that user is not displayed on the **Access Keys** page. If you want to add a key to that user, see Generating Access Key for API Users on page 110.

Deleting API Users

This section describes the procedure to delete an API user.

Before you begin

A non-admin user can delete API users only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions:

- View Object Store
- Create an Object Store

> **Note:** Administrators and non-admin users are Prism Central users with the following roles:
>
> - Administrator—A Super Admin or a Prism Admin in Prism Central.
> - Non-admin user—A Prism Central user without any administrator privileges.
>
> For more information on the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.

About this task

> **Note:**
>
> - You cannot delete multiple API users at the same time.
> - A deleted user can work up to 3 hours after deletion.

To delete an API user, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 831

3. Click **Access Keys**.
   The table displays the list of API users.

4. Select the user you want to delete, and then click **Delete User**.
   The **Delete User** button appears at the top after you select a user.

Figure 80: Access Keys Page - Deleting an API User

The user is deleted.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 832

BUCKET CREATION, OPERATIONS, AND BUCKET POLICY CONFIGURATION

Before you can upload objects to a bucket, you must create a bucket in an object store. You can create a bucket using both S3 and NFS protocols. You can also configure a S3 bucket while creating it except applying the WORM policy.

A user with Edit Buckets permissions can perform all bucket operations, such as create, update, and delete on all the buckets on the assigned Object Store.

You can enable Lifecycle Policies, Versioning, WORM, Replication, Static Website, CORS, and Notifications to an S3 bucket. These S3 features cannot be enabled in a multi-protocol access bucket (NFS). However, you can also filter, update, share, and delete a bucket, and view all the existing buckets list created through both protocols.

Bucket Naming Conventions

The name of a bucket must conform to the following rules:

- Be a unique DNS-compliant name within a deployed bucket instance.
- Can contain alphanumeric, dot, or hyphen characters.
- Begin with a lowercase letter or a number.
- Cannot contain uppercase and special characters.
- Minimum of 3 and a maximum of 64 characters long.

> **Note:** You cannot change the bucket name after creating the bucket.

Creating and Configuring an S3 Bucket

You can create and configure the bucket settings. There are multiple options available for configuring a bucket and all are accessible at the time of creating a bucket. However, you cannot configure a WORM bucket while creating a bucket. You can edit WORM policies only after creating a bucket. You cannot enable multi-protocol access on the S3 bucket.

Before you begin

Ensure that the bucket names are unique for all the users.

A non-admin user can create and configure S3 buckets only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions and the non-admin user must be assigned to specific objects instances:

- Edit Buckets
- View Buckets
- View Object Store

> **Note:**

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 833

- Administrators and non-admin users are Prism Central users with the following roles:
  - Administrator—A Super Admin or a Prism Admin in Prism Central.
  - Non-admin user—A Prism Central user without any administrator privileges.

  For more information on the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.
- Users with Edit Bucket permission can perform a create bucket operation on the buckets available in the object stores that are assigned to the respective users.

About this task

Note: While creating a new versioned bucket, the system will automatically create a lifecycle policy to expire the delete markers if they are the only remaining object versions.

To create and configure a bucket, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the object store in which you want to create a bucket. The object store opens in a new window.
4. Click **Buckets** > **Create Bucket**.

Figure 81: Create Bucket Window

Note: You can also create a bucket without enabling versioning and life cycle policies.

5. On the **General Settings** section, type a name for your bucket and select a namespace.
   For more about namespace, refer to Federation Overview on page 61 .
   For more information about naming buckets, refer to Buckets Naming Conventions.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 834

6. (Optional) On the **Object Versions** section, configure the following:
   For more information about versions, refer to Object Versioning.

   a. **Enable Versioning**: Select this check box to enable versioning on objects and to keep all the versions on the same bucket.
      To apply the life cycle policy with versioning enabled, refer to Rules for Lifecycle Policy When Object Versioning is Enabled on page 129.

      Note: When you select versioning, you are able to recover objects from accidental deletion or overwriting.

7. (Optional) On the **Lifecycle Policies** section, select the following:
   For more information, refer to Lifecycle Policies.

   a. **Expire current objects version after:**: Select to type a time period after which the current version of the object expires.
      You can specify the number in days, months, or years.

   b. **Expire previous objects versions after**: Select this check box to enter a time period to delete all the previous versions of the objects. This option is available only if versioning is enabled.
      You can specify the number in days, months, or years.

      Note:

      - If versioning is not enabled, the current object deletes permanently. When you enable versioning, the current object becomes a past object.
      - Multi-protocol access cannot be enabled on the S3 bucket. If you want to create buckets with multi-protocol access, refer to Creating and Configuring an NFS Bucket on page 120.

8. Click **Save**.
   The bucket is created successfully.

What to do next

After creating a bucket, you can perform object operations from the Objects Browser or the S3 APIs. For more information, refer to Object CRUD Operations on page 179 and Supported S3 APIs section. You can also configure object-tiering lifecycle rules. For more information, refer to Creating a Lifecycle Rule on page 134 section.

Creating and Configuring an NFS Bucket

You can create and configure the bucket with multi-protocol access. If you are enabling multi-protocol access on a bucket, S3 features such as Lifecycle Policies, Versioning, WORM, Replication, Static Website, CORS, and Notifications cannot be enabled on that bucket. You can perform update (only multi-protocol access configurations), delete, or share operations on these buckets.

Before you begin

Make sure you are aware of the uses cases, recommendations, NFS-S3 interoperability, and limitations of NFS on Objects. Refer to Use Cases and Recommendations for NFS on Objects on page 8, NFS-S3 Interoperability on page 8 and Limitations of NFS on page 59.

A non-admin user can create and configure NFS buckets only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions and the non-admin user must be assigned to specific objects instances:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 835

- Edit Buckets
- View Buckets
- View Object Store

Note:

- Administrators and non-admin users are Prism Central users with the following roles:
  - Administrator—A Super Admin or a Prism Admin in Prism Central.
  - Non-admin user—A Prism Central user without any administrator privileges.

  For more information on the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.
- Users with Edit Bucket permission can perform a create bucket operation on the buckets available in the object stores that are assigned to the respective users.

About this task

Note:

- If you deployed object store prior to Objects 3.3 version, then you will not get the option to enable NFS for the bucket of that object store. Similarly, if you upgrade to later versions of Objects, then the option to enable NFS will not be available.
- Ensure that the bucket names are unique for all users.
- As the Objects-NFS does not support NLM (Network Lock Manager), no lock option is required while mounting the NFS bucket.
- The total and available bytes returned in the FSSTAT response denote the logical capacity and logical available space and not the physical capacity of the cluster which also takes RF2 into consideration.

To create and configure a bucket with multi-protocol access, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the object store in which you want to create a bucket. The object store opens in a new window.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 836

4. Click **Buckets** > **Create Bucket**.

Figure 82: Create Bucket Window

5. On the **General Settings** section, type a name for your bucket and select a namespace.
   For more about the namespace, refer to Federation Overview on page 61.
   For more information about naming buckets, refer to Buckets Naming Conventions.

   Note: Versioning and lifecycle policies cannot be enabled on buckets with multi-protocol access.

   To create and configure buckets for S3 features, refer to Creating and Configuring an S3 Bucket on page 118

6. On the **Multiprotocol Access** section, select **Enable NFS v3 Access**.

   Note: Access cannot be enabled or disabled after the bucket is created.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 837

7. For owner and default permissions for S3 written objects, do the following.

   Note: For files written using NFS protocol, these settings are inherited from the client.

   a. In the **Owner** section, enter the **UID** and **GID**.

      Any object (file or directory) created from S3 protocol have UserID (UID) and GroupID (GID) in the NFS namespace.

   b. In the **Default Access Permissions** section, by default read, write, and execute permissions are set for the files and directories for the owner, group (other users in a group), and others (users that are not part of any group).

      The following are the default permissions for files:

      - **Owner**: Read, Write
      - **Group**: Read
      - **Others**: Read

      The following are the default permissions for directories:

      - **Owner**: Read, Write, Execute
      - **Group**: Read, Execute
      - **Others**: Read, Execute

      You can change these permissions as needed.

8. In the **Advanced Settings** section, select any one of the following squash options.

   » **None**: Select this option if you do not want to convert the UID and GID of the users on the server.

   » **Root Squash**: Select this option if the user has root privileges and you want to convert the UID and GID to an anonymous UID and GID on the server. The anonymous UID and GID are automatically generated, however, you can change it.

   » **All Squash**: Select this option if you want to map all users to a single identity. This will convert the UID and GID of all users to an anonymous UID and GID on the server.

9. Click **Create**.
   The bucket is created successfully.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 838

10. **Note:** Before mounting a bucket, add the client to the NFS allowlist. Only the client present in the NFS allowlist will be given access to the NFS buckets.

    For more information on adding and managing clients to NFS allowlist, refer to Managing NFS Allowlist on page 124.

    Mount the bucket from the client VM.

    ```
    $ sudo mount -tnfs -o nfsvers=3,proto=tcp,soft -v objectstore-endpoint-ip-address:/bucketname path/to/mount
    ```

    Here *objectstore-endpoint-ip-address* is the Objects Public IP address which is used to send any S3 request. You can find this Public IP address in the Object Store table. See Viewing Object Store Deployments on page 78. *bucketname* is the name of the bucket.

    For example,

    ```
    $ sudo mount -tnfs -o nfsvers=3,proto=tcp,soft -v 10.45.53.75:/test-nfs-bucket home/folder-1/mnt-point
    ```

    The bucket is mounted successfully.

What to do next

After creating a bucket, you create directories, files, and symbolic links from the NFS namespace. You can also perform object operations from the Objects Browser or the S3 APIs. For more information, refer to Object CRUD Operations on page 179 and Supported S3 APIs sections.

Managing NFS Allowlist

You need to add the IP addresses of the client VMs that are allowed to access an NFS bucket in an object store.

About this task

Note: Make sure that you add the required client IP addresses to the allowed list before you mount a bucket.

To add clients to the NFS, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the object store in which the bucket exists.
   The object store opens in a new window.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 839

4. Click **Settings** > **NFS Clients Allowlist** , and then click **Add Client**.
   The **Add NFS Clients** window appears.

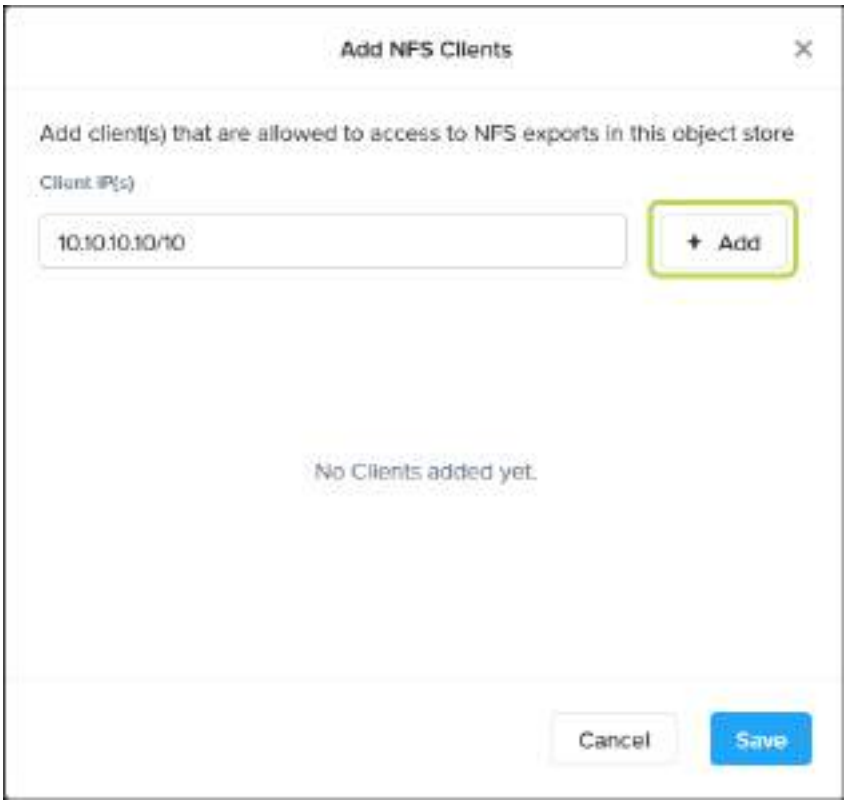


Figure 83: Add NFS Clients

   a. Enter the IP address of the client VM in Classless Inter-Domain Routing (CIDR) format and click **Add**.

   b. Click **Save**.
   The newly added IP address is listed in the **Added Clients** list.

> **Note:** The **Add** button appears only when you add the first IP address to the allowlist. To add more clients or to manage the existing clients, click **Manage Clients**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 840

5. Click **Manage Clients** to add or remove the clients.
   The **Manage NFS Clients** window appears.

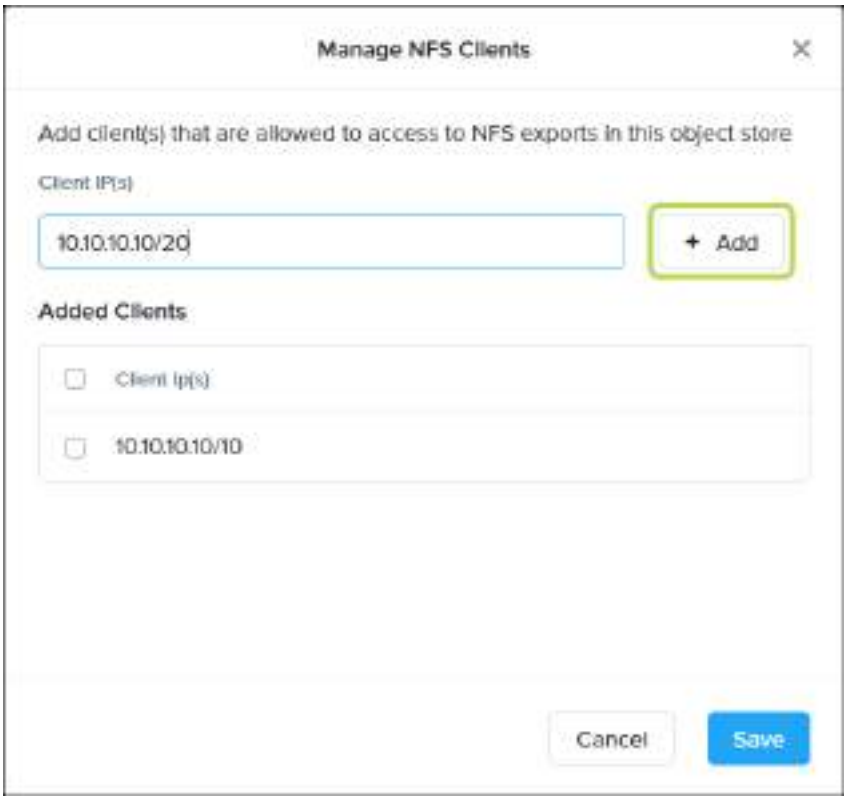


Figure 84: Manage NFS Clients

   a. (Optional) Enter the IP address of the client VM in Classless Inter-Domain Routing (CIDR) format and click **Add** to add client.

   b. (Optional) Select one or more IP addresses from **Client IP(s)** and click **Remove** to remove the clients.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 841

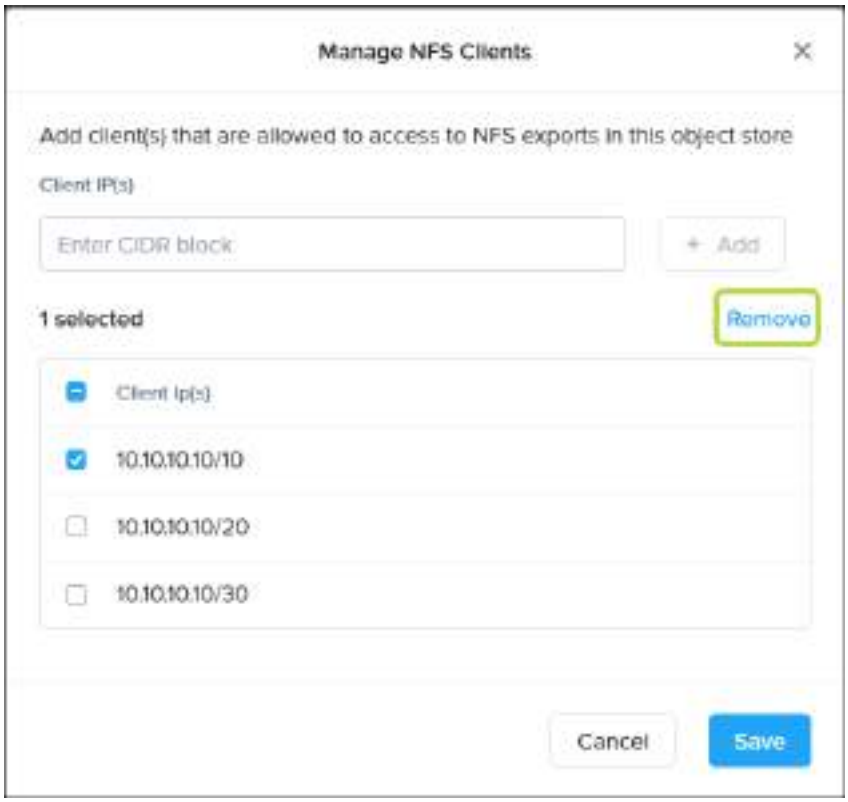


Figure 85: Manage NFS Clients

c. Click **Save**.
The IP address is removed from the **Added Clients** list.

What to do next

After adding the required clients to the NFS allowlist, you can mount the buckets and then perform tasks, such as creating files, directories, or symbolic links. For mounting the bucket, refer to Creating and Configuring an NFS Bucket on page 120.

Bucket Policy Configuration

You can configure multiple policies in a bucket such as object versioning, lifecycle policies, WORM, static website hosting and Cross-Origin Resource Sharing (CORS). Object versioning and lifecycle policies are accessible at the time of creating a bucket, however, you can apply WORM policy only after creating a bucket.

Note: Lifecycle Policies, Versioning, WORM, Replication, Static Website, CORS, and Notifications cannot be enabled for buckets created using NFS protocol.

Object Versioning

Object versioning enables you to keep multiple versions of an object in one bucket. By default, versioning is disabled for a new bucket. You can enable versioning while creating a bucket or editing a bucket. Refer to Creating and Configuring an S3 Bucket on page 118.

With the object versioning option, you can enable versioning on objects of that particular bucket. Object versioning varies depending on the lifecycle policies applied to the object.

For more information about the lifecycle rules for object versioning, refer to Rules for lifecycle policy.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 842

Note:

- Versioning cannot be enabled for the buckets created using the NFS protocol.
- For a versioned bucket, the number of objects shown for each bucket is indicative of the number of versions of all the objects present in the bucket.
- You cannot disable but can suspend the object versioning at any time.

When you suspend versioning, the accumulation of the new object versions is stopped and previous object versions are retained.

A non-admin user can enable versions on objects only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions and the non-admin user must be assigned to specific objects instances:

- Edit Buckets
- View Buckets
- View Object Store

Note:

- Administrators and non-admin users are Prism Central users with the following roles:
  - Administrator—A Super Admin or a Prism Admin in Prism Central.
  - Non-admin user—A Prism Central user without any administrator privileges.

  For more information about the built-in roles in Prism Central, see *Built-in Role Management* in the *Security Guide*.
- Users with Edit Bucket permission can perform object versioning on the buckets available in the object stores that are assigned to the respective users.

Lifecycle Policies

Lifecycle policy enables you to create or update a set of rules that define actions that Nutanix Objects applies to a group of objects. With these policies, you can expire objects when no longer required or move them to a low-cost storage tier to preserve for a longer-term.

A non-admin user can create lifecycle policies only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions and the non-admin user must be assigned to specific objects instances:

- Edit Buckets
- View Buckets
- View Object Store

Note:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 843

- Administrators and non-admin users are Prism Central users with the following roles:
  - Administrator—A Super Admin or a Prism Admin in Prism Central.
  - Non-admin user—A Prism Central user without any administrator privileges.

  For more information on the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.
- Users with Edit Bucket permission can apply lifecycle policies on the buckets available in the object stores that are assigned to the respective users.
- Lifecycle policies cannot be applied for the buckets created using NFS protocol.
- Rules or any updates to the rules get applied to the new objects that you create and will not apply to the objects existing before the rule creation or update.

You can apply these policies while creating a bucket. You can create multiple rules within a lifecycle policy. This means that different objects within the bucket can have different rules based on prefixes and tags.

Example: You can create rule 1 to expire the current versions of the objects with the tag value as a `dev`. Similarly, you can create multiple rules with different tiering and expiring configurations and apply them to other objects using prefixes and tags.

With lifecycle policies, you can configure a lifecycle policy rule to:

- Automatically delete objects after a specified number of days or months or years from the date of object creation.
- Tier objects to an S3-compatible object storage bucket after a specified number of days or months, or years from the date of tiering rule creation.
- Expire the current version and previous versions of an object independently. This means that you can set different expiration durations for the current version and the previous versions.
- Expire the incomplete multi-part uploads of an object.
- Apply to all objects or a subset of objects based on prefixes, tags, or both.

For example, if you want to store log files or business transaction records for a fixed period and after that period, you want to delete them.

Note: You cannot recover the objects once it is deleted.

To create or update a lifecycle rule, refer to Creating a Lifecycle Rule on page 134.

Rules for Lifecycle Policy When Object Versioning is Enabled

Following are the rules for the lifecycle policy when you enable object versioning:

- If you apply lifecycle policy **Expire current objects after # days/months/years** on an object with versioning enabled, it deletes the current version of the objects after the specified time, and does not delete any past versions of the objects.
- If you apply lifecycle policy **Expire previous objects versions after # days/months/years** on an object with versioning enabled, it deletes all the past versions after the specified time. This specified time gets calculated from the day the object version becomes non-current or past. This operation does not delete the current version.

  Note: This policy cannot be configured on a bucket with suspended versioning.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 844

- If you apply both the lifecycle policies **Expire current objects after # days/months/years** and **Expire previous objects versions after # days/months/years** on an object with versioning enabled, it deletes all the past versions based on the time specified in **Expire previous objects versions after # days/months/years**, and the current version expires based on the time specified in **Expire current objects after # days/months/years**.
- If you apply the lifecycle policy **Expire or Abort incomplete multipart uploads after # days/months/years** on an object, it deletes the parts associated with the multipart uploads after the specified time.
- If you apply any lifecycle policy to a WORM bucket with versioning enabled, the lifecycle policy is not applicable until the WORM retention period has elapsed.
- While creating a new versioned bucket, the system will automatically create a lifecycle policy to expire the delete markers if they are the only remaining object versions.

Cloud Tiering

Cloud tiering enables you to move objects to another S3-compatible object store bucket for saving storage space in the Nutanix Objects cluster. Tiering can help you to save costs by sending the infrequently accessed objects to platforms such as AWS S3, Microsoft Azure Blob Storage, and Google Cloud Platform (GCP). The supported endpoints are AWS S3, Azure Blob Storage, Google Cloud Platform (GCP) and a different Objects instance.

A non-admin user can configure a tiering endpoint only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions and the non-admin user must be assigned to specific objects instances:

- Create Endpoint
- Update Endpoint
- View Endpoint
- View Object Store

> **Note:** Administrators and non-admin users are Prism Central users with the following roles:
>
> - Administrator—A Super Admin or a Prism Admin in Prism Central.
> - Non-admin user—A Prism Central user without any administrator privileges.
>
> For more information about the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.

Cloud tiering is managed through lifecycle policies. You can configure multiple lifecycle rules for different objects within a bucket.

Cloud tiering configuration consists of the following steps:

- **Step 1: Configure a remote endpoint in the object store**

  You can configure remote endpoints using the **Tiering Endpoints** page in the object store instance. The objects within the bucket get moved to the endpoint according to the rules you configure.

- **Step 2: Create lifecycle rules for a bucket**

  You can create a tiering rule for a bucket where you define the scope (all objects or a subset of objects), select the remote endpoint, and specify the details for the rule.

Points to Note

Before you start with object tiering, note the following points:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 845

- It is strongly recommended that
  - Only encrypted data is stored on buckets for which tiering to the cloud is enabled.
  - Object store admins enable audit trails for the S3 bucket or other storage endpoints to ensure data is not being accessed or tampered with external malicious entities and that all access is only coming from the object store instance.
  - Admins follow recommended security best practices of AWS or other storage endpoints while setting up buckets for tiering.
- Tiering lifecycle policies are non-retroactive. The policy gets applied to the new objects that you create. The policy will not apply to existing objects.
- Tiering lifecycle policies get applied to both versioned and non-versioned objects in the same way. A separate non-current version transition action in lifecycle policies is not supported.
- Do not perform write operations on the configured-endpoint bucket. Ensure that the endpoint bucket gets used only for the object store instance.
- Removing a configured endpoint in the object store instance is not supported.
- There is a N:N relationship between the source bucket and the configured endpoint bucket. You can create multiple tiering-lifecycle rules for different objects within a bucket and use a separate endpoint for each tiering rule. Also, an endpoint bucket can be a destination to many Object Store buckets.
- Objects within a WORM-enabled bucket will continue to adhere to their WORM property even after getting tiered out to the endpoint bucket.
- Only the object data gets tiered to the endpoint bucket. The metadata of the object is not tiered.
- The behavior to access tiered objects using the `Object Get` method remains the same. If you send a request to retrieve an object from the Object store and the object is already tiered out, the Object store fetches the data from the endpoint bucket and fulfills your request.
- Users with **Edit Bucket** permission can create lifecycle rules bucket operation on the buckets available in the Object stores that are assigned to the respective users.
- Tiered objects are not readable on the tiering endpoint as they are moved in an unstructured form, without metadata.
- You can check if the objects are being tiered on the source Bucket **Summary** > **Tiering**. Also tiering endpoint bucket will grow in size and show data blocks.
- Once the specified time period has elapsed, an object becomes eligible for tiering out. However, it is important to note that the actual movement of the object may occur up to one day later.
- When reading a tiered object, the Objects cluster retrieves the object data from the tiering endpoint cluster and presents it to the client, without storing it locally that is no caching is performed.

Configuring a Tiering Endpoint

The infrequently used objects are moved to the configured endpoints according to the configured lifecycle rule for tiering. The supported endpoints are AWS S3, Microsoft Azure Blob Storage, Google Cloud Platform (GCP), and a different Objects instance.

About this task

Note:

- Cloud tiering supports GCP endpoint as *Other S3 compatible* endpoint type.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 846

- For tiering the objects to GCP, you need to create a bucket in GCP with the following default configurations. This bucket will be used as the tiering endpoint.
  - **Location type**: Multi-region
  - **Default storage class**: Standard
  - **Public access prevention**: Off
  - **Access control**: Uniform
  - **Protection tools**: None
- Ensure that the tiering endpoint has a Certificate Authority (CA) signed certificate. Note that self-signed certificates are not supported.

To configure a tiering endpoint, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the object store to configure tiering endpoint.
   The object store opens in a new window.
4. Click **Settings** > **Tiering Endpoint**.
5. To open the **Add Endpoint** page, click **Create**.

   If no endpoints are configured, the **Add** button appears in the center of the page. Click **Add** to start an endpoint configuration.

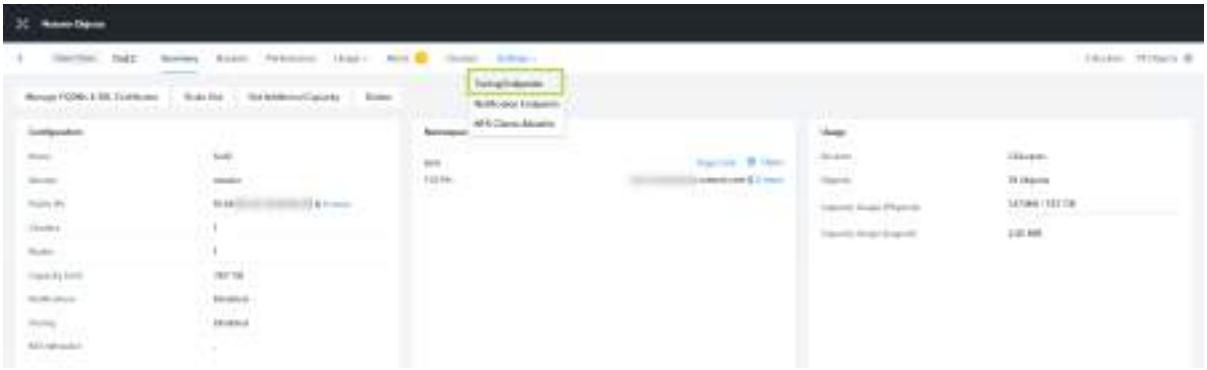


Figure 86: Tiering Endpoint Page

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 847

6. (Only for Nutanix Objects as the endpoint) Enter the following details:

   a. **Name**: Enter a name that identifies your tiering endpoint.

   b. **Endpoint Type**: Select Nutanix Objects as the endpoint type from the pull-down list.

   c. **Service Host**: Enter the complete URL of the endpoint that you want to use for tiering the objects. For example, the Objects public IP address or the domain name of an Object store instance.

      Example of a Nutanix Objects endpoint: `example.buckets.company.com`.

   d. **Bucket Name**: Enter the name of the bucket within the service host to which you want the objects to tier out.

   e. **Access Key**: Enter the access key of the bucket owner.

   f. **Secret Key**: Enter the secret key of the bucket owner.

   g. **Skip SSL Certificate Validation**: Select this check box to skip SSL certificate validation.

7. (Only for Other S3 Compatible as the endpoint) Enter the following details:

   a. **Name**: Enter a name that identifies your tiering endpoint.

   b. **Endpoint Type**: Select Other S3 Compatible as the endpoint type from the pull-down list.

   c. **Service Host**: Enter the complete URL of the endpoint that you want to use for tiering the objects.

      The AWS S3 URL format is `s3.`*`region`*`.amazonaws.com`

      Example of an AWS S3 endpoint: `s3.us-east-1.amazonaws.com`.

   d. **Bucket Name**: Enter the name of the bucket within the service host to which you want the objects to tier out.

   e. **Access Key**: Enter the access key of the bucket owner.

   f. **Secret Key**: Enter the secret key of the bucket owner.

8. (Only for Azure Blob Storage as the endpoint) Enter the following details:

   a. **Name**: Enter a name that identifies your tiering endpoint.

   b. **Endpoint Type**: Select Azure Blob Storage as the endpoint type from the pull-down list.

   c. **Container Name**: Enter the name of the container within the service host to which you want the objects to tier out.

   d. **Account Name**: Enter the Azure account name where the containers are located.

   e. **Secret Key**: Enter the secret key of the container owner.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 848

9. Click **Save** to complete configuring the endpoint.

   You can also update the access and secret keys of the bucket for the configured endpoints. For example, if the bucket owner generates new access and secret keys, the owner can update the configured endpoint with the new keys using the **Update** option.

Figure 87: Updating Tiering Endpoint

   Select the endpoint and click **Update** to open the **Update Endpoint** page. Update the required fields and click **Save** to complete the workflow.

What to do next

After you configure an endpoint, create lifecycle rules for tiering objects within your bucket. Refer to Creating a Lifecycle Rule on page 134.

Creating a Lifecycle Rule

You can create a lifecycle rule for a bucket where you define the scope (all objects or a subset of objects), select the remote endpoint, and specify the details for the rule.

Before you begin

Make sure to configure a tiering endpoint before creating object-tiering lifecycle rules.

A non-admin user can create lifecycle rules for a bucket in cloud tiering only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions and the non-admin user must be assigned to specific objects instances:

- Edit Buckets
- View Buckets
- View Endpoint
- View Object Store

Note:

- Administrators and non-admin users are Prism Central users with the following roles:
  - Administrator—A Super Admin or a Prism Admin in Prism Central.
  - Non-admin user—A Prism Central user without any administrator privileges.

  For more information about the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 849

About this task

When creating a bucket, you can enable versioning, set a rule to delete past versions, and add a lifecycle policy to expire the current objects after the specified time. Once the bucket gets created, you can go to the bucket page and configure object-tiering lifecycle rules.

To create a lifecycle rule to tier out objects, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the object store that contains the bucket where you want to create tiering rules.
   The object store opens in a new window.
4. Click the **Buckets** tab.
5. In the **Buckets** table, click the bucket that you want to tier out.
   The **Bucket** page appears.
6. Click the **Lifecycle** tab.
   You can view the rules that you defined while creating the bucket.
7. Click **Create Rule** to open the **Create Rule** page.
   You can also import lifecycle rule by clicking **Create Rule** > **Import XML**. Type or copy the lifecycle rule in XML format.
8. In the **Scope** page, do the following, and then click **Next**:
   a. In the **Name** box, enter a name that identifies the rule you are creating.
   b. In the **Scope** list, select **All objects** or **Tags/Prefix**.
      - Select **All objects** to apply the tiering rule to all the objects within the bucket.
      - Select **Tags/Prefix** to apply the tiering rule to specific objects. You can filter objects by entering a prefix, tags, or both. Objects with the prefix and tags you specified get filtered and the tiering rule applies to those objects.

      Objects is a flat namespace and directories are a file construct. Directories may be simulated in Objects but they are not true directories.

      Lifecycle policy prefix should include the entire directory hierarchy.

      Some examples of prefix and explanation which files (objects) it will apply to:

      - **log** - Only files/folders in the root of the bucket that start with "log".
      - **serverA**- All files in folder "serverA", which is in the root of the bucket.
      - **serverB/log** - Files in folder "serverB" that start with "log".

      Note:

      It is important to note that the S3 lifecycle prefix cannot be used as a bash path expansion. As a result, it is not possible to specify a prefix such as "server*/log" for all files that begin with "log" in folders that begin with "server".

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 850

9. In the **Configure Rule** page, do the following, and then click **Next**.

   a. Select the **Tiering** check box.

      1. In the **Endpoint** list, select the endpoint where you want to tier out the objects.
      2. Enter a time period after which you want to move the objects to the selected endpoint. You can specify the number in days, months, or years.

         Note: The time for tiering objects must be less than the expiration time.

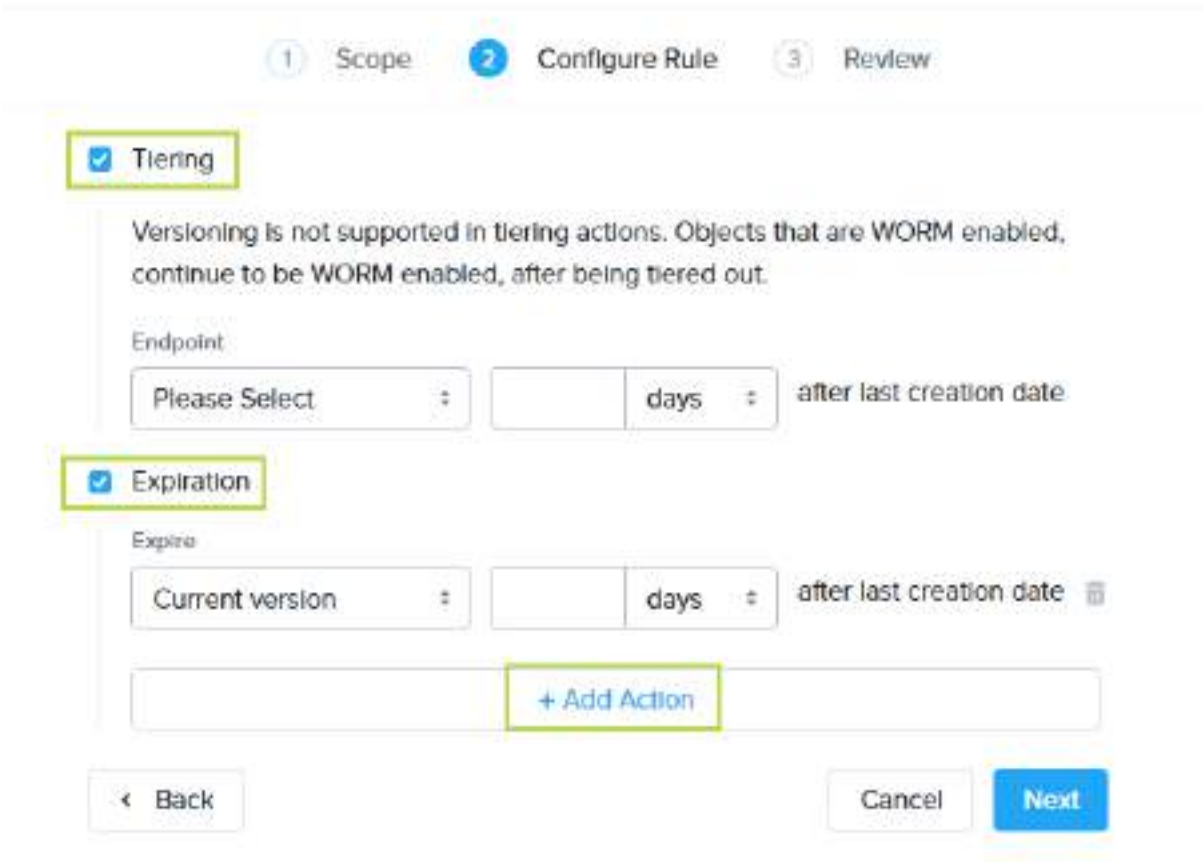


Figure 88: Creating Tiering Rule

   b. Select the **Expiration** check box.

      1. In **Expire**, select **Current version**, **Previous version**, **Multipart uploads**, or **Delete markers** according to your requirement.

         The **Previous version** and **Delete markers** options appear only for a version-enabled bucket.

         The expiration of delete marker and the current version cannot be configured in a single rule.

         Tip: It is recommended to create a rule to automatically expire delete markers to enhance the performance of your object stores.

      2. Enter a time period after which you want the objects to expire. You can specify the number in days, months, or years.

   You can click **Add Action** to add multiple expiration rules. You can create expiration rules for the current version, previous version, and multipart uploads.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 851

10. On the **Review** page, check your configurations. Then, click **Done** to create the rule.
    The rule you just created gets enabled and appears in the Rules table.

Figure 89: Tiering Rule - Actions

- You can select a bucket, and update, delete, disable, and enable the rule using the **Actions** drop-down.
- You can also export multiple rules to an XML file by clicking **Export to XML**.

Tiering Statistics

Cloud tiering supports endpoints such as, Nutanix Objects, Other S3 Compatible, and Azure Blob Storage. You can view the amount of object data moved to the endpoint bucket and the amount of pending data. You can also view the statistics for the source bucket (Object Store bucket) and the endpoint bucket.

Object Store Bucket - Statistics

In the object store instance page, click the **Bucket** tab. Click the bucket name, and then click the **Summary** tab to view its tiering statistics.

You can view the following information:

- **Tier out object size**: The amount of object data that has been tiered from this source bucket to the endpoint buckets.
- **Space pending reclamation**: The amount of the deleted data and metadata left out due to incomplete operations.
- **Total size of objects marked for tiering (pending)**: The amount of the object data (eligible for tiering) that is in the process of tiering.

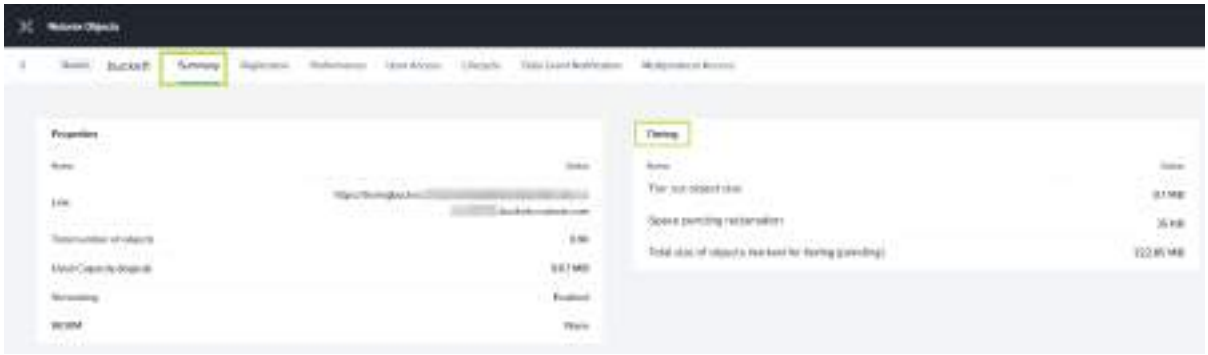


Figure 90: Source Bucket - Statistics

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 852

Endpoint Bucket - Statistics

You can view the tiering statistics for a configured endpoint-bucket. In the **Object Store** page, click **Settings** > **Tiering Endpoint**.

You can view the following information:

- **Name**: Name of the endpoint.
- **Usage**: The amount of object data moved to the endpoint bucket from the source buckets.
- **Objects pending for tiering (size)**: Amount of the object data that is in the process of tiering.
- **Average Bandwidth**: The rate at which the object data from all the source buckets is getting transferred to the endpoint bucket.
- **Endpoint Type**: Displays the type of endpoint.

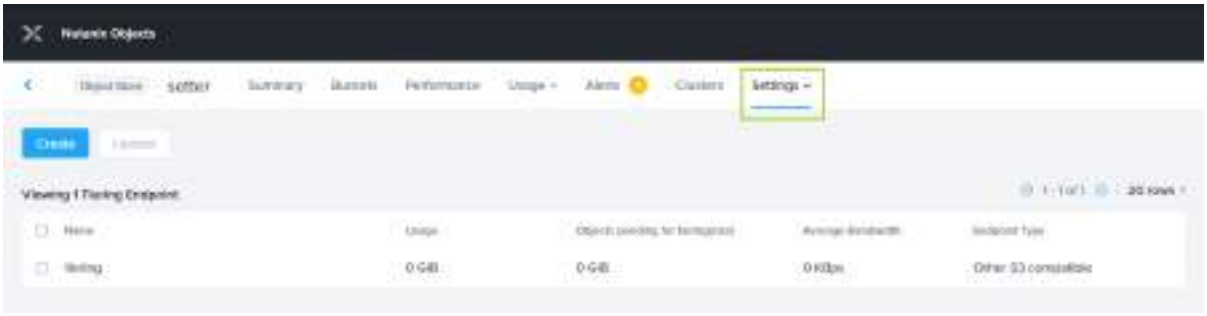


Figure 91: Endpoint Bucket - Statistics

Note: The tiering statistics are updated in the user interface after a tiering task is completed. However, when a large amount of data is tiered to an endpoint, you might experience a delay in seeing the updated statistics in the user interface.

Legal Hold for Objects

Legal hold allows you to lock an object indefinitely. There is no expiration date. A legal hold remains active until an authorized user explicitly removes it. Implementing a legal hold prevents the object data from being modified or deleted.

There are various cases where you would want to implement a legal hold on your object data. For example, put an indefinite lock on objects that you want to preserve for legal cases, audits, or compliance purposes.

Note the following points about the legal hold functionality in Nutanix Objects:

- A user with the write permission on the bucket can apply a legal hold to the objects within the bucket.
- Only an administrator or bucket owner can remove the legal hold applied to the objects.
- A legal hold can be applied while writing an object or to an existing object also.
- If a bucket gets created using the Prism GUI and a user with write permissions applies a legal hold to the objects within the bucket, an administrator user needs to be set up to remove the legal hold. Contact Nutanix support to set up an administrator user with the necessary permissions. It is recommended that the user should create a bucket. In this case, the user will be the bucket owner and will have permission to remove the legal hold.
- If you are replicating a bucket created in Object v3.1 (with the legal hold applied) to a bucket created in Objects v3.0, the legal hold attributes will not get replicated.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 853

A legal hold can be applied to the objects using the AWS S3 APIs. For more information, see Supported APIs on page 240.

WORM Bucket

Write-once-read-many (WORM) buckets protect your data and metadata. You can configure a WORM bucket to allow the creation of new objects and prevent overwrites or deletion of the existing content for a particular retention period. By default, versioning is not enabled on a bucket. When you apply the WORM policy on a bucket, you can choose to enable versioning. In some industries, regulations or compliance rules mandate long-term records retention, sometimes for more than 7 years. For example, in the financial and health services industry, you must maintain the records in their original state, which cannot be overwritten or erased.

A non-admin user can perform WORM bucket operations only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions and the non-admin user must be assigned to specific objects instances:

- Edit Buckets
- View Buckets
- View Object Store

Note:

- Administrators and non-admin users are Prism Central users with the following roles:
  - Administrator—A Super Admin or a Prism Admin in Prism Central.
  - Non-admin user—A Prism Central user without any administrator privileges.

  For more information about the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.
- Users with Edit Bucket permission can create WORM buckets on the buckets available in the Object stores that are assigned to the respective users.

When you increase the retention period of a bucket, the new retention period applies to the existing objects as well as the newly added objects.

When you apply any lifecycle policy to a WORM bucket with or without versions enabled, the policy is not applicable until the WORM retention period has passed.

Note:

- WORM can not be enabled for the buckets with NFS protocol support enabled.
- You cannot enable the WORM policy while creating a bucket.
- You can set 1 day as the minimum and 100 years as the maximum limit for the retention period.

Operations on a WORM Bucket

This topic lists the valid and invalid operations on a WORM bucket. You can refer to this list before performing any operation on a WORM bucket.

Valid Operations

Following are the valid operations:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 854

- Delete objects.

  Note: This operation does not delete the data, but creates a delete marker on top of the existing versions of objects.

- Delete the delete marker.
- Delete the target version of the object after the retention period.
- Create a new version of the object and retain old versions.
- Extend the retention period.

Invalid Operations

Following are the invalid operations:

- Enable WORM policy while creating a bucket.
- Enable WORM policy without specifying the retention period.
- Reduce the retention period.
- Delete the targeted version before the retention period.
- Change the version state.
- Does not support legal hold and governance mode.

Applying WORM Policy to Buckets from Prism Central

You can apply WORM policy only after the bucket is created. A WORM bucket allows you to create new objects and prevents you to overwrite or delete the existing content for a particular retention period.

About this task

Warning: You cannot modify or delete objects inside a WORM bucket for the specified time period.

To apply WORM policies to buckets.

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the object store which contains the bucket.
   The object store opens in a new window.
4. Click the **Buckets** tab.
5. In the Buckets table, select the bucket to apply the WORM policy.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 855

6. Click **Actions** > **Configure WORM**.
   The **Configure WORM on** *bucketname* window appears.

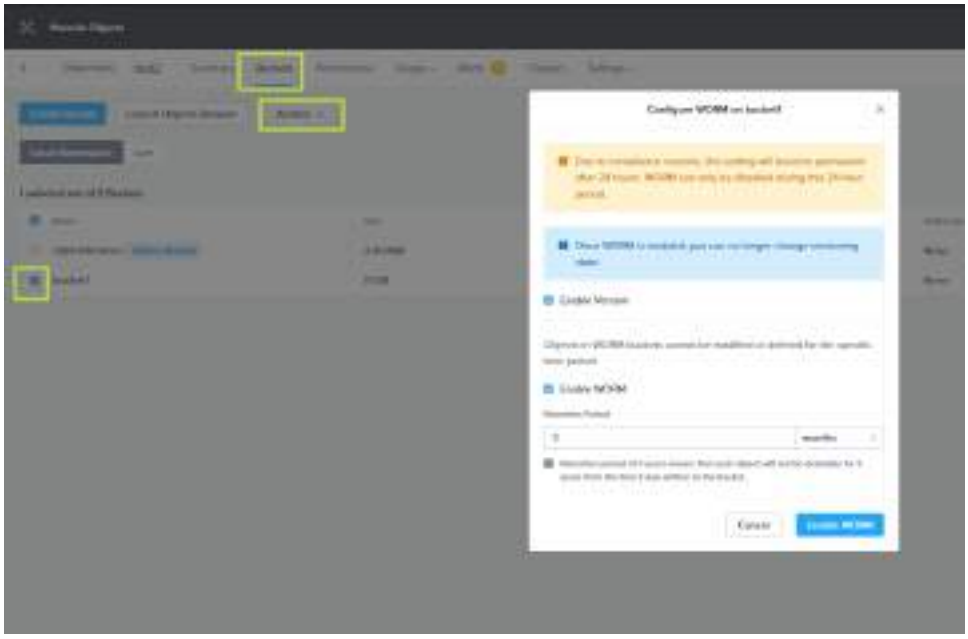


Figure 92: Configure WORM Window

Note:

- If versioning is disabled on a bucket, you can enable versioning while enabling WORM. However, once the WORM is enabled, you cannot change the versioning state.
- You cannot suspend versioning on WORM buckets.

Caution:

- For legal compliance reasons, the setting becomes permanent after 24 hours. You can disable the WORM policy within the first 24 hours of the grace period.
- You can only edit the retention period to increase the length of retention. You cannot decrease the retention period.

7. (Optional) Click the **Enable Version** check box to enable versioning.
8. Click the **Enable WORM** checkbox.
9. Type the retention period (in years or months or days) in the **Retention Period** field by entering a number, and then selecting the time period from the drop-down menu.
10. Click **Enable WORM**.
    This procedure successfully applies the WORM policy to the bucket.

Configuring a Bucket for Static Website Hosting

You can use Objects to host a static website that has individual web pages with static content. To host a static website on Objects, you can configure a bucket for website hosting, and then upload your website

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 856

files (objects) to the bucket. When you configure a bucket as a static website, you enable static website hosting, and optionally, add an index document and an error page. You can upload files (such as index documents and error pages) to the bucket using an S3 browser. The S3 browser uses the S3 protocols by providing access and the secret key. You can also choose to redirect to a website. Once you have configured your bucket as a static website, you can access the bucket through the object store endpoints for your bucket.

Before you begin

A non-admin user can configure static website hosting only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions and the non-admin user must be assigned to specific objects instances:

- Edit Buckets
- View Buckets
- View Object Store

> **Note:**
>
> - Website hosting implicitly grants anonymous public read access of all objects.
> - Administrators and non-admin users are Prism Central users with the following roles:
>   - Administrator—A Super Admin or a Prism Admin in Prism Central.
>   - Non-admin user—A Prism Central user without any administrator privileges.
>
>   For more information about the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.
> - Users with Edit Bucket permission can configure buckets for static website hosting on the buckets available in the Object stores that are assigned to the respective users.

About this task

> **Note:**
>
> - Static website hosting cannot be configured for the buckets created using the NFS protocol.
> - Once you configure the static website for a bucket, you cannot turn off this feature from the Objects user interface. To turn off the static website for buckets, contact Nutanix Support.

To configure a bucket for static website hosting, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the object store which contains the bucket.
   The object store opens in a new window.
4. Click the **Buckets** tab.
5. In the **Buckets** table, select the bucket to configure for static website hosting.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 857

6. Click **Actions** > **Static Website**.
   The **Configure Static Website** window appears.

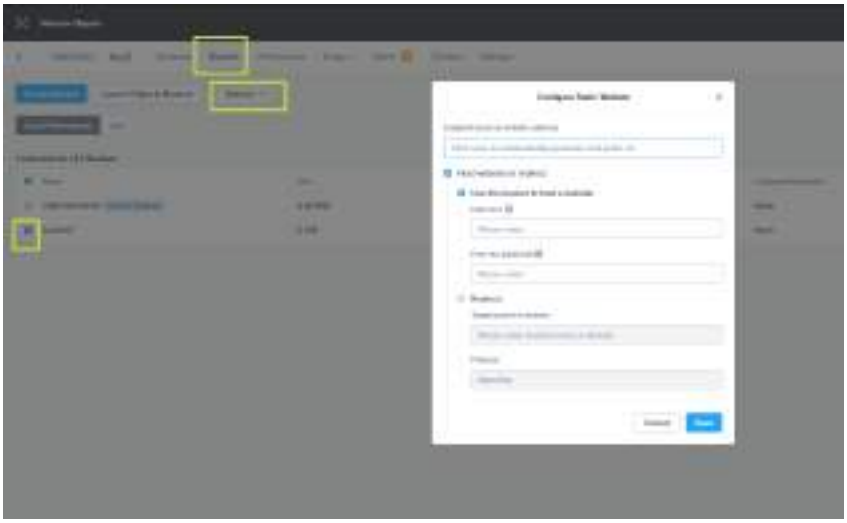


Figure 93: Configure Static Website Window

7. By default, the endpoint is auto-populated when you click **Save** at the last step.

   For example, when an endpoint auto populates, the URL will be in the format *objectstorename*.*domain*/*bucketname*. For example, `testobjectstore.nutanix.com/teamobjects`. However, if they have set up the DNS correctly, then you can also access the website with *bucketname*.*objectstorename*.*domain* endpoint using HTTP or HTTPS. For example, `https://teamobjects.testobjectstore.nutanix.com`.

8. Click the **Host Website or Redirect** check box.

   » **Use this bucket to host a website**: Select this option to use the bucket to host the website. Optionally, you can enter the name of the index document (for example, myindex.html) and an error page.

   An index document is a web page that Objects returns when you request the root of a website. It is the default page that loads when you are not requesting any specific page. After you enable static website hosting for your bucket, you can upload an HTML file with the index document name (for example, myindex.html) to your bucket. For example, if you specify no object in the URL, then the website loads the index page (myindex.html) that you have configured. If you have not configured an index document, then website access to the root will return an access denied error message.

   A custom error page is a web page that Object returns when an error occurs. For example, if you are trying to load an object that does not exist, the website loads the error page that you have configured.

   » **Redirect**: Select this option to enter a website URL to redirect to that website. For example, when you try to access the bucket endpoint, you will be redirected to this website. The protocol used is either HTTP or HTTPS.

9. Click **Save**.

   An endpoint is auto-generated when you click **Save**. This endpoint will be the object store endpoint for your bucket and is used as the website address.

   You can now use your bucket as a static website. You can use the endpoint to test your static website.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 858

Cross-Origin Resource Sharing (CORS) Overview

Cross-Origin Resource Sharing (CORS) allows a web application loaded in one domain to access the restricted resources that are requested from another domain. With CORS support in Objects, you can create rich web applications and allow cross-origin sharing of resources from Objects.

For example, if you upload an image (for example, `image1.png`) in a bucket (for example, *first-bucket*) in *domain1* that contains some security-related information, and you are not allowed to make access to `image1.png` from a website (for example, `www.example.com`) on *domain2*. Then you can configure a CORS policy for that *first-bucket* to allow `www.example.com` to access the resources of the *first-bucket*.

Note:

- CORS cannot be configured for the buckets created using NFS protocol.
- When you configure a bucket for static website hosting, public can have only read access to that bucket. POST, PUT, and DELETE requests on the bucket will be denied.

For configuring CORS for a bucket, create an XML document with the following. The document size is limited to 64 KB.

- Rules that identify the origins that you will allow to access your bucket.
- The operations (HTTP methods) that will support each origin.
- Other operation-specific information.

When Objects receives a cross-origin request for a bucket, it checks the CORS configuration on the bucket and uses the first `CORSRule` rule that matches the incoming browser request to enable a cross-origin request. You can add up to 100 rules to the configuration.

Following are the conditions to match the rules.

- The `Origin` header of the request must match `AllowedOrigin` elements.
- The request method (for example, GET, PUT, HEAD, and so on) or the `Access-Control-Request-Method` header for a pre-flight `OPTIONS` request must be one of the `AllowedMethod` elements.
- Every header specified in the `Access-Control-Request-Headers` request header of a pre-flight request must match an `AllowedHeader` element.

Following is an example of CORS configuration with two `CORSRule`:

```
<CORSConfiguration>
 <CORSRule>
   <AllowedOrigin>http://www.example.com</AllowedOrigin>
   <AllowedMethod>PUT</AllowedMethod>
   <AllowedMethod>DELETE</AllowedMethod>
   <AllowedHeader>*</AllowedHeader>
 </CORSRule>
 <CORSRule>
   <AllowedOrigin>*</AllowedOrigin>
   <AllowedMethod>GET</AllowedMethod>
 </CORSRule>
</CORSConfiguration>
```

- The first `CORSRule` allows cross-origin PUT and DELETE requests whose origin is `http://www.example.com` origin. The rule also allows all headers in a pre-flight `OPTIONS` request through the

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 859

`Access-Control-Request-Headers` header. So, in response to any pre-flight `OPTIONS` request, Objects will return any requested headers.

> **Note:** Other than pre-flight `OPTIONS` request, no other requests are denied that fail the CORS policy checks.

- The second rule allows cross-origin GET requests from all the origins.

  The `*` wild-card character refers to all the origins.

Configuring CORS on a Bucket

Cross-Origin Resource Sharing (CORS) allows a web application loaded in one domain to access the restricted resources that are requested from another domain.

Before you begin

A non-admin user can configure CORS only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions and the non-admin user must be assigned to specific objects instances:

- Edit Buckets
- View Buckets
- View Object Store

> **Note:**
>
> - Administrators and non-admin users are Prism Central users with the following roles:
>   - Administrator—A Super Admin or a Prism Admin in Prism Central.
>   - Non-admin user—A Prism Central user without any administrator privileges.
>
>   For more information about the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.
> - Users with Edit Bucket permission can configure CORS on the buckets available in the object stores that are assigned to the respective users.

About this task

You set this configuration on a bucket so that the bucket can service cross-origin requests.

To configure CORS for a bucket, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the object store which contains the bucket.
   The object store opens in a new window.
4. Click the **Buckets** tab.
5. In the **Buckets** table, select the bucket to configure CORS.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 860

6. Click **Actions** > **CORS**.

Figure 94: Configure CORS Window

The **Configure CORS** window appears.

7. Type or copy and paste a configuration file, or edit an existing configuration.
   The configuration file must be an XML file.

8. Click **Save**.
   The CORS configurations are saved for the bucket.

Adding Tags to a Bucket

A tag is a label that you assign to a bucket, and it consists of a key and a value pair that you can define. You can add or remove tags from your buckets.

About this task

To add tags to a bucket, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the object store which contains the bucket.
4. Click the **Buckets**tab, and from the **Buckets** table, select the bucket to add tags.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 861

5. Click **Actions** > **Tags**.
   The **Add Tags** window appears.

Figure 95: Add Tag Window

6. To add a new tag, click **+ add tag**.
   The existing tags will be auto-populated. You can click the delete icon to delete a tag.

   Note:

   - The maximum number of tags allowed per bucket is 50.
   - Tag keys can be up to 128 Unicode characters in length, and tag values can be up to 256 Unicode characters in length.
   - Tag keys and values are case-sensitive.
   - Tag key should be unique and is a mandatory field, but tag value is optional.

   A new row appears to fill the key value of the tag.

7. Enter the key and value.

8. Click **Save**.
   The changes are saved.

Viewing Buckets

The Buckets view allows you to view the list of buckets in the object store and access detailed information about each bucket.

Before you begin

A non-admin user can view buckets only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions and the non-admin user must be assigned to specific objects instances:

- View Buckets
- View Object Store

Note:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 862

- Administrators and non-admin users are Prism Central users with the following roles:
  - Administrator—A Super Admin or a Prism Admin in Prism Central.
  - Non-admin user—A Prism Central user without any administrator privileges.

  For more information about the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.
- Users with View Buckets permission can view all the buckets on an assigned object store.

About this task

To view the list of buckets, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the object store in which you want to create a bucket. The object store opens in a new window.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 863

4. Click the **Buckets** tab.

Figure 96: Buckets List View

A new window appears with the list of buckets in a tabular view.

The following list describes the fields that appear in the buckets list. A dash (-) is displayed in a field when a value is not available or applicable.

> **Note:**
>
> In Prism Central, the object store only displays the federated buckets that it hosts and not all buckets that are part of the federation. To view all the buckets in a federation namespace, you need to use the Object Browser or any S3 client.

- **Name**: Displays the name of the bucket. Click the name to display the bucket summary. Refer to
- **Size**: Displays the size of the bucket.
- **Num. Objects**: Displays the number of objects in a bucket.
- **Versioning**: Displays if versioning is enabled or disabled in a bucket.
- **WORM**: Displays if WORM is enabled or disabled in a bucket.
- **Outbound Replication**: Displays the outbound replication status. The following statuses are displayed:
  - Enabled—If a replication rule is enabled.
  - Disabled—If all the replication rules are disabled.
  - None—If no replication rule is created on the bucket.
- **Multiprotocol Access**: Displays if multiprotocol access is enabled or disabled for the bucket.
- **Notifications** Displays if notifications are enabled or disabled.
- **Static Website & CORS**: Displays if static website or CORS is configured for a bucket.

You can also launch the Objects Browser for this object store, click **Launch Objects Browser**.

Bucket Summary

This page displays the bucket properties and tiering details.

To view the **Summary** page of a bucket, click the name of the bucket in the buckets table, and then click **Summary**. Refer to Viewing Buckets on page 147.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 864

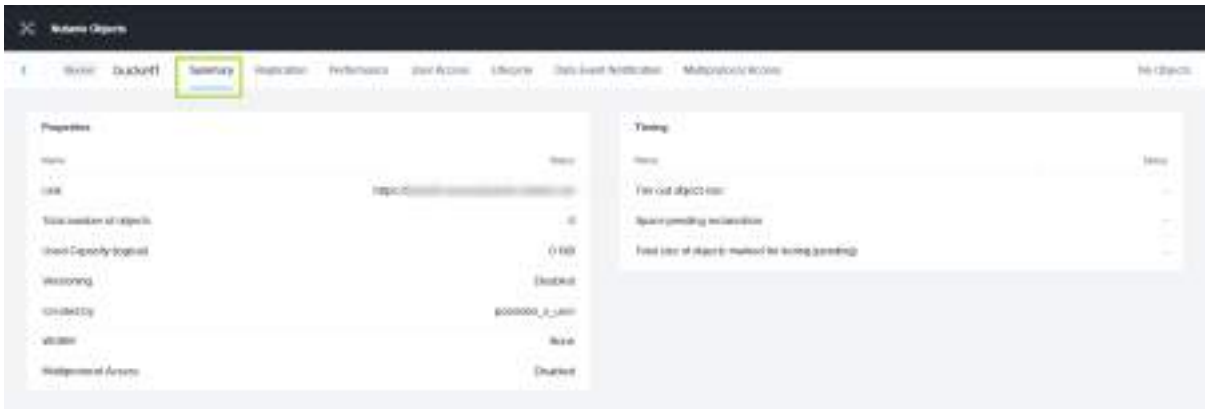


Figure 97: Bucket Summary

Updating a Bucket

You can update the bucket settings after creating the buckets and adding the objects to the buckets.

Before you begin

A non-admin user can update buckets only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions and the non-admin user must be assigned to specific objects instances:

- Edit Buckets
- View Buckets
- View Object Store

Note:

- Administrators and non-admin users are Prism Central users with the following roles:
  - Administrator—A Super Admin or a Prism Admin in Prism Central.
  - Non-admin user—A Prism Central user without any administrator privileges.

  For more information on the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.
- Users with Edit Bucket permission can perform an update bucket operation on the buckets available in the object stores that are assigned to the respective users.

About this task

Note:

- You cannot disable versioning (if enabled) but you can suspend it.
- You cannot edit multiple buckets at a time.

To edit a bucket, do the following:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 865

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the object store which contains the bucket.
   A new object store window appears.
4. Click the **Buckets** tab.
5. In the **Buckets** table, select the bucket for which you want to change the settings.
6. Click **Actions** > **Update**.
   The **Update Bucket** window appears.

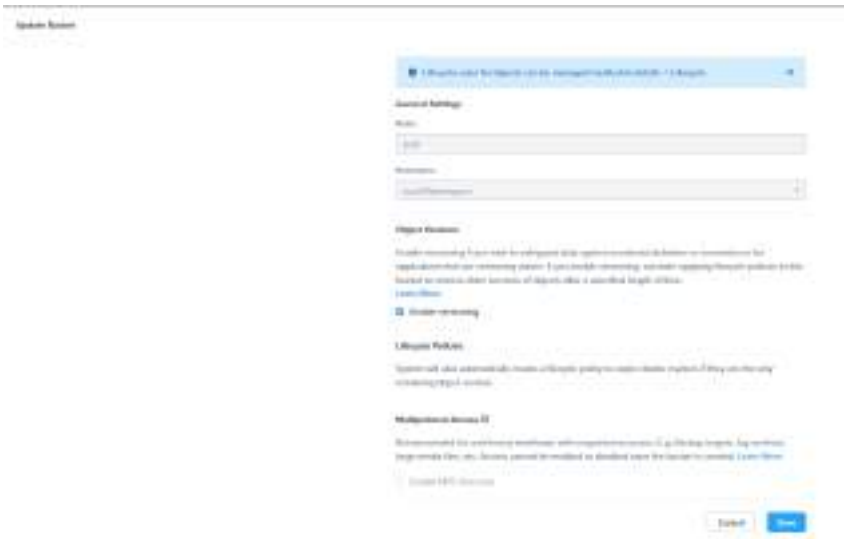


Figure 98: Update Bucket Window

7. Edit the settings that you want to change.
   For more information about the bucket settings, refer to Bucket Configuration.
8. Click **Save**.
   The changes are saved.

Sharing a Bucket

You can share a bucket with multiple users that have access keys.

Before you begin

A non-admin user can share a bucket only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions and the non-admin user must be assigned to specific objects instances:

- Edit Buckets
- View Buckets
- View Object Store

Note:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 866

- Administrators and non-admin users are Prism Central users with the following roles:
  - Administrator—A Super Admin or a Prism Admin in Prism Central.
  - Non-admin user—A Prism Central user without any administrator privileges.

  For more information on the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.
- Users with Edit Bucket permission can share a bucket available in the object stores that are assigned to the respective users.
- You can share only one bucket at a time.

About this task

To share a bucket, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the Object Store which contains the bucket.

Figure 99: Object Store List

The object store opens in a new window.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 867

4. Click the **Buckets** tab, and in the **Buckets** table, select the bucket that you want to share with other users.

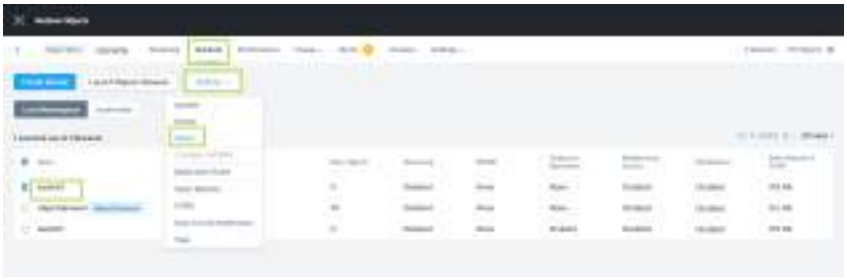


Figure 100: Sharing the Bucket

Note: You can only add users who have access keys.

5. Click **Actions** > **Share**.
6. Type the email address of the user and set the permission for that user.

Figure 101: Share Bucket Window

To generate access keys, refer to Generating Access Key for API Users on page 110.
To know more about Bucket Permissions, refer to Bucket Access Policies.

7. To add more users, click **+ Add User**.
8. Click **Save**.
The bucket is now shared with the listed users with the allotted permissions.

What to do next

You can list the buckets that are shared with you.

For more information, refer to Listing the Shared Buckets on page 157.

Bucket Access Policies

This section describes the authorization and access policies implemented in Objects.

Nutanix supports the following list of policies on a bucket:

- **Read Only**: Provides read-only access to the user.
- **Full Access**: Provides all access to the user.
- **Custom**: Provides customizing of varied levels of access to the user.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 868

Note: To evaluate the policy for a user, the union of the user specific policy and the anonymous policy is computed. For example, if the user specific policy contains one set of S3 actions and the anonymous policy for the bucket contains another set of S3 actions, then the resulting policy for the user for that bucket will be union of both set.

Table 8: Access Roles

Access Role	Description
User context with respect to buckets	
Owner	The user who creates the bucket. The owner can grant and revoke access to the non-admin users on the bucket. Owner can implicitly perform all operations.
Admin	PC admin who can manage the object-store from the UI.
Shared user	The non-owner user who gains access to the bucket based on the bucket policy assigned. A shared user can apply a bucket policy and grant access to various operations to any other user, provided they have the necessary access to perform `PutBucketPolicy` API.
Other (non-shared) users	The bucket is not shared with them and they do not have access to the bucket.
Anonymous	Refers to someone who does not authenticate themselves, such as static website users.
User privilege levels (IAM)	
Admin user	Admin user will be implicitly allowed all the bucket resource related operations as mentioned in Permissions for Nutanix Objects Operations on page 154 .
Standard user	Any user who is not an admin. They have full control on the bucket which they create.

Permissions for Nutanix Objects Operations

This section describes the operations that can be performed by the owners and the admin users.

Owner Privileges

The owner can perform any S3 operations on a bucket. They have full control over the buckets they create and can grant access to the buckets to other users (non-admin users).

Any user can make changes as long as they have the necessary access permissions specified in the policy to perform the desired operation.

Bucket Owner has all actions permissions.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 869

Table 9: Operations Performed by an Owner

AbortMultipartUpload
DeleteBucket
DeleteBucketWebsite
DeleteObject
DeleteObjectTagging
DeleteObjectVersion
DeleteObjectVersionTagging
GetAccelerateConfiguration
GetAnalyticsConfiguration
GetBucketAcl
GetBucketCORS
GetBucketLocation
GetBucketLogging
GetBucketNfsConfiguration
GetBucketNotification
GetBucketObjectLockConfiguration
GetBucketPolicy
GetBucketPolicyStatus
GetBucketPublicAccessBlock
GetBucketRequestPayment
GetBucketTagging
GetBucketVersioning
GetBucketWebsite
GetEncryptionConfiguration
GetInventoryConfiguration
GetLifecycleConfiguration
GetMetricsConfiguration
GetObject
GetObjectLegalHold
GetObjectRetention
GetObjectTagging
GetObjectVersionTagging
ListBucket
ListBucketMultipartUploads
ListBucketVersions
ListMultipartUploadParts

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 870

PutBucketCORS
PutBucketNfsConfiguration
PutBucketNotification
PutBucketObjectLockConfiguration
PutBucketPolicy
PutBucketTagging
PutBucketVersioning
PutBucketWebsite
PutEncryptionConfiguration
PutInventoryConfiguration

Admin Privileges

An admin user is implicitly granted permission to perform all operations related to bucket resources.

An admin can perform the following actions:

Table 10: Operations Performed by an Admin

DeleteBucket
DeleteBucketWebsite
GetAccelerateConfiguration
GetAnalyticsConfiguration
GetBucketAcl
GetBucketCORS
GetBucketLocation
GetBucketLogging
GetBucketNfsConfiguration
GetBucketNotification
GetBucketObjectLockConfiguration
GetBucketPolicy
GetBucketPolicyStatus
GetBucketRequestPayment
GetBucketTagging
GetBucketVersioning
GetBucketWebsite
GetEncryptionConfiguration
GetInventoryConfiguration
GetLifecycleConfiguration
GetMetricsConfiguration

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 871

GetReplicationConfiguration

ListBucket

ListBucketMultipartUploads

ListBucketVersions

PutBucketCORS

PutBucketNfsConfiguration

PutBucketNotification

PutBucketObjectLockConfiguration

PutBucketPolicy

PutBucketTagging

PutBucketVersioning

PutBucketWebsite

PutInventoryConfiguration

PutLifecycleConfiguration

PutReplicationConfiguration

Listing the Shared Buckets

Listing the Shared Buckets feature extends the S3 ListBuckets API and displays the buckets owned by or shared with the current user.

The current behavior of the S3 API for ListBuckets is to list the buckets that the current owner (caller of the API) owns. If you have created a bucket, then you are the owner of that bucket. For example, when an admin creates a bucket using the Objects user interface, the owner of all such buckets is the admin user. You (owner of the buckets) can choose to share buckets with one or more IAM users with *Read Only* or *Full Access* or *Custom* permissions. IAM users with whom a bucket is shared can access the bucket and its objects subject to the permissions granted. However, the Vanilla S3 API for ListBuckets does not allow for the discovery (listing) of buckets that were shared with them.

In earlier versions of Objects, if you share a bucket, you have to inform the user which bucket is shared with them. However, with Objects 2.1 and later versions, *Listing the Shared Bucket* feature extends the S3 ListBuckets API and displays the buckets owned by or shared with the current user. If you delete a bucket that is shared, the bucket will automatically be removed from the list.

Note:

- This feature is a departure from the S3 specifications and is enabled by default. To disable the feature, contact Nutanix Support.
- This feature is only enabled for sharing relations created using Objects 2.1 or later versions. You cannot list the buckets created using earlier versions of Objects. A workaround to enable this feature retroactively is to have the owner of the bucket remove all the sharing relations and recreate them using the latest Objects version.

For example, an Admin created three buckets B0, B1, and B2. B1 and User2 were shared with User1 with any set of S3 actions. Following are the outputs of the `ListBuckets` API call before and after the introduction of *Listing the Shared Buckets* feature.

Before the introduction of *Listing the Shared Bucket* feature:

```
Admin B0 B1 B2
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 872

```
User1
User2
```

After the introduction of *Listing the Shared Bucket* feature:

```
Admin B0 B1 B2
User1 B1
User2 B2
```

Viewing Bucket Users

You can view all the users and their permissions for a particular bucket.

Before you begin

A non-admin user can view bucket users only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions and the non-admin user must be assigned to specific objects instances:

- View Buckets
- View Object Store

> **Note:**
>
> - Administrators and non-admin users are Prism Central users with the following roles:
>   - Administrator—A Super Admin or a Prism Admin in Prism Central.
>   - Non-admin user—A Prism Central user without any administrator privileges.
>
>   For more information about the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.
> - Users with View Buckets permission can view all the buckets on an assigned object store.

About this task

To view the usage of the bucket, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the object store which stores the bucket.
   The object store opens in a new window.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 873

4. Click the **Buckets** tab, and then from the Buckets list table, click the name of the bucket.

Figure 102: Buckets List

5. Click **User Access**.

Figure 103: List of Users

The table displays the list of users and their permissions.

You can edit the user access by clicking **Edit User Access**.

For more information about editing user access, refer to Editing User Access on page 159 topic.

Editing User Access

You can modify user access to grant different permissions, including read-only access, full access, or custom access to provide varied levels of access.

Before you begin

The non-admin user must be assigned to specific objects instances:

- Edit Buckets
- View Buckets
- View Object Store

Note:

- Administrators and non-admin users are Prism Central users with the following roles:
  - Administrator—A Super Admin or a Prism Admin in Prism Central.
  - Non-admin user—A Prism Central user without any administrator privileges.

  For more information on the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.
- If you access any of the buckets that are still utilizing the old-style policy, they will automatically be upgraded to the new policy. During the upgrade process, the set of access permissions will remain the same as it was before.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 874

About this task

To edit user access, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the Object Store which contains the bucket. The object store opens in a new window.
4. Click the **Buckets** tab, and then from the buckets list table, click the name of the bucket.
5. Click **User Access** > **Edit User Access** to edit.

Figure 104: List of Users

Bucket access configuration opens in a new window.

6. Type the email address of the user and set the permission for that user.

Figure 105: Share Bucket Window

Nutanix supports the following list of permissions on a bucket:

- **Read Only**: Provides read-only access to the user.
- **Full Access**: Provides all access to the user.
- **Custom**: Provides customizing of varied levels of access to the user.

7. To add more users and permissions, click **+ Add User and Permissions**.

Note:

- Ensure that multiple users that share the same set of permissions, are added as a single entry. This approach reduces the overall policy size and enables the sharing of buckets with a larger number of users without reaching the policy document size limit.
- If you add **All users** as **Users** and grant them **Full Access**, the user will be able to perform all operations without any authentication.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 875

8. Click the delete icon to remove an existing set of user and permission.
9. Click **Save**.
   The bucket is now shared with the listed users with the allotted permissions.

   Note: It is not possible to save a policy with an empty set of permissions. It is required to have at least one user and permission.

Deleting a Bucket

If you no longer require a bucket, you can delete the bucket.

Before you begin

A non-admin user can delete a bucket only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions and the non-admin user must be assigned to specific objects instances:

- Edit Buckets
- View Buckets
- View Object Store

Note:

- Administrators and non-admin users are Prism Central users with the following roles:
  - Administrator—A Super Admin or a Prism Admin in Prism Central.
  - Non-admin user—A Prism Central user without any administrator privileges.

  For more information about the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.
- Users with Edit Bucket permission can delete a bucket available in the object stores that are assigned to the respective users.

About this task

You can delete the following:

- Multiple empty buckets at a time.
- A bucket with versioning enabled; however, it permanently deletes all the versions of the buckets.

  Note: You cannot delete buckets containing objects and WORM-enabled buckets

To delete a bucket, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the object store which contains the bucket.
   The object store opens in a new window.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 876

4. Click the **Buckets** tab, and then from the Buckets list table, click the check box next to the name of the bucket that you want to delete.
5. Click **Actions** > **Delete**.

Figure 106: Delete Bucket Window

6. On the dialog box, click **Confirm**.
   A message appears to confirm the deletion of the bucket.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 877

OBJECTS BROWSER

The Objects Browser is a User Interface (UI) that allows the users to directly launch the object store instance in a web browser and perform bucket and object-level operations. This eliminates the steps of logging into Prism Central and launching the Objects service.

The administrators use Prism Central to manage the object stores. When an administrator creates an object store, a default bucket (*objectsbrowser*) gets created. The static website hosting capability is already enabled on this default bucket. The Objects Browser UI is hosted on this default bucket.

To launch the Objects Browser, select the object store and click **Actions** > **Launch Objects Browser**. Objects Browser will be opened in a new window. You can also launch the Objects Browser from the buckets list page (Refer to Viewing Buckets on page 147).

Alternatively, if you have multiple load balancer IP addresses for the object store, you can click any of the IP addresses to launch the Objects Browser for that object store.

Figure 107: Prism Central - Launch Objects Browser

The administrator can also share the object store URL with the user to access the Objects Browser UI. The URL can be formed using the Objects Public IP address.

`http://objects-public-ipaddress/objectsbrowser`

> **Note:** You can use http or https to access the Objects Browser.

Refer to the following image to understand the URL formation.

Figure 108: Objects Browser URL

> **Note:**
>
> - Refreshing the page would log out the user and cancel the pending and in-progress uploads.
> - Any uploads taking more than 60 minutes gets terminated and retried three times before getting canceled.

Administrator Workflow: Objects Browser

The administrator needs to perform the following steps to grant access to the Objects Browser to a particular user.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 878

About this task

Note:

- Objects Browser does not store the access and secret keys.
- If the user refreshes the page with the refresh button of the web browser, they will need to provide the credentials again, and any unsaved changes will be lost (including any pending or in-progress uploads).

To grant access to Objects Browser, do the following:

Procedure

1. Add the IAM user.
   For more information, refer to Generating Access Key for API Users on page 110.
   After the administrator adds the user, the access and secret keys are generated.
2. (Optional) Grant access permissions (read only, full access, or custom) to the buckets.
   For more information, refer to Sharing a Bucket on page 151.

   Note: This step is optional and can be performed if the administrator wants to share bucket of another user with a new user. If the administrator does not perform this step, the buckets list will be empty for the IAM users. The users can still create buckets from the Objects Browser UI.
3. Share the Objects Browser URL with a user to launch the object store in a web browser.
4. Share the access and secret keys that you generated for the user.
   The user would require to enter the keys in the login page of the Objects Browser UI.

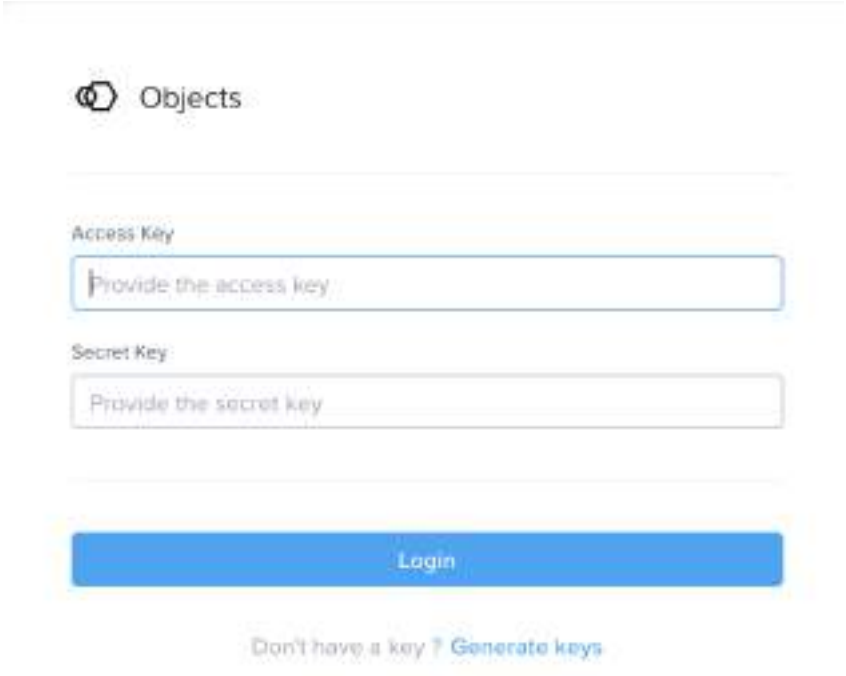


Figure 109: Objects Browser Login Page

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 879

What to do next

The user can log on to the Objects Browser UI and perform CRUD operations within the object store. For example, create buckets, upload objects, assign a tag to objects, and so on. Refer to Supported Operations on page 167.

Launching the Objects Browser

You can use the object store URL and keys shared by the administrator to launch the Objects Browser UI.

About this task

To launch the Objects Browser, do the following:

Procedure

1. Open the object store URL shared by the administrator in a web browser.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 880

2. In the **Objects Browser** login page, enter the **Access** and **Secret** keys to access the object store instance.

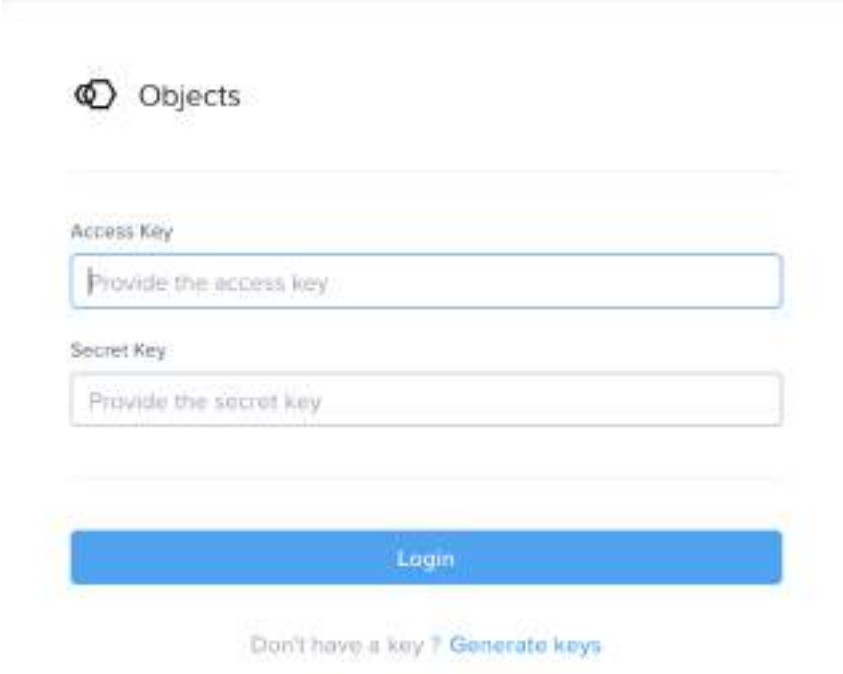


Figure 110: Objects Browser Login Page

Note: Access and Secret keys will be shared by the Administrator.

The object store will be opened in the Objects Browser.

Figure 111: Object Browser Landing Page

What to do next

You can now perform CRUD operations on buckets and objects. Refer to Supported Operations on page 167. You can also change the mode from light to dark, logout, or see the version by clicking the user name at top-right corner.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 881

Supported Operations

This section describes the various CRUD operations that a user can perform in the buckets and objects of an object store from the Objects Browser UI.

Bucket Operations

After you log into the Objects Browser, all the buckets that the administrator shared with you are listed with creation date and owner information.

Figure 112: Objects Browser - Bucket CRUD Operations

You can perform the following operations at the bucket level:

- **Create Bucket**: Allows you to create buckets. For more information, see Creating an S3 Bucket Using Objects Browser on page 168.
- **Lifecycle**: Allows you to create lifecycle rules.

  Click the name of the bucket, and then click the **Lifecycle** option at the left pane. For information, refer to Creating Lifecycle Rules Using Objects Browser on page 173.
- You can use the **Actions** list to update bucket properties, host a static website, configure CORS, and delete a bucket.
  - **Update**: Allows you to update the bucket properties.

    To update bucket properties, select the bucket, and then click **Actions** > **Update**.
  - **Delete**: Allows you to delete a bucket.

    To delete a bucket, select the bucket, and then click **Actions** > **Delete**.

    Note: You can only delete an empty bucket. In the case of a version-enabled bucket, the delete operation performed on an object is not permanent. The object gets removed from the list and moved

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 882

to Recycle Bin and a Delete Marker gets created. For more information, see Understanding Object Versions on page 185.

- **Share**: Allows you to share the bucket.

  To update bucket properties, select the bucket, and then click **Actions** > **Share**.

  You can share a bucket with multiple users and provide permissions such as **Read only**, **Full Access**, and **Custom**. For more information see, Sharing a Bucket Using Objects Browser on page 171.

- **Static Website**: Allows you to configure a bucket to host a static website.

  You can configure a bucket for website hosting, and then upload your website files (objects) to the bucket. For more information see, Configuring a Bucket for Static Website Hosting on page 176.

- **CORS**: Allows you to configure CORS on a bucket.

  This allows the bucket to service cross-origin requests. For more information see, Configuring CORS on a Bucket on page 177.

Creating an S3 Bucket Using Objects Browser

You can create, modify, and delete a bucket using the Objects Browser.

About this task

Note:

- Make sure that the bucket names are unique for all users.
- You cannot configure a WORM bucket while creating a bucket. You can edit WORM policies only after creating a bucket.
- You cannot enable multi-protocol access on an S3 bucket.
- NFS buckets cannot be created using Objects Browser.
- While creating a new versioned bucket, the system will automatically create a lifecycle policy to expire the delete markers if they are the only remaining object versions.

To create and configure a bucket, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. Click the name of the object store in which you want to create a bucket and launch the Objects Browser.

   For more information about launching the Objects Browser, see Launching the Objects Browser on page 165.

   The object store opens in a new window.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 883

4. Click **Create Bucket**.
   The **Create Bucket** window appears.

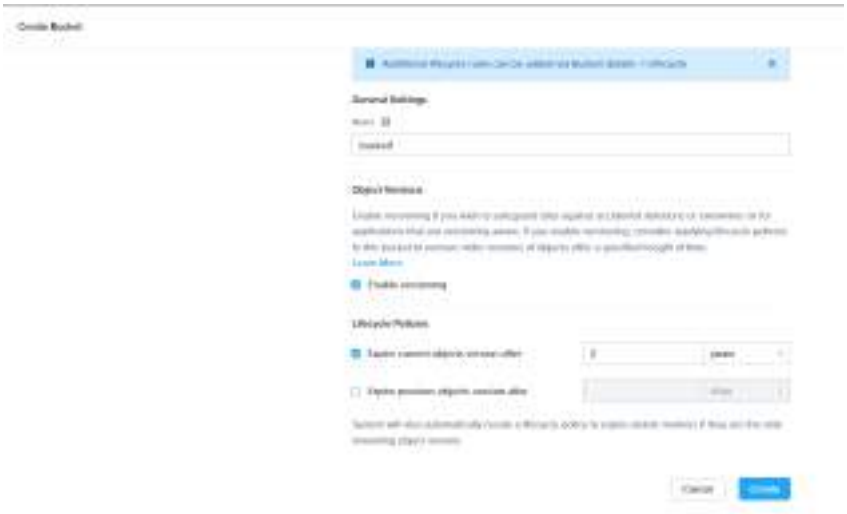


Figure 113: Create Bucket Window

5. On the **General Settings** section, type a name for your bucket.
   For more information about naming buckets, see Buckets Naming Conventions.

6. (Optional) On the **Object Versions** section, configure the following:
   For more information about versions, see Object Versioning.

   a. **Enable Versioning**: Select this check box to enable versioning of objects.
      This allows you to keep all versions of an object in the same bucket. For more information about versions, see Object Versioning.
      To apply life cycle policy with versioning enabled, see Rules for Lifecycle Policy When Object Versioning is Enabled on page 129.

      Note: Enabling versioning allows you to recover objects from accidental deletion and overwrite.

7. (Optional) On the **Lifecycle Policies** section, select the following:
   For more information, refer to Lifecycle Policies.

   a. **Expire current objects version after:**: Select to type a time period after which the current version of the object expires.
      You can specify the number in days, months, or years.

   b. **Expire previous objects versions after**: Select this check box to enter a time period to delete all the previous versions of the objects. This option is available only if versioning is enabled.
      You can specify the number in days, months, or years.

      Note:

      - If versioning is not enabled, the current object is deleted permanently. When you enable versioning, multiple versions of the same object are maintained in a bucket.
      - NFS buckets cannot be created using Objects Browser.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 884

8. Click **Save**.
   The bucket is created successfully.

What to do next

After creating a bucket, you can create objects through S3 APIs and manage them. For more information, see Supported S3 APIs.

You can also perform various actions on a bucket, such as configuring static websites and configuring CORS on a bucket.

- For more information on creating lifecycle rules, see Creating Lifecycle Rules Using Objects Browser on page 173.
- For more information on configuring static websites, see Configuring a Bucket for Static Website Hosting on page 176.
- For more information on configuring CORS on a bucket, see Configuring CORS on a Bucket on page 177.

Updating a Bucket

After you create a bucket, you can update the bucket settings using Objects Browser.

About this task

> **Note:** Life cycle rules created for a bucket cannot be modified from here. To modify the lifecycle rules for a bucket, refer to Creating Lifecycle Rules Using Objects Browser on page 173.

To update bucket settings, do the following:

Procedure

1. Log on to the Objects Browser.
   For more information about launching an Objects Browser, see Administrator Workflow: Objects Browser and Launching the Objects Browser.
2. From the object store, select the bucket that you need to update.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 885

3. Click **Actions** menu > **Update**.

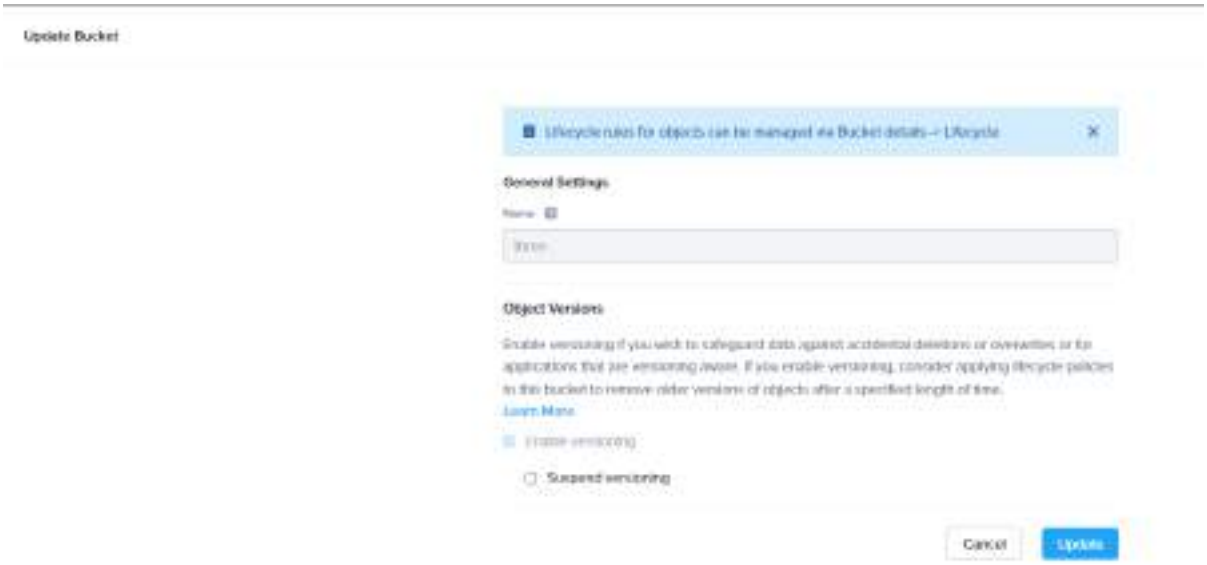


Figure 114: Update Bucket Window

4. On the **Object Versions** section, select one of the checkboxes to enable or disable versioning of objects in the bucket.

   a. **Enable versioning**: Select this check box to enable versioning on objects and to keep all the versions of the object on the same bucket.

   > **Note:** Select this option to recover objects from accidental deletion or overwrite.

   b. **Suspend versioning**: Select this check box to disable versioning of objects in a bucket.

   When you suspend versioning, accumulation of the new object versions is stopped. However, versions of objects already existing in the bucket are retained.

5. Click **Done**.
   The updated settings are applied to the bucket successfully.

Sharing a Bucket Using Objects Browser

You can modify user access to grant different permissions, including read-only access, full access, or custom access to provide varied levels of access.

Before you begin

The ability to perform the share bucket operation is limited to the owners of the bucket. If a non-owner attempts to update the policy, they must have the necessary permissions granted by the owner or administrator in the bucket policy. Without these permissions, the non-owner will receive an `Access Denied` error message.

About this task

To share a bucket, do the following:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 886

Procedure

1. Log on to the Objects Browser.
   All the buckets that the administrator shared with you are listed with creation date and owner information in a new window.
2. Click the **Buckets** tab, and in the **Buckets** table, select the bucket that you want to share with other users.

Figure 115: Sharing the Bucket

3. Click **Actions** > **Share**.
4. To **Add Users and Permissions** type the email address of the user and set the permission for that user.

Figure 116: Share Bucket Window

To generate access keys, refer to Generating Access Key for API Users on page 110.

To know more about Bucket Permissions, refer to Bucket Access Policies.

Nutanix supports the following list of permissions on a bucket:

- **Read Only**: Provides read-only access to the user.
- **Full Access**: Provides all access to the user.
- **Custom**: Provides customizing of varied levels of access to the user.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 887

5. To add more users and permissions, click **+ Add User and Permissions**.

> **Note:**
>
> - If you add **All users** as **Users** and grant them **Full Access**, the user will be able to perform all operations without any authentication.
> - To add a new user, it is necessary to enter the precise user name without any variations or errors. As there are no auto suggestions provided.
> - You can enter multiple user name by providing space in between each user names.

6. Click the delete icon to remove an existing set of user and permission.
7. Click **Save**.
   The bucket is now shared with the listed users with the allotted permissions.

> **Note:**
>
> - It is not possible to save a policy with an empty set of permissions. It is required to have at least one user and permission.
> - Modifying or revoking permissions for a user who is the bucket owner does not affect the bucket. The owner retains unrestricted access and can continue to perform all operations on the bucket.

Creating Lifecycle Rules Using Objects Browser

Lifecycle policy enables you to create or update a set of rules that define actions that Nutanix Objects applies to a group of objects within a bucket. With these policies, you can expire objects when no longer required.

Before you begin

Refer to Lifecycle Policies on page 128.

About this task

> **Note:** Rules or any updates to the rules get applied to the new objects that you create and do not apply to the objects existing before the rule creation or update.

To create a lifecycle rule, do the following:

Procedure

1. Log on to the Objects Browser.
2. In the list of buckets, click the name of the bucket for which you want to create a rule.
3. Click **Lifecycle**.

Figure 117: Objects Browser - Create Lifecycle Rule

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 888

4. Click **Create Rule**.
   When you have no rules created, you can directly import the XML. The **Import XML** option is not available if you already have rules to avoid overwriting.
5. In the **Scope** section, do the following, and then click **Next**:

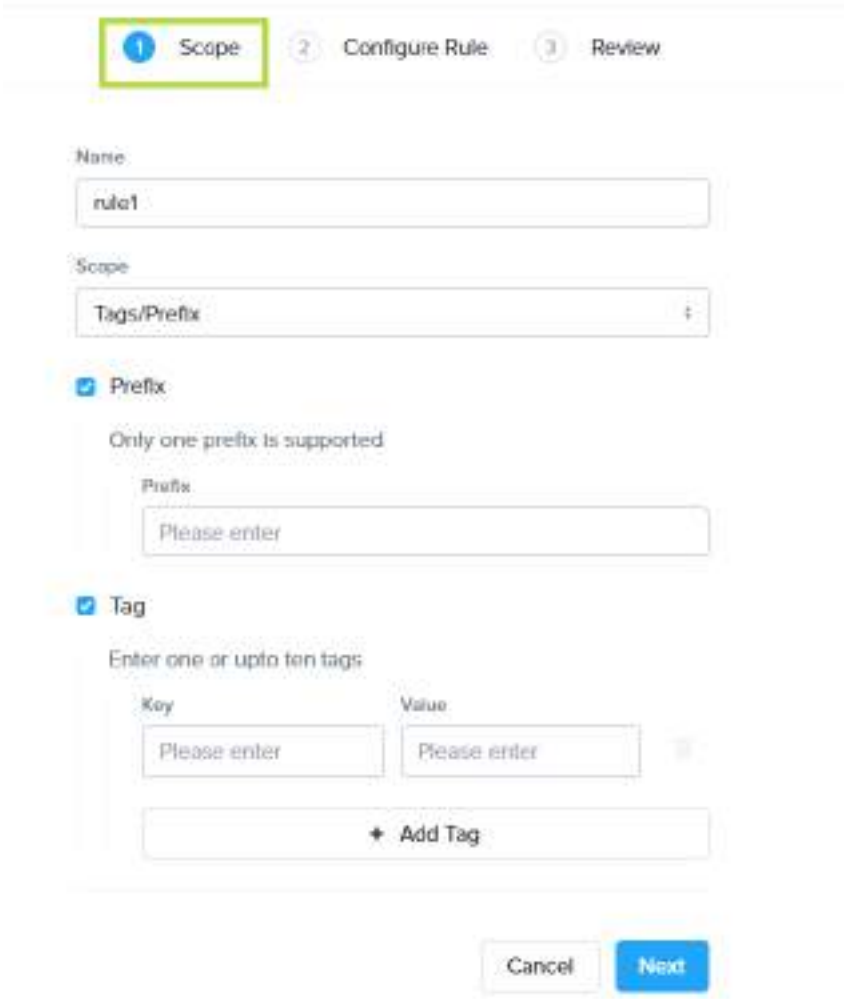


Figure 118: Defining Scope for a Rule

a. **Name**: Enter a name that identifies the rule you are creating.
b. **Scope**: Select the scope of the rule to either all objects of that bucket, or to tags and prefixes.
   - » **Prefix**: You can enter only one prefix.
   - » **Tag**: You can enter up to 10 tags in key value pair.
     Click **+ Add Tag** to add more tags.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 889

6. In the **Configure Rule** section, do the following, and then click **Next**:

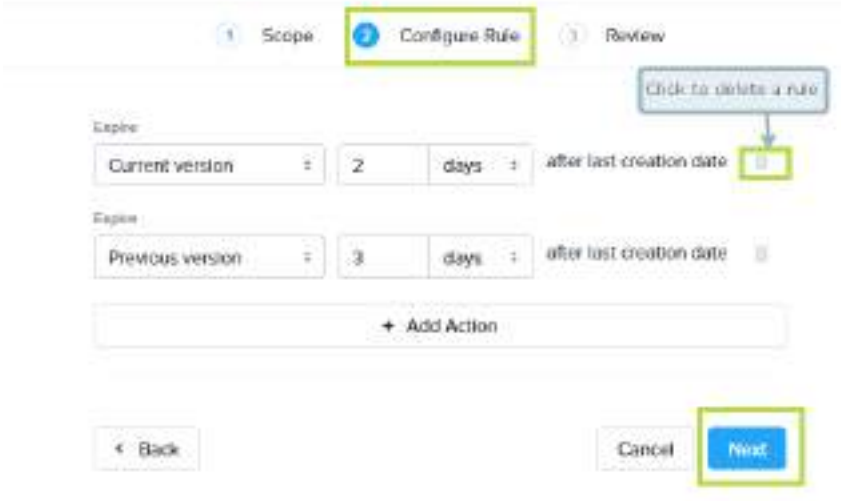


Figure 119: Configuring Rule

> **Note:** You cannot configure the tiering endpoints from the Objects Browser. You can configure it from the Objects UI and the same is visible as *Read Only* in the Objects Browser UI.

a. **Expire** Select which version to expire: **Current version**, **Previous version**, **Multipart uploads**, or **Delete markers** according to your requirement.

- The **Previous version** and **Delete markers** options appear only for a version-enabled bucket.
- Duplicate expiration field is not allowed. For example, you cannot create two rules for the current version expiration.
- Expiration of delete marker and the current version cannot be configured in a single rule.

> **Tip:** It is recommended to create a rule to automatically expire delete markers to enhance the performance of your object stores.

> **Note:** Multipart uploads expiration should not be specified with tag-based filters.

b. **after last creation date** Specify the number in days, months, or years after which that respective version of the object expires after last creation date of that object.

You can click **Add Action** to add up to three expiration rules. You can create expiration rules for the current version, the previous version, and multipart uploads.

Click **Delete Icon** to delete the rule.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 890

7. In the **Review** section, review the scope and actions, and then click **Done**.

   - You can select a bucket, and update, delete, disable, and enable the rule using the **Actions** drop-down.
   - You can also export the multiple rules to an XML file by clicking **Export to XML**.

   > **Note:** Actions listed are executed in sequence.

   The rule you just created gets enabled and appears in the Rules table.

Configuring a Bucket for Static Website Hosting

You can use Objects Browser to host a static website that has individual web pages with static content. To host a static website on Objects, you can configure a bucket for website hosting, and then upload your website files (objects) to the bucket. When you configure a bucket as a static website, you enable static website hosting, and optionally, add an index document and an error page. You can upload files (such as index documents and error pages) to the bucket using the Objects Browser or S3 browser. The S3 browser uses the S3 protocols by providing access and the secret key. You can also choose to redirect to a website. Once you have configured your bucket as a static website, you can access the bucket through the object store endpoints for your bucket.

About this task

To configure a bucket for static website hosting, do the following:

Procedure

1. Log on to the Objects Browser.
2. In the **Buckets** table, select the bucket to configure it for static website hosting.
3. Click **Actions** > **Static Website**.
   The **Configure Static Website** window appears.

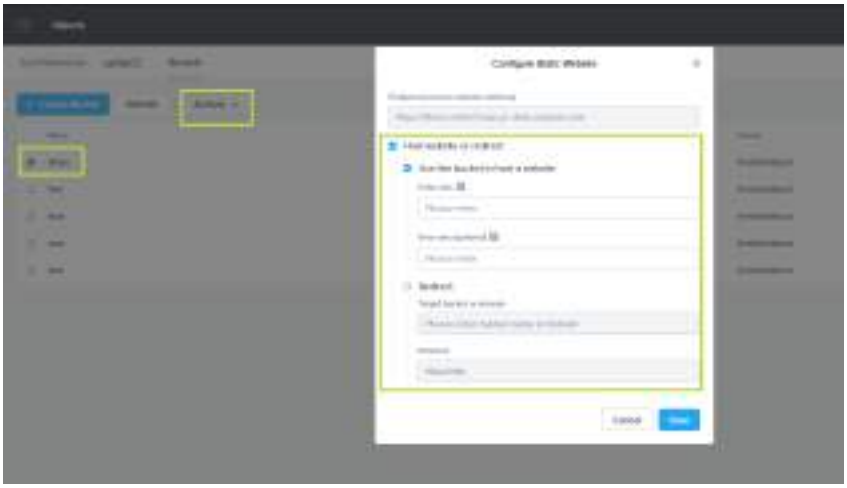


Figure 120: Configure Static Website Window

4. By default, the endpoint is auto-populated when you click **Save** at the last step.
   For example, when an endpoint auto populates, the URL will be in the format `objectstorename.domain/bucketname`. For example, `objectstore.nutanix.com/teamobjects`. However, if they have set up the DNS correctly, then you can also access the website with

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 891

bucketname.*objectstorename*.*domain* endpoint using HTTP or HTTPS. For example, `https://teamobjects.objectstore.nutanix.com`.

5. Click the **Host Website or Redirect** check box.

   » **Use this bucket to host a website**: Select this option to use the bucket to host the website. Optionally, you can enter the name of the index document (for example, myindex.html) and an error page.

   An index document is a web page that Objects returns when you request the root of a website. It is the default page that loads when you are not requesting any specific page. After you enable static website hosting for your bucket, you can upload an HTML file with the index document name (for example, myindex.html) to your bucket. For example, if you specify no object in the URL, then the website loads the index page (myindex.html) that you have configured. If you have not configured an index document, then a website access to the root will return an access denied error message.

   A custom error page is a web page that Object returns when an error occurs. For example, if you are trying to load an object that does not exist, the website loads the error page that you have configured.

   » **Redirect**: Select this option to enter a website URL to redirect to that website. For example, when you try to access the bucket endpoint, you will be redirected to this website. The protocol used is either HTTP or HTTPS.

   To remove the static website configuration from the Objects Browser, uncheck **Host website or redirect**, and then click **Save**.

6. Click **Save**.

   An endpoint is auto-generated when you click **Save**. This endpoint will be the object store endpoint for your bucket and is used as the website address.

   You can now use your bucket as a static website. You can use the endpoint to test your static website.

Configuring CORS on a Bucket

Cross-Origin Resource Sharing (CORS) allows a web application loaded in one domain to access the restricted resources that are requested from another domain.

Before you begin

Refer to Cross-Origin Resource Sharing (CORS) Overview on page 144.

About this task

You set this configuration on a bucket so that the bucket can service cross-origin requests.

To configure CORS for a bucket, do the following:

Procedure

1. Log on to the Objects Browser.
2. In the **Buckets** table, select the bucket to configure CORS.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 892

3. Click **Actions** > **CORS**.

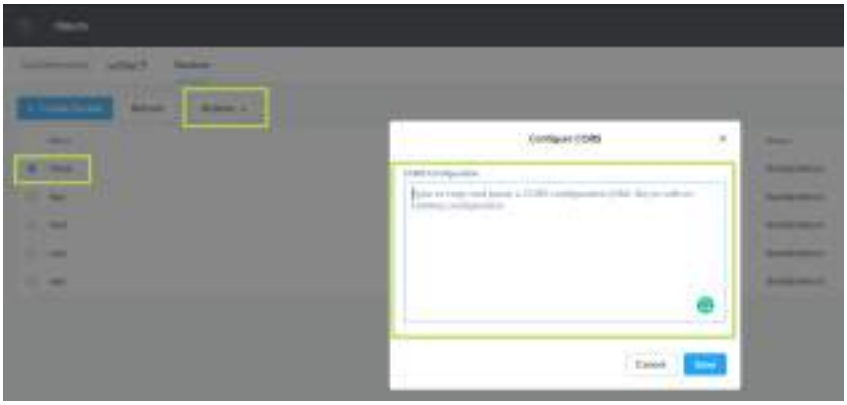


Figure 121: Configure CORS Window

The **Configure CORS** window appears.

4. Type or copy and paste a configuration file, or edit an existing configuration.
   The configuration file must be an XML file.

5. Click **Save**.
   The CORS configurations are saved for the bucket.

Adding Tags to a Bucket Using Objects Browser

A tag is a label that you assign to a bucket, and it consists of a key and a value pair that you can define. You can add or remove tags from your buckets using the Objects Browser.

About this task

To add tags to a bucket from the Objects Browser, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. Click the name of the object store and launch the Objects Browser.
   For information on launching the Objects Browser, see Launching the Objects Browser on page 165.
   The object store opens in a new window.
4. In the **Buckets** table, select the bucket to add tags.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 893

5. Click **Actions** > **Tags**.
   The **Add Tags** window appears.

Figure 122: Add Tag Window

6. To add a new tag, click **+ add tag**.
   The existing tags will be auto-populated. You can click the delete icon to delete a tag.

   Note:

   - The maximum number of tags allowed per bucket is 50.
   - Tag keys can be up to 128 Unicode characters in length, and tag values can be up to 256 Unicode characters in length.
   - Tag keys and values are case-sensitive.
   - Tag key should be unique and is a mandatory field, but tag value is optional.

   A new row appears to fill the key value of the tag.

7. Enter the key and value.

8. Click **Save**.
   The changes are saved.

Object CRUD Operations

You can perform various CRUD operations on the objects within a bucket.

Figure 123: Objects Browser - Object CRUD Operations

The CRUD operations that you can perform on an object are as follows:

- **Upload Objects**: Allows you to upload files, or folders containing multiple files.

  For information on uploading objects and creating new folders, see Uploading an Object Using Objects Browser on page 181.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 894

- **New Folder**: Allows you to create folders to organize and manage your data within a bucket.

  > **Note:** You cannot create new folders in NFS-enabled buckets.

  For information on uploading objects and creating new folders, see Uploading an Object Using Objects Browser on page 181.

- You can use the **Actions** list to download an object, add tags for an object, manage object versions for version-enabled buckets, and delete an object.

  - **Download**: Allows you to download an object.

    To download an object, select the object, and then click **Actions** > **Download**.

    > **Note:** The object is downloaded to the default download folder of your browser. You can also download the object by clicking the name of the object in the objects list.

  - **Copy sharing link**: Allows you to generate a link to the object that you can share with other users.

    To share an object with another user, select the object, and click **Actions** > **Copy sharing link**.

    Other users can directly open the shared object using the link and perform actions depending on the permissions. Users are prompted to log on when they open the link.

  - **Tags**: Allows you to add tags to an object.

    > **Note:** You can add up to 10 tags for an object.

    For more information on adding tags, see Adding Tags to an Object Using Objects Browser on page 183.

  - **Versions**: Allows you to view and manage the different versions of an object. Versioning allows you to revert an earlier version of an object to its latest version.

    On the **Versions** page, you can revert, delete, and download the object versions. For more information, see Understanding Object Versions on page 185.

  - **Delete**: Allows you to delete any object.

    To delete an object, select the object, and then click **Actions** > **Delete**.

    > **Note:** For versioned buckets, the delete operation performed on an object is not permanent and a delete marker is created. You can view the deleted objects, and if needed, retrieve it from the **Recycle Bin**.
    >
    > For non-versioned buckets, the delete operation performed on an object is permanent and cannot be retrieved. Non-versioned buckets do not have a **Recycle Bin**.

- **Search**: You can perform a prefix-based search in the search bar. You can perform the search on the objects list page and the Recycle Bin. You can enter any prefix as a search keyword and the objects

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 895

starting with that keyword will be listed. For example, if you search for the prefix *copy*, all objects whose names start with the keyword *copy* are listed.

You can also search for exact name matches. For example, if you search for the keyword *copy.txt*, the search result is an exact match. It will not search for the keyword starting with the keyword *copy.text*, but will find an exact match.

Note:

- The search you do is limited to the folder that you are working on. For example, if you do a search from within the *BigData* folder, then the search results appear only from the objects in the *BigData* folder, and not from the entire list of objects.
- The search is case-sensitive.

Object Naming Conventions

The object key name is a sequence of UTF-8 characters not exceeding 1024 bytes.

You can use the following characters to create an object key name or prefixes:

- Alphanumeric characters—lowercase letters (a-z), uppercase letters (A-Z), and numbers (0-9)
- Special characters—forward slash (/), exclamation mark (!), hyphen (-), underscore (_), period (.), asterisk (*), single quote ('), open parenthesis ((), and close parenthesis ())

Consider the following limitations before you create an object key name:

- Only the UTF-8 character set is supported.
- The length of the object key name cannot exceed 1024 bytes.
- Special characters, such as pound (#) and percent (%) are not supported.

Note: The following restrictions apply to the object key names:

Uploading an Object Using Objects Browser

After creating a bucket, you can use the Objects Browser to select and upload files or folders to a bucket.

About this task

To upload files or folders to a bucket, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. Click the name of the object store in which you want to create a bucket and launch the Objects Browser.
   For information on launching the Objects Browser, see Launching the Objects Browser on page 165.
   The object store opens in a new window.
4. Click the bucket name to which you want to upload files or folders.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 896

5. (Optional) Click **Upload Objects** > **Select Files** to select and upload a file.
   The **Upload Objects** window appears.

   Note:

   - This page displays the upload progress, the upload status, the bucket name, the object name, the size of the object, and the actions that you can perform on the object. You can also search by object name, bucket name or prefix.
   - Uploading objects is an asynchronous process. If the upload size is large, you can close the **Upload Objects** window and perform other operations in the Object Browser UI. You can check the upload status by clicking the status icon in the top-right corner of the page.
   - Multi-part upload is used to upload large files (more than 1 GB). This feature enables to upload objects of any size to the object store. Depending upon the size of the file, upload may take a few minutes.
   - If you refresh the page using the refresh button of the web browser, logout, or navigate to any non-application URL, any unsaved changes will be lost. This includes any pending or in-progress uploads. A warning message appears if you try to log out or refresh the page while an upload is in progress. Keep the Objects Browser open until the uploads are complete.

Figure 124: Upload Objects Window

   a. Click the **Cancel All Updates** to cancel the updates that are in progress.

   b. Click the **Close** button or the **X** icon, to close the **Upload Objects** window.

6. (Optional) Click **Upload Objects** > **Select Folder** to select and upload a folder and the files in the folder.
   The **Upload Objects** window appears.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 897

7. Click **Create Folder** to create a new folder in the bucket.
   You can create multiple folders to organize the objects in a bucket.

   Note:

   - **Create New Folder** feature is not supported in NFS-enabled buckets.
   - The objects within the folders is listed in the Recycle Bin with the folder name. For example, if *object1.txt* is in the folder *BigData*, then the deleted object listed in the Recycle Bin will be displayed as *BigData/object1.txt*.
   - When you create a folder, Objects Browser creates a 0-byte object using the folder name you specified followed by a slash (/).

8. (Optional) Click **Summary** to view the bucket summary.

What to do next

After you upload objects to the bucket, you can add a tag to an object, download an object, view and manage the versions of an object, and also delete an object. For more information, see:

- Object CRUD Operations on page 179
- Adding Tags to an Object Using Objects Browser on page 183
- Understanding Object Versions on page 185
- Deleting an Object Using the Objects Browser on page 184

Adding Tags to an Object Using Objects Browser

You can use the Objects Browser to add tags to an object in a bucket.

About this task

To add tags to an object, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. Click the name of the object store and launch the Objects Browser.
   For information on launching the Objects Browser, see Launching the Objects Browser on page 165.
   The object store opens in a new window.
4. Click the bucket name that contains the object.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 898

5. To tag an object, select the object that you need to tag, and click **Actions** > **Tags**.
   The **Add Tags** window appears.

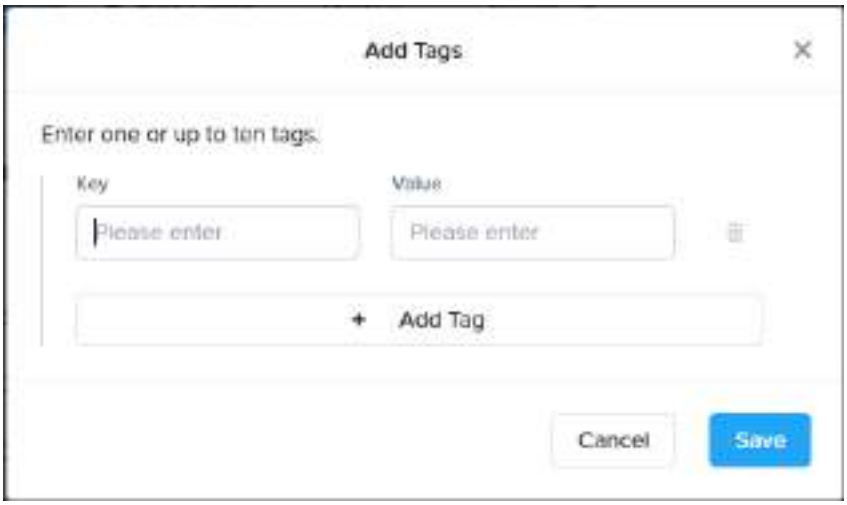


Figure 125: Adding Tags

   a. Enter the key and value pair.

   b. Click **Add Tag** to add more tags.

> **Note:** You can add up to 10 tags for an object.
>
> Click the delete icon against a key-value pair to delete it.

   c. Click **Save**.

What to do next

You can perform other object-related tasks, such as uploading objects, managing versions, and deleting an object. For more information, see:

- Object CRUD Operations on page 179
- Understanding Object Versions on page 185
- Deleting an Object Using the Objects Browser on page 184

Deleting an Object Using the Objects Browser

You can use the Objects Browser to delete objects in a bucket that you do not need.

About this task

To delete objects from a bucket, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 899

3. Click the name of the object store and launch the Objects Browser.
   For information on launching the Objects Browser, see Launching the Objects Browser on page 165.
   The object store opens in a new window.
4. Click the bucket name that contains the object.
5. Select the objects that you need to delete, and click **Actions** > **Delete**.
6. Click **Confirm**, to confirm deletion of the objects.

   Note:

   - For non-versioned buckets, the delete operation performed on any object is permanent and cannot be reverted. The Recycle Bin is not available for non-versioned buckets.
   - For versioned buckets, the delete operation performed on any object is not permanent and a delete marker is created. The deleted objects can be viewed and recovered from the Recycle Bin.

7. Click **Recycle Bin**, select the objects to be deleted permanently, and then click **Delete Permanently**.

Figure 126: Delete Objects

Note:

- This action permanently deletes all versions of the selected objects. You cannot recover the deleted objects after you perform this operation.
- Any new version added to an object that is currently being deleted, gets automatically deleted.

What to do next

You can perform other object-related tasks, such as uploading objects and folders, managing versions, and adding tags to an object. For more information, see:

- Object CRUD Operations on page 179
- Understanding Object Versions on page 185
- Adding Tags to an Object Using Objects Browser on page 183

Understanding Object Versions

Versions allow you to view and manage the different versions of an object. From the **Versions** page, you can revert, delete, and download the different versions of an object. These options are available only for version-enabled buckets.

For more information about versions, see Object Versioning.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 900

For more information about managing object versions, see Managing Object Versions Using Objects Browser on page 186.

When you delete a version-enabled object from the **Bucket** page, it is removed from the objects list and moved to the **Recycle Bin**.

To view the latest version of an object, click the object name, and then click **View all versions**. The latest version is listed with a **Delete Marker** banner in the **Recycle Bin**.

You can permanently delete any version by selecting the object version, and then by clicking the **Delete** button. You can also permanently delete the selected objects including all its versions from the **Recycle Bin**. Select the objects, and then click **Delete Permanently**.

Note:

- Selection of objects is limited to a page-by-page basis. If you select all objects listed in the Recycle Bin, all the objects listed on the first page are deleted. For example, if the total number of objects in the Recycle Bin is 150, but the first page has 100 objects listed, then the 100 objects are deleted.
- For the selected objects, if any new version is added while the deletion is in progress, that version is also deleted.

To restore (revert) this object to any previous version, select the object, and then click **View all versions**. Select the version of the object, and then click **Revert**. Now, the reverted version is the latest version visible in the objects list. You can also select the latest delete marker and delete it to restore the object to the last version.

Figure 127: Managing Object Versions - Using Objects Browser

Note: Versions with *a Delete Marker* banner can only be deleted permanently. After deletion, they cannot be reverted or downloaded.

Managing Object Versions Using Objects Browser

You can use the Objects Browser to view and manage the versions of an object. Version allows you to revert an earlier version of an object to its latest version. You can also delete or download any version of the object.

About this task

To manage objects versions, do the following:

Procedure

1. Log on to the Prism Central web console.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 901

2. In the Application Switcher, click **Objects**.
3. Click the name of the object store and launch the Objects Browser.
   For information on launching the Objects Browser, see Launching the Objects Browser on page 165.
   The object store opens in a new window.
4. Click the bucket name that contains the object.
5. Select the objects whose version you need to manage, and click **Actions** > **Versions**.

Figure 128: Objects Versions

Note: The latest version of an object is indicated by appending the banner `Latest` appended to the object name.

6. (Optional) Select a version that you need to revert as the latest version, and click **Revert**.

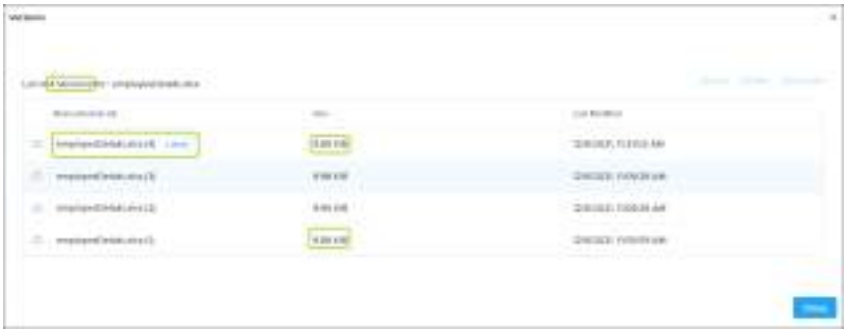


Figure 129: Revert Version

The above image depicts an example, where `employeeDetails.xlsx (1)` is reverted to the latest version indicated by `employeeDetails.xlsx (4)` [Latest].

Note:

- Using the revert feature, you can designate any earlier version of an object as its latest version.
- If you deleted an object from the **Buckets** page, where all the objects within the bucket are listed. On the **Versions** page, you can select a version that does not have the Delete Marker banner, and then click **Revert**. The object gets restored on the **Bucket** page.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 902

7. (Optional) Select a version of the object that you need to delete, and click **Delete**.
   This action permanently deletes the selected version of the object.
8. (Optional) Select a version of the object that you need to download, and click **Download**.
   You cannot download the object version that is marked with a `Delete Marker` banner. The object is downloaded to the default download folder of your browser.
9. Click **Close** or the **X** icon, to close the window.

Bucket Summary

The Summary page allows you to view the list of various policies applied to the bucket.

To view the **Summary** page of a bucket in an object store, click the name of the bucket in the buckets table, and then click **Summary**.

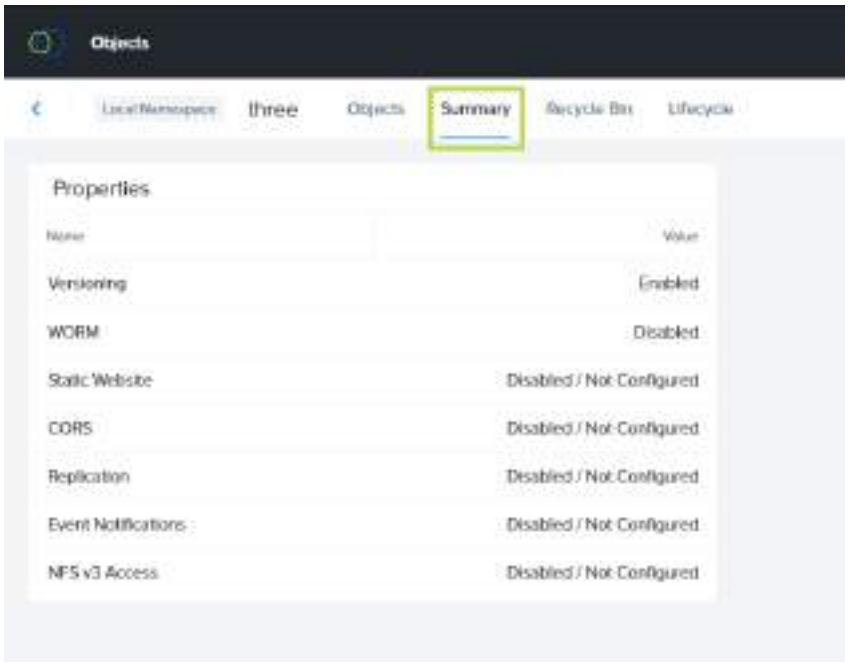


Figure 130: Objects Browser - Bucket Summary Page

OBJECTS STREAMING REPLICATION

Objects streaming replication enables automatic and asynchronous copying of source buckets to the target buckets in different Objects instances.

You can now create up to three replication rules. This provides you with the ability to replicate a single source bucket to a maximum of three destination buckets. These destination buckets can be on the same PC cluster or on a remote PC cluster.

For version-enabled buckets, you can also replicate the delete markers to a destination bucket.

> **Note:** Objects streaming replication is only supported for buckets created using the S3 protocol.

Objects streaming replication helps you with the following:

- Maintain another copy of data for disaster recovery.
- Maintain another copy of data at different sites for local access. This helps to minimize latency in accessing data.

Points To Remember

Note the following points about Objects streaming replication.

- The source and target buckets must belong to different Objects instances.
- The Objects instances can be within the same Prism Central (PC) or different PCs.
- If the Objects instances belong to different PC clusters, a trust has to be set up between the PC clusters by adding each other as Availability Zones.

  Availability Zone - A physically isolated site where you can replicate the data that you want to protect. An instance of Prism Central represents an availability zone.
- For replication-enabled buckets, versioning, and WORM modifications are prevented.
- Objects streaming replication between buckets relies on the connection (for example, a secure VPN connection) for encryption.
- Network Address Translation (NAT) performed by any device in between the two Objects instances is not currently supported.
- Proxy between Objects instances is not supported.

Types of Replication

There are two types of bucket replication.

Objects instances within the same PC

Replicating a bucket to an Objects instance within the same PC involves the single step of creating a replication rule.

Objects instances within different PC instances

Replicates buckets to an Objects instance within a different PC. This involves three steps.

- Step 1 - Adding the remote PC clusters as an availability zone.
- Step 2 - Performing IAM synchronization between the source PC cluster and remote PC clusters.
- Step 3 - Creating a replication rule.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 904

After you set up the replication rule between the source and destination bucket, you can track the replication statistics for each bucket. For more information, see Viewing Replication Statistics for a Bucket.

Replication Guarantees and Topologies

Refer to this section to understand the replication guarantees, how replication works, and supported replication topologies.

Replication Guarantees

The following object attributes get replicated:

- Object operations—Object PUT, Object Copy, Updates (PutTags, PutObjectLock), and Deletes.
- Object metadata—ETag, create and modification time and lock property.
- Version numbers, User metadata, and Tags.

> **Note:** Source and destination buckets are independently managed and not replicated. Also, any changes to the bucket policies (for example, access- or lifecycle policies) do not get replicated.

How Replication Works

Note the following points about how the Objects streaming replication works:

- Replication starts as soon as the object gets written on the source bucket.
- The replication completion time may vary depending on the object size and other factors such as available bandwidth, number of replications, and so on.
- Objects replications may not strictly follow the same time order in which they get written on the source bucket.
- Replication of the versions of an object may not happen in sequential order, but they get replicated eventually.

Replication Topology

> **Note:** Note the following points:
>
> - Ensure that applications do not perform conflicting write operations (objects with the same name) on the remote bucket while replication is enabled.
> - There are no restrictions on the I/O operations performed on the remote bucket. You can perform read-and-write operations on a remote bucket.
> - For an N:1 replication relation, a bucket can have a maximum of five inbound relationships. For example, Bucket A can be the destination bucket for a maximum of five source buckets.
> - For a 1:N replication relation, a bucket can have a maximum of three outbound relationships. For example, Bucket A can be the source bucket for a maximum of three destination buckets.

The following are the topologies that you can use for your replication scenarios:

Single-Replication Relation

In this topology, you replicate objects one way from the source to the destination.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 905

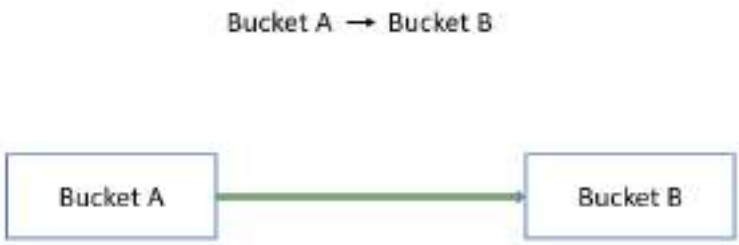


Figure 131: Single Replication - Unidirectional

Different buckets on the source Objects instance can replicate to buckets belonging to different Objects instances.

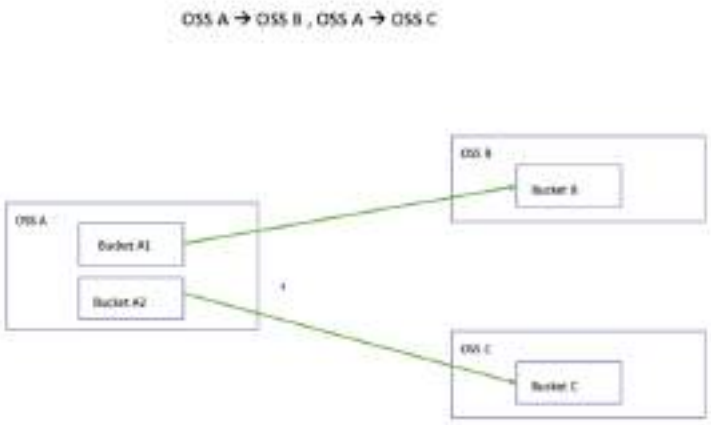


Figure 132: Single Replication - Different Objects Instances

Bidirectional Replication Relation

In this topology, you can set up a bidirectional-replication relation between a pair of buckets. Objects written on one side get replicated on the other side.

Independent replication relations between the buckets have to be created, that is, create a replication rule with Bucket A as the source and Bucket B as the destination and the other way around.

> **Note:** Ensure that the application does not write conflicting objects (objects with the same name) on both buckets while replication is enabled.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 906

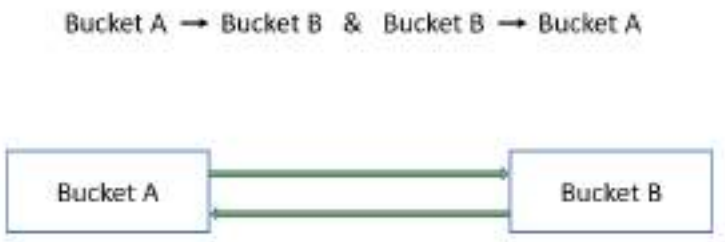


Figure 133: Bidirectional Replication

Chain Replication Relation

In this topology, objects from Bucket A can be replicated to Bucket B, and objects that originated in Bucket B can be replicated to Bucket C.

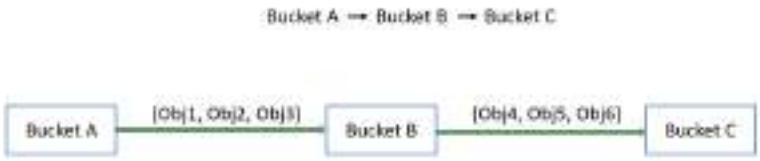


Figure 134: Chain Replication

N:1 Replication Relation

In this topology, a bucket can be a destination to many source buckets.

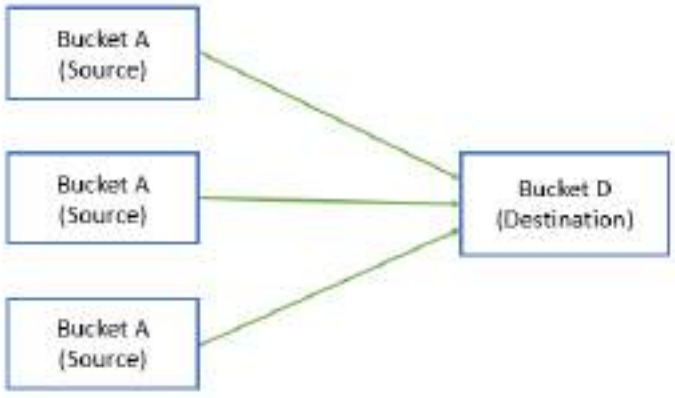


Figure 135: N:1 Replication

1:N Replication Relation

In this topology, a source bucket can replicate to a maximum of three destination buckets. You can have a maximum of three rules in this topology. By default, the priority of replication on all three destination buckets is equal.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 907

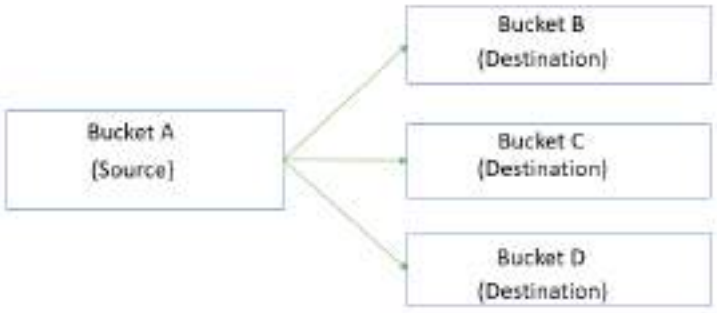


Figure 136: 1:N Replication

Replication Prerequisites

This section lists the prerequisites for bucket replication.

The prerequisites for replicating buckets are as follows:

- Object instances that contain the source and destination buckets must be deployed with Objects version 3.0 or later.
- For *Objects instances within different PC instances* replication, ensure to deploy Objects instances with IAM users if you want the same users to have access to the replicated objects.
- For *Objects instances within different PC instances* replication, you should establish a secure VPN connection between the PC clusters. For *Objects instances within the same PC* replication, you should establish a secure VPN connection between the clusters (PE).
- For IAM pairing, ensure that both Prism Centrals have either IAM-HA enabled or disabled.
- Ensure that the traffic to port 7100 on the load balancers of the Objects instances is allowed by the firewall for replication purposes.

Adding Remote Prism Central as Availability Zone

For *Objects instances within different PC instances* replication, you need to add the remote PC clusters as an Availability Zone (AZ) on the source PC cluster to establish a secure connection.

About this task

To add the remote PC as an availability zone, do the following:

Procedure

1. Log on to the Prism Central web console.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 908

2. In the Application Switcher, select **Infrastructure** > **Administration** > **Availability Zones**.

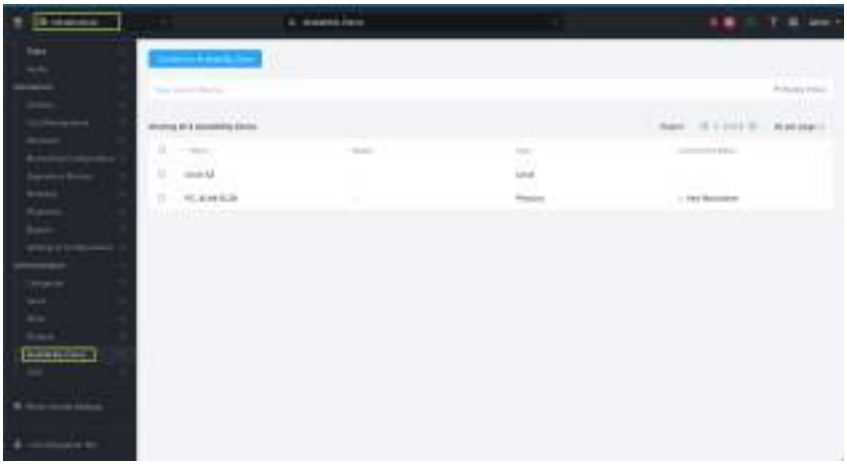


Figure 137: Administration - Availability Zones Page

3. Click **Connect to Availability Zone**.
4. In the **Availability Zone Type** list, click **Physical Location**.

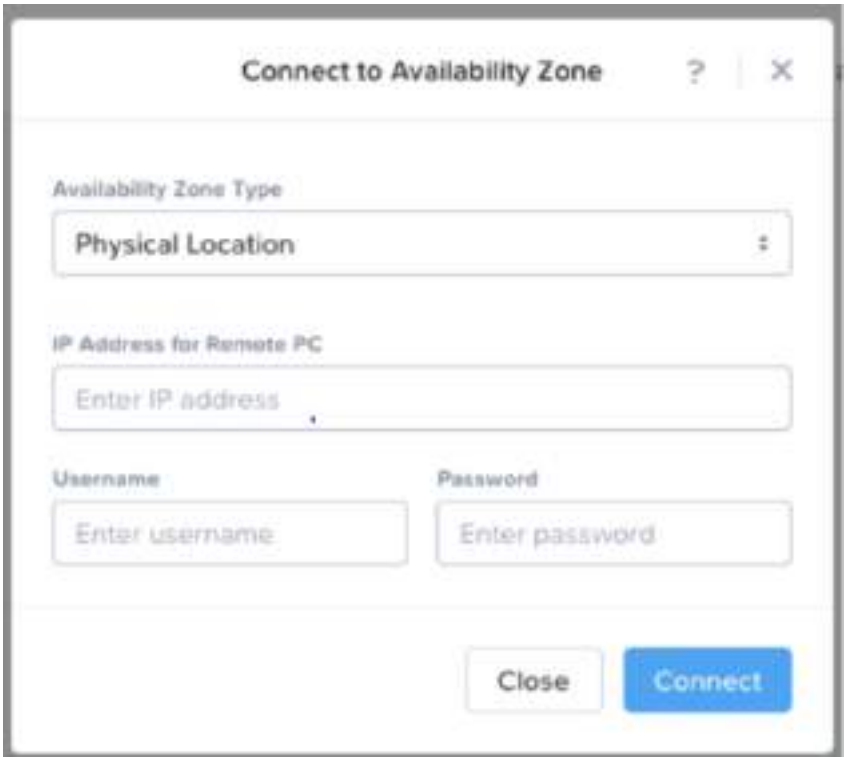


Figure 138: Add an Availability Zone

5. Enter the IP address and login credentials of the remote PC in the corresponding boxes.
6. Click **Connect**.
   The remote PC gets added as an AZ in the source PC and the connectivity status is shown as **Reachable**.

Setting up IAM Synchronization with a Different PC

To replicate Objects on a different Prism Central (PC), you must perform IAM synchronization of the source PC with the corresponding remote PC. The IAM users of the source Objects instance get replicated to the destination Objects instance belonging to a different PC with the same access key and secret key pair. The admin or bucket owner needs to provide permission to the users for the replicated buckets.

Before you begin

A non-admin user can set up IAM synchronization with a different Prism Central only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions:

- Create an Object Store
- View Object Store

Note: Administrators and non-admin users are Prism Central users with the following roles:

- Administrator—A Super Admin or a Prism Admin in Prism Central.
- Non-admin user—A Prism Central user without any administrator privileges.

For more information about the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.

Note: IAM pairing works only if both source and target Prism Centrals have either IAM-HA enabled or disabled.

About this task

To perform the IAM pairing, do the following:

Procedure

1. Log on to the source Prism Central web console.
2. In the Application Switcher, click **Admin Center** > **IAM** .
3. Click the **Access Keys** tab.
4. Click **IAM Replication Settings**, and then click **Add IAM Pairing**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 910

5. In the **Target Prism Central** list, select the remote PC that you added as an Availability Zone (AZ) in the source PC.

   Note:

   - Only the PCs added in **Administration** > **Availability Zones** appear in this list.
   - The target Prism Central IAM must have all the Active Directory configured in this source Prism Central IAM.

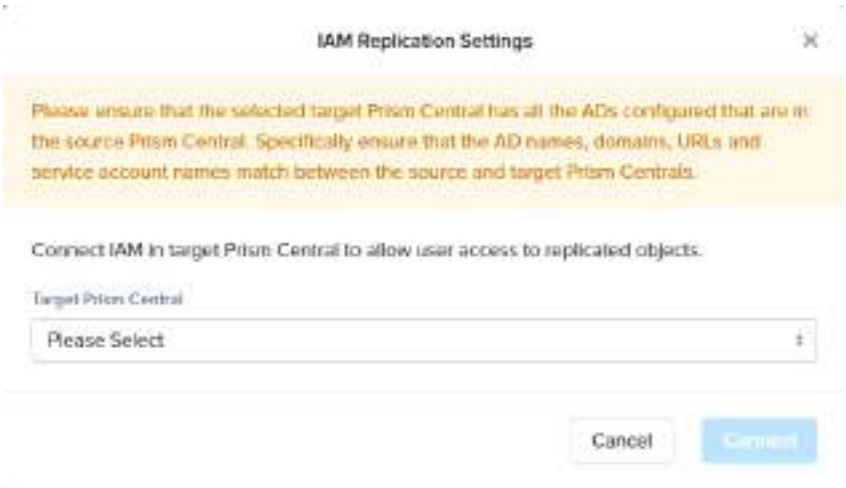


Figure 139: Add IAM Pairing

6. Click **Connect** to complete the pairing.

   Note: You cannot add more than five IAM replication targets.

   After you click **Connect**, all existing users get replicated to the target Prism Central IAM. You can monitor the progress of the replication on the **IAM Replication Settings** page. Once the IAM pairing is complete, all the future users and keys that are created and deleted get replicated to the target Prism Central IAM.

   If any of the replication fails, go to the **IAM Replication Settings** page and click **Sync** to replicate any unreplicated users to the target Prism Central. The administrators can view the users for whom the replication failed and use the export option to download the list of errors.

   Note: The **Sync** option will not replicate a user or a key deletion. For a failed replication for delete operations, you must log on to the target Prism Central and delete the unwanted users and keys.

Figure 140: IAM Replication - Sync Option

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 911

Prerequisites for Creating a Replication Rule

Before you create a replication rule, make sure that the following prerequisites are fulfilled.

- In the case of remote-PC cluster replication, ensure that the Fully Qualified Domain Name (FQDN) of the object store instances in two different PC clusters is different.
- If you plan to replicate data to a bucket on a different PC, ensure that you perform IAM synchronization of the source PC with the corresponding remote PC.
- Bucket access permissions are not automatically replicated to the destination bucket. You need to manually assign them to the destination bucket.
- Lifecycle policies are not replicated and can be assigned independently on the source and the destination buckets.
- If you are replicating a bucket created in Object v3.1 (with the legal hold applied) to a bucket created in Objects v3.0, the legal hold attributes will not get replicated.
- Versioning, WORM state, and WORM retention period must be the same between the source and destination buckets.
- Only objects added to the buckets or modified after the replication rule has been created will be transferred to the destination bucket.
- For replication-enabled buckets, versioning, and WORM modifications are prevented. To make changes, you need to delete the replication rule, perform the required edits on the buckets, and again create the replication rule.
- When creating a replication rule for buckets in different object store instances, ensure that the first relationship to the object store containing the destination bucket is created using the Prism GUI. For example, create a rule for Bucket 2 in object store A with Bucket 6 in object store B as the destination using the GUI. For successive replication rules for any buckets in object store A to any other bucket in object store B, you can use the GUI or S3 API.

A non-admin user can create replication rules between buckets only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions and the non-admin user must be assigned to specific objects instances:

- Edit Buckets
- View Buckets
- View Object Store

Note:

- Administrators and non-admin users are Prism Central users with the following roles:
  - Administrator—A Super Admin or a Prism Admin in Prism Central.
  - Non-admin user—A Prism Central user without any administrator privileges.

  For more information on the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.
- Users with Edit Buckets permission can configure bucket replication on all the buckets on an assigned object store.

If the target object store is on the same Prism Central, then the user must have View Object Store access to the target object store also. If the target Object store is on a different Prism Central, then the user will be able to select any object store on the target Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 912

Creating Replication Rules for Buckets

You can create a replication rule for buckets that allows you to replicate data in a bucket to other buckets. You can replicate the data to a destination bucket in the same PC or in a remote PC.

Before you begin

Ensure that the prerequisites for creating a replication rule are met. For more information, see Prerequisites for Creating a Replication Rule on page 197

About this task

To create a replication rule for buckets, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the object store which stores the bucket.
   The object store opens in a new window.
4. Click the **Buckets** tab, and then from the buckets list table, select the source bucket.
5. Click **Actions** > **Replication Rules**.

Figure 141: Replication Rules

The **Replication** page appears.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 913

6. Click **Create Rule**.
   The **Create Replication Rule** page appears.

Figure 142: Create Replication Rule Page

7. Enter the following details:

   a. **Prism Central**: Select a namespace to replicate the Object.
      You can replicate the bucket on the same PC cluster or on a remote PC cluster.

      - You can select **Local AZ** to replicate the source bucket to a destination bucket on the same PC cluster.
      - You can select a remote PC from the **Prism Central** list to replicate your bucket to a destination bucket on the remote PC cluster.

   b. **Object Store**: Select the Objects instance that contains the destination bucket.

   c. **Bucket**: Enter the name of the destination bucket.

   d. (Optional) Select the **Replicate delete operations** check box to replicate delete markers to the destination bucket.

      Note:

      - Selecting the **Replicate delete operations** check box enables the `DeleteMarkerReplication` parameter and replicates delete markers to the destination bucket.
      - The `DeleteMarkerReplication` status now appears in the Objects user interface. You can also find the `DeleteMarkerReplication` status using S3 API. The

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 914

relations created using Objects versions earlier than Objects 3.5 return the correct `DeleteMarkerReplication` enabled status.

- Set `DeleteMarkerReplication` as `Disabled` when you create a replication relationship. This will ensure that the replicated objects are not deleted from the destination bucket when the corresponding object is deleted from the source bucket.

  However, if objects that are pending replication are deleted from the source, these objects will not be replicated to the destination bucket. Hence, the object will not be available on the destination bucket.
- You can create a maximum of three rules for the 1:N replication.
- For more information on the replication scenarios, see Objects Streaming Replication Scenarios on page 200.

8. Click **Save** to create the replication rule.

   The replication rule between the buckets is established. The replication time might vary and depends on various factors, such as object size, workloads on the objects cluster, and so on. This replication rule is applied to all the new objects uploaded after this rule is created.

   For more information about replication alerts, see Nutanix Objects Specific Alerts on page 219.

   Notes on disconnected Availability Zones

   If you remove a Prism Central from the Availability Zones after setting up the IAM synchronization and bucket replication:

   - Successive IAM user additions and deletions are not replicated.
   - Existing bucket replication is not affected. However, you will not be able to create new replication rules to the Objects Store deployed in the disconnected availability zone.

   You can select the destination bucket and click **View** on the **Replication** page to view the replication rule details.

   You can also view the overview or statistics of the replication rule by clicking the **Overview** tab. See Viewing Bucket Replication Statistics on page 201.

What to do next

You can also delete a replication rule. For more information, refer to Deleting a Replication Relation on page 201

Objects Streaming Replication Scenarios

This section describes the application behavior in a few replication scenarios.

Unidirectional Replication

DeleteMarkerReplication is enabled:

- Non-versioned bucket—Delete operation is replicated to the destination bucket.
- Versioned bucket—Delete marker is replicated to the destination bucket.

DeleteMarkerReplication is disabled:

- Non-versioned bucket—Delete operation is not replicated to the destination bucket.
- Versioned bucket—Delete marker is not replicated to the destination bucket.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 915

Deleting a Replication Relation

This section provides the steps to delete a replication relation.

About this task

A typical scenario where you may require to delete a replication rule is if you want to modify the versioning and WORM state of a replication-enabled bucket. Since versioning and WORM changes are prevented, you need to delete the replication rule, perform the required edits on the bucket, and then create the replication rule again.

> **Note:** Deleting a replication relation would cause all pending replications for that relationship to be dropped immediately. It is recommended to wait for the pending replications to complete, then start making changes by deleting the relation.

To delete a replication rule for a bucket, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. Click the name of the object store where the bucket is deployed.
   The object store opens on a new window. You can view the list of buckets in the Objects instance.
4. From the **Buckets** table, select the replication-enabled bucket.
5. Click **Actions** > **Replication Rules**.

Figure 143: Replication Rules

   The **Replication** page appears.

6. In the **Replication Rule** table, select the replication destination bucket.
7. Click **Delete**.
   After the replication rule is deleted, new objects are not replicated to the destination bucket.

Viewing Bucket Replication Statistics

This section describes the steps to view the replication statistics, such as the replication properties and the average bandwidth for a bucket.

Before you begin

A non-admin user can view replication statistics only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions and the non-admin user must be assigned to specific objects instances:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 916

- View Buckets
- View Object Store

Note:

- Administrators and non-admin users are Prism Central users with the following roles:
  - Administrator—A Super Admin or a Prism Admin in Prism Central.
  - Non-admin user—A Prism Central user without any administrator privileges.

  For more information on the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.
- Users with View Buckets permission can view the replication statistics on all the buckets on an assigned object store.

About this task

To view the replication statistics, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the object store which stores the bucket.
   The object store opens in a new window.
4. Click the **Buckets** tab, and then from the Buckets list table, select the replication-enabled bucket.
5. Click **Actions** > **Replication Rules**.
   The **Replication** page appears.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 917

6. Click the **Overview** tab.
   The replication properties and the average bandwidth appears on the **Overview** page.

Figure 144: View Replication Overview

If the bucket has both inbound and outbound traffic, you can select either of the traffic types from the **Traffic Type** list and then select the corresponding source or destination bucket.

- **Outbound from this bucket**—Shows the statistics for replication of objects from the selected bucket (source) to the destination bucket.
- **Inbound to this bucket**—The selected bucket can be a destination to many source buckets. Inbound statistics show the data for the replication of objects to the selected bucket. You can select the source bucket and view the inbound statistics from that bucket.

  > **Note:** The updates to the destination bucket happen periodically. This might result in a lag in the destination bucket statistics display.

- **Destination Bucket**—The destination bucket for replication.
- **Destination Bucket Object Store**—The name of the object store that contains the destination bucket.
- **Last replication point**—Point-in-time up to which all the objects created on the source bucket have been replicated.
- **Number of objects pending replication**—Object count pending replication.
- **Objects size pending replication**—Total amount of data pending replication.
- **Average bandwidth**—The rate of the amount of data transferred from the source to the destination. For inbound relationships, the average bandwidth is the cumulative value of all the incoming data from the source buckets. The bandwidth graph helps you to visualize the progress of the replication.

What to do next

You can create more replication rules for buckets. For more information, refer to Creating Replication Rules for Buckets on page 198.

Achieving Fault Tolerance for IAM

This section describes how you can use IAM replication and bucket replication to withstand data center failures.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 918

Note: This section is applicable only if IAM-HA is not enabled. For more information, see Objects IAM-High Availability Overview on page 106.

IAM Service on Objects

At present, all the Object Stores (Objects instance) in the same PC share a single IAM. This IAM instance resides in the first object store (primary) that is deployed in the PC. If that primary object store becomes unavailable, the IAM service will not be available for all secondary object stores of that PC.

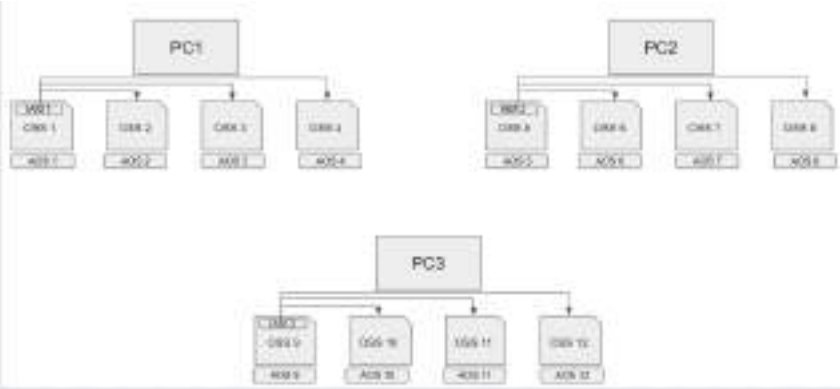


Figure 145: IAM Service on Objects

For example, you have one PC managing all your clusters that is *PC1*. This *PC1* has four object stores (OSS 1, 2, 3 and 4). However, *IAM 1* resides only in the first object store *OSS 1* (primary object store). All other secondary object stores on that PC (OSS 2, 3 and 4) are for back up of *OSS 1* and relies on *IAM 1* for authentication. If *OSS 1* goes down, then all other back ups also goes down. In this case, Nutanix recommends you the following IAM replication configuration.

Note: The Objects cluster will work even when the PC fails.

Recommended IAM Replication Configurations

Nutanix recommends to transition to multiple PC, that is multiple IAM solution for achieving fault tolerance for IAM replication. You can have one or more PCs to manage IAM replication. The remote PC can have different object stores, and you can set up IAM replication between primary PC and remote PC.

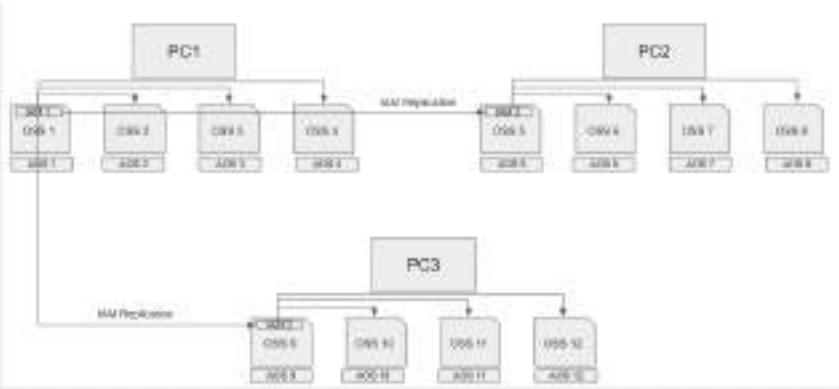


Figure 146: Objects IAM Service with Replication across Prism Centrals

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 919

For example, in the preceding image, you have three PCs managing all your clusters that is *PC1*, *PC2*, and *PC3*. *PC1* has four object stores (OSS 1, 2, 3 and 4) with *IAM 1* residing only in the first object store *OSS 1* (primary object store). All other secondary object stores on that PC (OSS 2, 3 and 4) relies on *IAM 1* for authentication.

Similary, *PC2* and *PC3* have different object stores respectively (OSS 5, 6, 7, 8 and OSS 9, 10, 11, 12) with *IAM 2* and *IAM 3* residing only in the first object stores *OSS 5* and *OSS 9* (primary object stores) of *PC2* and *PC3*.

Now as recommended, you use *PC2* and *PC3* for replication of *PC1*. In this case, even if any object store in *PC1* goes down, then replicated buckets will be available in *PC2* and *PC3* without any disruption.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 920

BASELINE REPLICATOR TOOL

Baseline Replicator tool is a tool with which you can replicate existing objects in your bucket to a bucket at a remote site. You can use this tool only after a replication relationship is created with the destination bucket. You need to first identify the destination bucket, and then run this tool against the source bucket.

The Baseline Replicator tool performs the following operations:

- Lists objects in the source bucket.
- Touches meta-data of each object on the bucket so that it gets set up for native replication.

Note:

- This tool does not replicate the objects to the destination bucket. Instead, it sets up the objects for replication and expects the native replication protocol to replicate it over to the destination bucket.
- You cannot replicate an object from the source bucket if an object with the same name already exists on the destination bucket.
- Baseline replicator tool can be used to replicate up to 100 million objects in a single bucket.
- When baseline replication is set up between two versioned buckets, all the versioned objects will be replicated over to the destination bucket. However, the delete markers from the source bucket are not replicated over to the destination bucket.

Accessing and Running the Baseline Replicator Tool

Prism Central admin users can access this tool inside the Service Manager pod (aoss_service_manager) in the Prism Central. Copy the tool from the Service Manager pod to a temporary folder on the Prism Central VM or the Linux VM. You can also download the Baseline Replicator tool from the Nutanix Support Portal in your Linux VM or the Prism Central VM.

Before you begin

Ensure that you conform to the following requirements before running this tool:

- Your machine should have connectivity with the object store (endpoint URL) hosting the source bucket.
- You have a valid secret key and access key.
- User must have read-write access to the bucket.

About this task

To run the Baseline Replicator tool, do the following:

Procedure

1. SSH into the Prism Central VM or the Linux VM where the tool is present.
2. Copy the tool from the Service Manager pod and paste it in any folder, or download the tool from Nutanix Support Portal and paste it to any folder.

```
nutanix@pcvm$ docker cp aoss_service_manager:/svc/bin/baseline_replicator /tmp/
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 921

3. (Optional) To see the usage of the tool, run `nutanix@pcvm$ /tmp/baseline_replicator`.

   The Baseline Replicator tool has the following parameters:

   - source_bucket_name: Name of the source bucket.
   - source_endpoint_url: Endpoint URL of the object store hosting the bucket.
   - source_access_key: Access key of the source bucket.
   - source_secret_key: Secret key of the source bucket.
   - region_name: Specify the region name.
   - keys_prefix: Choose which objects to replicate by giving a prefix. For example, `ntnx` is the keys prefix, then only the objects with the prefix `ntnx` will be scheduled for replication.
   - start_key: If any interruption occurs while replicating, provide the start_key to resume the replication from that object.
   - log_path: Provide the path if you want to save the log in a specific location.
   - max_concurrency: Specify how many concurrent operations you want the tool to perform. Default concurrency is 50. You can increase the number based on the resources of the VM where the tool is running.
   - skip_prelim_test: When the tool is run, a preliminary test is run. If you want to skip the prechecks, use this --skip_prelim_test parameter.
   - log_level: Specify the levels of the logs you want to display, such as Debug, Info, Warn, Error, Fatal in order of decreasing verbosity.
   - resume: Use this option if the tool was stopped abruptly. You can run the tool again with --resume, and the tool takes care of identifying the last object that was setup for replication and provides that as the start_key.

   The following output appears with the usage details.

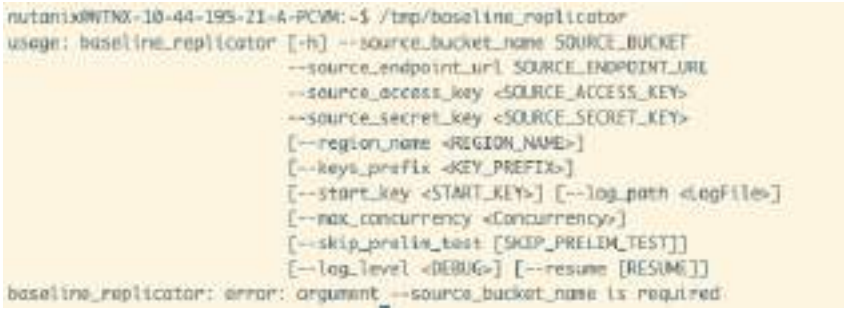


Figure 147: Baseline Replicator Usage

Here `tmp` is the folder name where the tool is copied.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 922

4. Run the Baseline Replicator tool.

```
nutanix@pcvm$ /tmp/baseline_replicator --source_endpoint_url=source-endpoint-
url --source_bucket_name=bucket-name --source_access_key=source-access-key --
source_secret_key=source-secret-key --max_concurrency=concurrency
```

For example,

```
nutanix@pcvm$ /tmp/baseline_replicator --source_endpoint_url=http://10.45.28.101 --
source_bucket_name=1million --source_access_key=v0cfi3kRMBv0cfi3kRMBv0cfi3kRMBz --
source_secret_key=NTY7_Xok_UEYOvz-Y9zdkVs_koV-YrMa --max_concurrency=200
```

If you lose connectivity or any interruption occurs, all objects may not get tagged for replication. In that case, you can check the logs to find the last object that was successfully setup for replication. You can then restart the replication by providing the start key parameter (start_key) to resume the replication from that object. Alternatively, you can restart the script by running the same command but with an additional --resume parameter.

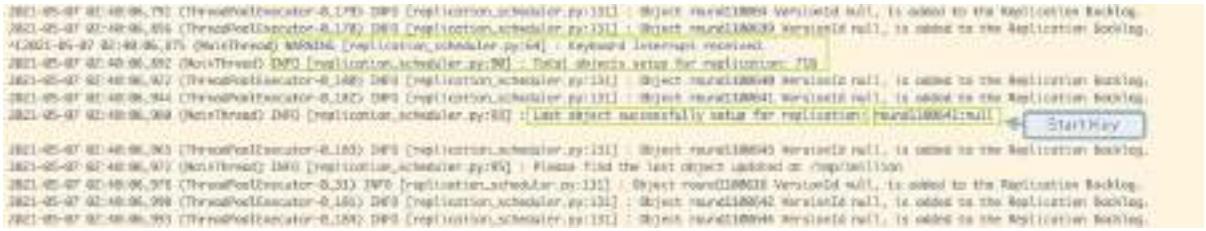


Figure 148: Checking Logs for Start Key

For example,

```
nutanix@pcvm$ /tmp/baseline_replicator --source_endpoint_url=http://10.45.28.101 --
source_bucket_name=1million --source_access_key=v0cfi3kRMBv0cfi3kRMBv0cfi3kRMBz --
source_secret_key=NTY7_Xok_UEYOvz-Y9zdkVs_koV-YrMa --start_key=round1100641:null --
max_concurrency=200 --resume
```

You can check the logs to find the last object that was set up for replication. Go to `/tmp/bucket-name` to find the logs.

> **Note:** The Baseline Replicator tool might fail when used against an HTTPS endpoint.
>
> `[SSL: CERTIFICATE_VERIFY_FAILED]certificate verify failed`
>
> This is because the Botocore library validates the certificate using a CA certificate.

For the library to successfully validate the CA certificate should be downloaded and placed on the system from which the tool is run.

a. Download the CA certificate from the Objects landing page on PC.

b. Select the intended objects instance, Click **Actions**, **Manage FQDNs & SSL Certificates**, and **Download CA Certificate**.

c. Copy the CA certificate onto the system from which the tool is run.

d. Set the following environment variable before running the tool:

```
nutanix@pcvm$ export AWS_CA_BUNDLE=path to the CA Cert
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 923

OBJECTS PROMETHEUS EXPORTER

The Objects Prometheus Exporter provides a solution for Objects observability. The Objects Prometheus Exporter service runs on Prism Central. Using an external Prometheus server, stats can be periodically retrieved from the exporter service and visualized through Grafana dashboards. You can also use any other observability tools that can import stats in Prometheus format and store and visualize them.

The exporter can be used to monitor the following stats:

- Object stores and buckets stats:
  - Capacity consumed or usage
  - Number of objects
  - Number of buckets
- Performance stats (individual bucket level as well as cumulative object store level): Total requests/sec, GET/sec, PUT/sec, throughput.
- Object store resource consumption stats: CPU and memory consumption for object store services - Object Controller, Metadata service, Atlas, and Load Balancer.

List of stats at bucket level

- nutanix_objectstore_total_object_data_gets
- nutanix_objectstore_object_count
- nutanix_objectstore_total_object_data_puts
- nutanix_objectstore_storage_usage_bytes
- nutanix_objectstore_total_deletes
- nutanix_objectstore_total_batch_deletes
- nutanix_objectstore_total_batch_delete_objects
- nutanix_objectstore_total_batch_delete_with_versions
- nutanix_objectstore_total_delete_with_versions
- nutanix_objectstore_total_heads
- nutanix_objectstore_total_lists
- nutanix_objectstore_total_list_versions
- nutanix_objectstore_total_multipart_lists
- nutanix_objectstore_total_multipart_uploads
- nutanix_objectstore_total_posts
- nutanix_objectstore_total_requests_sec
- nutanix_objectstore_total_select_content_ops
- nutanix_objectstore_total_throughput_in_sec
- nutanix_objectstore_total_throughput_out_sec

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 924

List of stats at object store level

- nutanix_objectstore_total_object_data_gets
- nutanix_objectstore_total_batch_deletes
- nutanix_objectstore_total_batch_delete_objects
- nutanix_objectstore_total_batch_delete_with_versions
- nutanix_objectstore_total_delete_with_versions
- nutanix_objectstore_num_buckets
- nutanix_objectstore_num_objects
- nutanix_objectstore_total_object_data_puts
- nutanix_objectstore_total_deletes
- nutanix_objectstore_total_heads
- nutanix_objectstore_total_lists
- nutanix_objectstore_total_list_versions
- nutanix_objectstore_total_multipart_lists
- nutanix_objectstore_total_multipart_uploads
- nutanix_objectstore_total_posts
- nutanix_objectstore_total_requests_sec
- nutanix_objectstore_total_select_content_ops
- nutanix_objectstore_total_throughput_in_sec
- nutanix_objectstore_total_throughput_out_sec
- nutanix_objectstore_usage_bytes

List of resource stats for services of an object store

CPU and memory usage for Atlas, Object Controller and Metadata Server.

For more information about the integration steps with external Prometheus and Grafana, contact your Nutanix account team for further guidance.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 925

MONITORING AND ALERTS

You can monitor the usage and the performance of object stores and buckets, and you can also view system-generated alerts for Objects.

A non-admin user can view the usage and performance of object stores and buckets, and also view system-generated alerts for objects only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have view object store permission and the non-admin user must be assigned to specific objects instances.

Note: Administrators and non-admin users are Prism Central users with the following roles:

- Administrator—A Super Admin or a Prism Admin in Prism Central.
- Non-admin user—A Prism Central user without any administrator privileges.

For more information about the built-in roles in Prism Central, see *Built-in Role Management* in the *Security Guide*.

Note: For the object counts that are shown at the object store instance level, Nutanix Objects counts each upload of a multipart upload as a separate object until the object is finalized. However, for the object count at the bucket level, Nutanix Objects does not include the upload counts in the objects count since an object is considered uploaded in a bucket only after it is finalized. For example, if you have done a multipart upload of 10 objects (suppose 5 parts of each object), then the multipart count of the objects is shown as 50 in the object store instance level. However, at the bucket level, it is shown as 0 because the objects are not finalized or completely uploaded.

Viewing Performance of Object Stores

You can view and analyze the performance of an object store by placing the cursor anywhere on the horizontal axis to display the value at that time. You can also select the time interval (last 3 hours, last 6 hours, and last 12 hours) from the pull-down list above the graphs.

About this task

To view the performance of an object store, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the object store to view its performance.
   The object store opens in a new window.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 926

4. Click **Performance**.

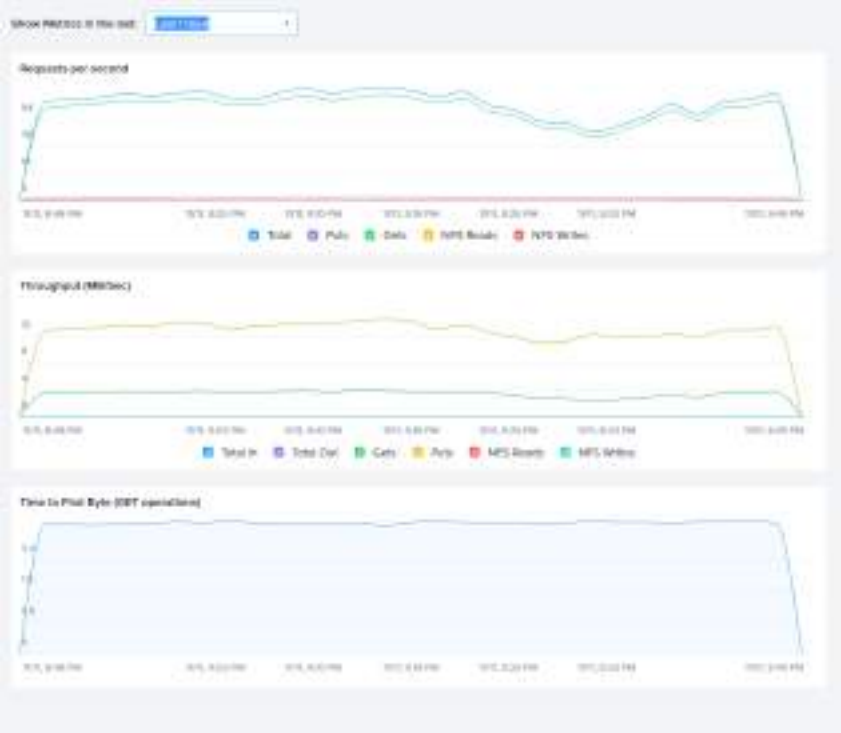


Figure 149: Object Store Performance Graph

The graph shows the following information:

a. **Requests Per Second**: Displays the following graphs:

- The **Total** graph displays the total input and output requests in each second in the object store or bucket.
- The **Puts** graph displays the total input in each second
- The **Gets** graph displays the total output in each second.
- The **NFS Reads** graph displays the total NFS reads in each second.
- The **NFS Writes** graph displays the total NFS writes in each second.

b. **Throughput (MB per sec)**: The Throughput graph displays granular read-and-write throughput in MB in each second.

You can see the total in, total out, gets, puts, NFS reads, and NFS writes in a bucket.

c. **Time to First Byte (GET Operations)**: This graph displays the time taken to read the first byte from the object in milliseconds.

Viewing Performance of Buckets

You can view and analyze the performance of a bucket by placing the cursor anywhere on the horizontal axis to display the value at that time. You can also select the time interval (last 3 hours, last 6 hours, and last 12 hours) from the pull-down list above the graphs.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 927

About this task

> **Note:** The **Throughput** chart shows data for each connection. This data is not the cumulative throughput across all the clients and connections.

To view the performance of a bucket, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the object store to view its performance.
   The object store opens in a new window.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 928

4. Click the **Bucket** tab, and then click the name of the bucket from the Buckets list table, and then click **Performance**.

Figure 150: Bucket Performance Graph

The graph displays the performance of the bucket.

a. **Requests Per Second**: Displays the following graphs:

   - The **Total** graph displays the total input and output requests in each second in the object store or bucket.
   - The **Puts** graph displays the total input in each second
   - The **Gets** graph displays the total output in each second.
   - The **NFS Reads** graph displays the total NFS reads in each second.
   - The **NFS Writes** graph displays the total NFS writes in each second.

b. **Throughput (MB per sec)**: This graph displays granular read-and-write throughput in MB per second.

   You can see the total in, total out, gets, puts, NFS reads, and NFS writes in a bucket.

c. **Time to First Byte (GET Operations)**: This graph displays the time taken to read the first byte from the object in milliseconds.

Viewing Object Store Usage

The Usage tab displays the physical and logical storage usage. You can view the space used across all buckets in an object store.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 929

About this task

To view the object store usage, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the object store to view its usage.
   The object store opens on a new window.
4. Click **Usage** > **Usage Summary**.

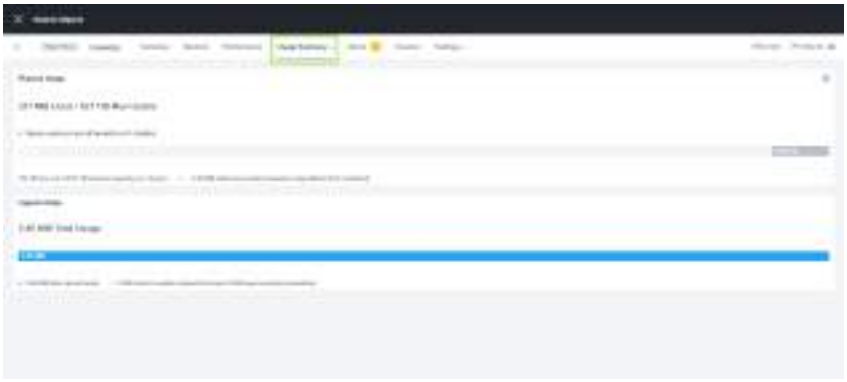


Figure 151: Object Store Usage

The storage usage section displays the following information:

Physical Usage: Displays the physical capacity used by the object store on the cluster.

- Total used and total usable storage for the cluster.
- Space used across all buckets on the existing cluster displayed in a bar.
- Total and free physical capacity of the cluster.
- Logical capacity assigned for the object store.

Logical Usage: Displays the logical capacity used by the object store on the cluster. As the Redundancy Factor is 2 (RF-2), the data is stored in two backups.

- Data stored locally
- Data tiered to another S3 endpoint

Assigning Quota Policy to a User

Assigning a quota policy to a user enables Objects to set soft and hard thresholds on storage limits of all buckets owned by the user and number of buckets created by the user within an object store. You can assign quota policy to multiple users at the same time. If a soft threshold is set and if any user exceeds the limit, they can still create buckets and objects, however an alert is raised in the Alerts page. However, if a hard threshold is set, then the user is restricted from exceeding the limit. For example, if a user has 20 TB storage and has six buckets, then storage for all the six buckets will be accounted. If you are an owner of a bucket and have shared your bucket with multiple users, then your storage quota will be used up even if other users use the shared bucket storage. Quota policies will be automatically removed within 24 hours

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 930

after the user is deleted. If some multi-part operations are pending, those pending parts will count towards the quota.

Before you begin

A non-admin user can assign quota policy to a user only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions:

- Create Quota Policy
- Delete Quota Policy
- View Quota Policy
- View Object Store

> **Note:** Administrators and non-admin users are Prism Central users with the following roles:
>
> - Administrator—A Super Admin or a Prism Admin in Prism Central.
> - Non-admin user—A Prism Central user without any administrator privileges.
>
> For more information on the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.

About this task

> **Note:**
>
> - You cannot list the buckets only owned by a particular user. So, if you have exceeded your storage quota and try to delete a bucket shared with you to release the storage space, the quota level remains as is. You have to delete your own bucket to release the storage space.
>
> For example, if user A has exceeded the storage quota and tries to list all the buckets, the bucket list will also contain the buckets that were shared with user A by user B. To release the storage space within user A quotas, if user A deletes objects in the buckets shared with user A by user B, the quota level remains as is.
>
> You can run `get-bucket-acl` command on the bucket to list the user owned buckets, and then delete the data from that bucket.
> - Quota policies are enforced for buckets or space usage across all namespaces, federated or non-federated alike.
> - If federation is enabled, quotas for a particular owner/user are enforced only on the OSS cluster where the policy was created and not on other OSS clusters which are part of the same federation.

To assign a quota policy to a user, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the object store to see the object store usage and to assign quota policy to the users.
   The object store opens on a new window.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 931

4. Click **Usage** > **Quota Policy**.
5. Select the user for which you want to create the quota policy.
   If you are creating quota policy for the first time, skip this step.
6. Click **+ Create Policy**.

Figure 152: Create Quota Policy

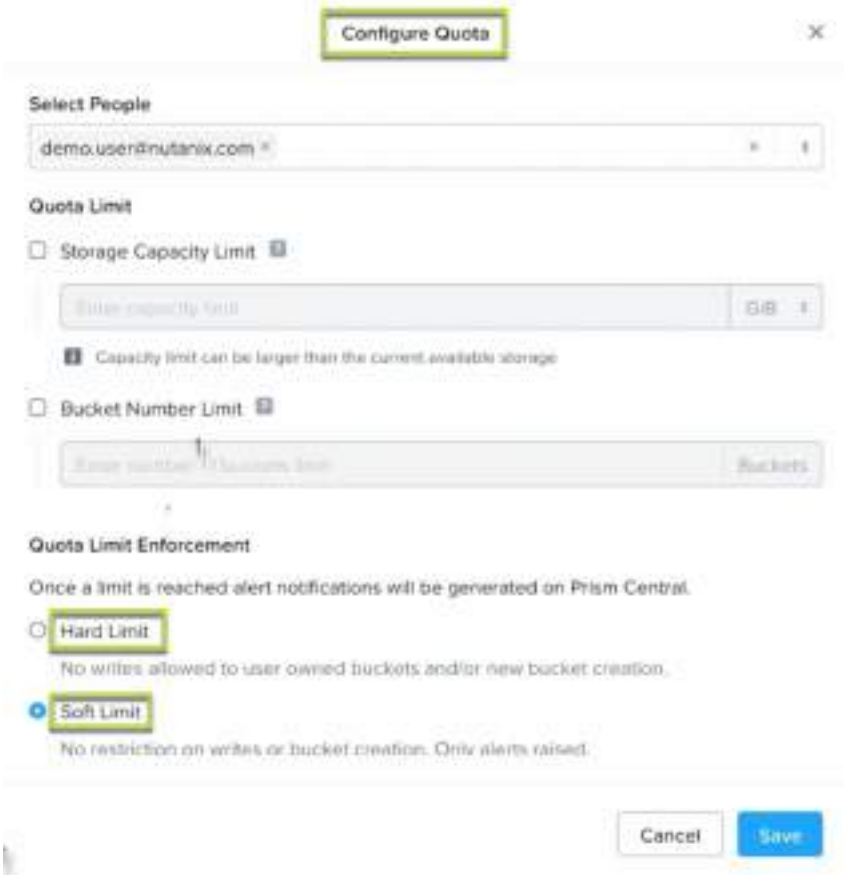


Figure 153: Configure Quota

A **Configure Quota** window appears.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 932

7. Select a user or multiple users from the **People** drop-down.

   > **Note:** You can create quote policy for multiple users simultaneously, but you cannot assign multiple quotas to the same user.

8. In the **Quota Limit** section, select either one check box or both check boxes, and enter the limit.

   a. (Optional) Click the **Storage Limit** check box and enter the total storage capacity limit for the user.

      > **Note:** Capacity Limit cannot be larger than the current available storage.

   b. (Optional) Click the **Bucket Number Limit** check box and enter the number of buckets the user can create.

9. In the **Quota Limit Enforcement** section, select any of the following, and then click **Save**.

   » **Hard limit**: Once the user reaches the specified quota limits, the request is blocked.

   » **Soft limit**: Once the user has exceeded the specified quota limits, only alerts are raised and the request is not blocked.

   > **Note:** You can always update the existing policy.

   A list of users with the configured storage- and bucket-quota, and the current usage is displayed.

   When the storage usage or bucket usage reaches 90% of the defined limit, you are notified with an exclamation mark.

   A background task checks for any violation of quota policies and generates this alert. So, it can take about an hour to generate the alert. On a heavily loaded object store, it can take up to a day to generate an alert.

What to do next

You can view the alerts. For more information, refer to Viewing Alerts on page 218 section.

Viewing Alerts

The Alerts tab apprises administrators of informational, warning, and critical alerts. The Alerts tab presents all notifications and events in an easy-to-consume table format. The table presents each alert with the color-coded severity level, a description of the alert, and the time stamp.

About this task

To view the object store alerts, do the following:

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the object store to view its performance.
   The object store opens in a new window.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 933

4. Click **Alerts**.

Figure 154: Alerts List

The alerts table displays the following information:

Table 11: Alerts Table

Field	Description
Name	This column displays the name of the alert.
Description	This column displays a description of the alert issue.
Severity	This column displays the severity level of the alert. Following are the three severity levels: • **Critical**: A critical alert is one that requires immediate attention. • **Warning**: A warning alert is one that might need attention soon. • **Info**: An info alert highlights a condition to be aware of.
Created	This column displays the number of days since the alert was created. Hover over the number of days to view the date and time when the alert was created.
Silenced	This column provides the option to suppress the alert.

You can also suppress multiple alerts by using **Silence** at the top-left of the screen.

> **Note:** Silencing of alerts is temporary.

You can use **Filters** at the top-right corner to filter the alerts you want to view. You can filter the alerts by severity levels (**Critical**, **Warning**, and **Info**) and state (**Active** and **Silenced**).

Nutanix Objects Specific Alerts

The following tables describe the Objects specific alerts. Apart from the Objects specific alerts, alerts that monitor the underlying infrastructure of the Objects clusters are also triggered. For more information about these alerts, you can contact Nutanix Support at https://portal.nutanix.com.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 934

Table 12: Objects Alert - HighTimeToFirstByte

Name	`HighTimeToFirstByte`
Description	The `HighTimeToFirstByte` alert appears when the Time To First Byte (TTFB) for all the HTTP GET operations in the past 10 minutes exceeds 1 second.
Alert Message	`Get operations issued to the object store in the past 10 minutes have been showing TTFB of <value> msec`
Cause	High network latency, improper sizing, and component crashes may generate `HighTimeToFirstByte` alert.
Impact	The response for Object GET requests becomes slow.
Resolution	Do the following: • Check for the networking issues impacting the nodes in the Prism Element cluster. • Check if the GETs in each second and PUTs in each second shown on the **Performance** page of the object store exceeds the estimated workload at the time of deployment. If there is an indication of an overload, consider reducing the workload on the Object Store Service (OSS). • Check for crashing services on the object store. • Check the Prism Element cluster on which you deployed the object store for any alerts that may be relevant to `HighTimeToFirstByte` alert.

Table 13: Objects Alert - HighObjectStoreUsage

Name	`HighObjectStoreUsage`
Description	The `HighObjectStoreUsage` alert appears when the total object store space usage exceeds the estimated capacity specified at the time of deployment.
Alert Message	`Current object store usage <val> TB exceeds the provisioned capacity <val>TB`
Cause	The following may cause the `HighObjectStoreUsage` alert to generate. • Missing lifecycle management policies • Performing too many object operations.
Impact	Object store gets overloaded, thus causing slow performance.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 935

Resolution	Do the following: • Delete nonessential objects from the object store to reduce the number of objects in the object store. • If the object store usage is unexpectedly high based on the workload and available resources, check for misconfigured Lifecycle Policies on the buckets in the object that may be retaining objects longer than intended. • If the storage space on the Prism Element cluster outside of the object store is high, consider deleting nonessential VMs, snapshots, data, or adding extra nodes to free the storage space in the Prism Element cluster.

Table 14: Objects Alert - HighErrorRate

Name	`HighErrorRate`
Description	The `HighErrorRate` alert appears when the object store returns one or more HTTP 4XX or HTTP 5XX errors in each second for the last 10 minutes.
Alert Message	`Operations issued to Nutanix Buckets have been failing with 5XX/4XX errors with observed error rate <val>/s over the past 10 minutes`
Cause	Improper credentials and component crashes may generate the `HighErrorRate` alert.
Impact	The object store operations fail.
Resolution	Do the following: • Check the client applications for the correct access and secret key combination. • Check for any crashing services on the object store. • Check the Prism Element cluster on which you deployed the object store for any alerts that may be relevant to `HighErrorRate` alert.

Table 15: Objects Replication Alert - ReplicationRPOTimeExceeded

Name	`ReplicationRPOTimeExceeded`
Description	The `ReplicationRPOTimeExceeded` alert appears when the replication of pending objects does not finish even after 12 hours of RPO.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 936

Alert Message	`Last sync time for bucket <bucket name> exceeded RPO time by <time_period_secs>`
Cause	The cause can be a combination of many reasons, such as low network bandwidth, sizing, replication failures, and so on.
Impact	Replication of bucket to remote site lags.
Resolution	Do the following: • Check if any other replication alerts are generated. • Check the connectivity or if the available network bandwidth is sufficient. • Check for any alerts generated due to service crashes.

Table 16: Objects Replication Alert - RemoteEndpointStorageFull

Name	`RemoteEndpointStorageFull`
Description	The `RemoteEndpointStorageFull` alert appears when the object store instance where the remote bucket exists runs out of storage space.
Alert Message	`Storage full on replication endpoint <endpoint name> over the last 15 minutes.`
Cause	The remote objects instance storage becomes full.
Impact	Replication of bucket to remote site fails.
Resolution	Add capacity to the remote objects PE cluster.

Table 17: Objects Replication Alert - RemoteEndpointUnreachable

Name	`RemoteEndpointUnreachable`
Description	The `RemoteEndpointUnreachable` alert appears when the object store instance where the remote bucket exists is not reachable.
Alert Message	`Replication to endpoint <endpoint name> has lost connectivity for the last 15 minutes`
Cause	The following can be the reasons for this alert: • The network connectivity to the remote object store instance is lost. • The remote object store instance is down.
Impact	Replication of bucket to remote site fails.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 937

Resolution	Do the following: • Check the network connectivity to the remote objects instance. • Check if the remote objects instance is up and running.

Table 18: Objects Nfs Alert - HighNfsOpsDropRate

Name	`HighNfsOpsDropRate`
Description	The `HighNfsOpsDropRate` alert is triggered when some of the NFS ops are not being executed for past 10 minutes.
Alert Message	`Due to high payload, few operations submitted to NFS are not executed for the past 10 minutes. Operations are dropped when the outstanding NFS operations have exceeded the threshold value of 1000, or when the QoS queue has reached its maximum capacity of 128 ops, or when the operation wasn't admitted to the queue within 10 seconds.`
Cause	The following can be the reasons for this alert: • NFS payload is causing the number of ops to exceed the threshold value of 1000. • Overall high payload is causing QoS queue to reach its maximum capacity.
Impact	NFS ops are being dropped. Latencies may increase due to client retries.
Resolution	Do the following: • Reduce the overall payload on the impacted bucket. • Modify maximum number of concurrent NFS requests. For example, in CentOS, this can be done by changing `/proc/sys/sunrpc/tcp_slot_table_entries` value to 128.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 938

OBJECTS NOTIFICATIONS

Notifications for Objects enables you to send the completed events logs to the configured endpoints in your Objects instance. This helps you with centralized events log management, thus enabling you to monitor and analyze the logs and identify performance or configuration issues. TCP is the supported protocol for Objects notifications.

The following endpoints are supported for logging the notification events:

- **Syslog**—System Logging Protocol is a standard protocol for sending events logs to the Syslog server. Enter the hostname or host IP address and port number of your Syslog server when configuring the endpoints. Only one endpoint is supported for Syslog. The Syslog server should be up and running when performing the endpoint configuration in your Objects instance.
- **Nats-streaming**—A lightweight, reliable streaming platform built on top of the core NATS platform that provides persistent logs. Enter the hostname or host IP address and port number of your NATS streaming server when configuring the endpoints. Only one endpoint is supported for NATS streaming. NATS streaming server should be up and running when performing the endpoint configuration in your Objects instance.

  > **Note:** The default topic used to create the NATS queue is *OSSEvents*. You can use this as the subject while using the NATS client to connect to the NATS streaming server.

- **Apache Kafka**—Kafka is a distributed system consisting of *servers* and *clients* that communicate through a high-performance TCP network protocol. It can be deployed on bare-metal hardware, virtual machines, and containers in on-premise as well as cloud environments. Enter the hostname or host IP address and port number of your Kafka server when configuring the endpoints. You can add up to 10 Kafka Brokers for an endpoint for Kafka. The Kafka server should be up and running when performing the endpoint configuration in your Objects instance.

Notification Types for Objects

There are two types of notifications for Objects that can be enabled for either successful, or failed, or both successful and failed instance-level and data events.

- **Instance-level events**—All operations performed on a bucket. For example, create a bucket, update a bucket, delete a bucket, enable versioning, and so on. The following instance-level events are supported for successful, or failed, or both successful and failed events:

  > **Note:** All the instance-level events notifications are enabled by default once you configure the endpoints. You cannot enable or disable the notifications for a single instance-level event.

Table 19: S3 APIs for Only Successful Instance-level Events

Supported Instance-level Events	S3 APIs for Only Successful Instance-level Events
Create bucket	S3:BucketCreated:Put
Delete bucket	S3:BucketRemoved:Delete
Add bucket policy	S3:BucketPolicy:Put
Enable static website	S3:BucketWebsite:Put
Disable static website	S3:BucketWebsite:Delete

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 939

Supported Instance-level Events	S3 APIs for Only Successful Instance-level Events
Create bucket CORS	S3:BucketCORS:Put
Delete bucket CORS	S3:BucketCORS:Delete
Update bucket lifecycle policy	S3:BucketLifecyclePolicy:Update
Delete bucket lifecycle policy	S3:BucketLifecyclePolicy:Delete
Enable bucket lock (WORM)	S3:BucketLock:Enabled
Disable bucket lock (WORM)	S3:BucketLock:Disabled
Add bucket replication rule	S3:BucketReplication:Put
Delete bucket replication rule	S3:BucketReplication:Delete
Enable bucket versioning	S3:BucketVersioning:Enabled
Suspend bucket versioning	S3:BucketVersioning:Disabled
Enable bucket notification	S3:BucketNotify

Table 20: S3 APIs for Only Failed Instance-level Events

Supported Instance-level Events	S3 APIs for Only Failed Instance-level Events
Create bucket	S3:BucketCreatedError:Put
Delete bucket	S3:BucketRemovedError:Delete
Add bucket policy	S3:BucketPolicyError:Put
Enable static website	S3:BucketWebsiteError:Put
Disable static website	S3:BucketWebsiteError:Delete
Create bucket CORS	S3:BucketCORSError:Put
Delete bucket CORS	S3:BucketCORSError:Delete
Update bucket lifecycle policy	S3:BucketLifecyclePolicyError:Update
Delete bucket lifecycle policy	S3:BucketLifecyclePolicyError:Delete
Enable bucket lock (WORM)	S3:BucketLockError:Enabled
Disable bucket lock (WORM)	S3:BucketLockError:Disabled
Add bucket replication rule	S3:BucketReplicationError:Put
Delete bucket replication rule	S3:BucketReplicationError:Delete
Enable bucket versioning	S3:BucketVersioningError:Enabled
Suspend bucket versioning	S3:BucketVersioningError:Disabled

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 940

Supported Instance-level Events	S3 APIs for Only Failed Instance-level Events
Enable bucket notification	S3:BucketNotifyError

Table 21: S3 APIs for Both Successful and Failed Instance-level Events

Supported Instance-level Events	S3 APIs for Both Successful and Failed Instance-level Events
Create bucket	S3:BucketCreated:Put and S3:BucketCreatedError:Put
Delete bucket	S3:BucketRemoved:Delete and S3:BucketRemovedError:Delete
Add bucket policy	S3:BucketPolicy:Put and S3:BucketPolicyError:Put
Enable static website	S3:BucketWebsite:Put and S3:BucketWebsiteError:Put
Disable static website	S3:BucketWebsite:Delete and S3:BucketWebsiteError:Delete
Create bucket CORS	S3:BucketCORS:Put and S3:BucketCORSError:Put
Delete bucket CORS	S3:BucketCORS:Delete and S3:BucketCORSError:Delete
Update bucket lifecycle policy	S3:BucketLifecyclePolicy:Update and S3:BucketLifecyclePolicyError:Update
Delete bucket lifecycle policy	S3:BucketLifecyclePolicy:Delete and S3:BucketLifecyclePolicyError:Delete
Enable bucket lock (WORM)	S3:BucketLock:Enabled and S3:BucketLockError:Enabled
Disable bucket lock (WORM)	S3:BucketLock:Disabled and S3:BucketLockError:Disabled
Add bucket replication rule	S3:BucketReplication:Put and S3:BucketReplicationError:Put
Delete bucket replication rule	S3:BucketReplication:Delete and S3:BucketReplicationError:Delete
Enable bucket versioning	S3:BucketVersioning:Enabled and S3:BucketVersioningError:Enabled
Suspend bucket versioning	S3:BucketVersioning:Disabled and S3:BucketVersioningError:Disabled
Enable bucket notification	S3:BucketNotify and S3:BucketNotifyError

For more information, see Configuring Events Notification on page 229.

The following is the structure of the notification output for instance-level events that get published to the endpoints.

```
{"EventType":"s3:BucketCreated:Put","Key":"frst","Records":
[{"eventError":"","eventVersion":"2.0","eventSource":"aws:s3","awsRegion":"us-
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 941

```
east-1","eventTime":"2022-02-09T07:40:13Z","eventName":"s3:BucketCreated:Put","userIdentity":
{"principalId":"upgrade@ntnx.com"},"requestParameters":
{"sourceIPAddress":"10.44.91.64"},"responseElements":
{"x-amz-id-2":"110000+1229+2129+240","x-amz-request-
id":"110000+1229+2129+240","x-ntnx-origin-endpoint":"0.0.0.0"},"s3":
{"s3SchemaVersion":"1.0","configurationId":"SuccessfulWriteManagementEvent","OSSDomain":"rc4.eng
{"name":"frst","ownerIdentity":
{"principalId":"upgrade@ntnx.com"},"arn":"arn:aws:s3:::frst"}}}],"level":"info","msg":"","time":
```


- **Data events**—Data events are specific to data operations. These events can be enabled for each bucket. To enable notifications for successful, or failed, or both data events for a bucket, you need to create notification rules. You can define the scope of a notification rule by selecting **All Objects** or **Subset of objects**. For more information, see Creating Notification Rules for Data Events on page 235.

  The following is the structure of the notification output for data events that get published to the endpoints.


```
{"EventType":"s3:ObjectCreated:Put","Key":"put","Records":
[{"eventError":"","eventVersion":"2.0","eventSource":"aws:s3","awsRegion":"us-
east-1","eventTime":"2022-02-09T08:04:48Z","eventName":"s3:ObjectCreated:Put","userIdentity":
{"principalId":"upgrade@ntnx.com"},"requestParameters":
{"sourceIPAddress":"10.44.91.64"},"responseElements":
{"x-amz-id-2":"110000+1229+2791+297","x-amz-request-
id":"110000+1229+2791+297","x-ntnx-origin-endpoint":"0.0.0.0"},"s3":
{"s3SchemaVersion":"1.0","configurationId":"5836c513-51ef-45a9-9c84-6a0c01996e40","OSSDomain":"r
{"name":"put","ownerIdentity":
{"principalId":"upgrade@ntnx.com"},"arn":"arn:aws:s3:::put"},"object":
{"key":"csv.docx","size":"31","eTag":"c7a74379a77360a6b85926adb8b2aafb","versionId":"1","sequenc
```


The following data events are supported for successful, or failed, or both successful and failed events:

> **Note:** You can enable notifications for all Objects Create Events, Objects Access Events, or Objects Delete Events, or you can choose to enable notifications for one or more sub-categories of Objects Create Events (such as Put, Post, Copy, Multipart Upload Complete), Objects Access Events (such as Get, Head), or Objects Delete Events (such as Delete, Delete Markers).

Table 22: S3 APIs for Only Successful Data Events

Supported Data Events	S3 APIs for Only Successful Data Events
All Create Events	s3:ObjectCreated:*
Put	s3:ObjectCreated:Put
Post	s3:ObjectCreated:Post
Copy	s3:ObjectCreated:Copy
Multipart Upload	s3:ObjectCreated:CompleteMultipartUpload
All Access Events	s3:ObjectAccessed:*
Get	s3:ObjectAccessed:Get
Head	s3:ObjectAccessed:Head
All Delete Events	s3:ObjectRemoved:*
Delete	s3:ObjectRemoved:Delete

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 942

Supported Data Events	S3 APIs for Only Successful Data Events
Delete Markers	s3:ObjectRemoved:DeleteMarkerCreated

Table 23: S3 APIs for Only Failed Data Events

Supported Data Events	S3 APIs for Only Failed Data Events
All Create Events	s3:ObjectCreatedError:*
Put	s3:ObjectCreatedError:Put
Post	s3:ObjectCreatedError:Post
Copy	s3:ObjectCreatedError:Copy
Multipart Upload	s3:ObjectCreatedError:CompleteMultipartUpload
All Access Events	s3:ObjectAccessedError:*
Get	s3:ObjectAccessedError:Get
Head	s3:ObjectAccessedError:Head
All Delete Events	s3:ObjectRemovedError:*
Delete	s3:ObjectRemovedError:Delete
Delete Markers	s3:ObjectRemovedError:DeleteMarkerCreated

Table 24: S3 APIs for Both Successful and Failed Data Events

Supported Data Events	S3 APIs for Both Successful and Failed Data Events
All Create Events	s3:ObjectCreated:* and s3:ObjectCreatedError:*
Put	s3:ObjectCreated:Put and s3:ObjectCreatedError:Put
Post	s3:ObjectCreated:Post and s3:ObjectCreatedError:Post
Copy	s3:ObjectCreated:Copy and s3:ObjectCreatedError:Copy
Multipart Upload	s3:ObjectCreated:CompleteMultipartUpload and s3:ObjectCreatedError:CompleteMultipartUpload
All Access Events	s3:ObjectAccessed:* and s3:ObjectAccessedError:*
Get	s3:ObjectAccessed:Get and s3:ObjectAccessedError:Get
Head	s3:ObjectAccessed:Head and s3:ObjectAccessedError:Head

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 943

Supported Data Events	S3 APIs for Both Successful and Failed Data Events
All Delete Events	s3:ObjectRemoved:* and s3:ObjectRemovedError:*
Delete	s3:ObjectRemoved:Delete and s3:ObjectRemovedError:Delete
Delete Markers	s3:ObjectRemoved:DeleteMarkerCreated and s3:ObjectRemovedError:DeleteMarkerCreated

Configuring Events Notification

While configuring events notification, you specify the endpoints. Once you have configured events notification, by default, only successful instance-level events get logged to the endpoints. You can choose to log only successful, only failed, both successful and failed events or none.

Before you begin

A non-admin user can configure event notifications only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions and the non-admin user must be assigned to specific objects instances:

- Set Notification Endpoint
- View Notification Endpoint
- View Object store

Note: Administrators and non-admin users are Prism Central users with the following roles:

- Administrator—A Super Admin or a Prism Admin in Prism Central.
- Non-admin user—A Prism Central user without any administrator privileges.

For more information on the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.

Note:

- Objects now supports notifications via Syslog, NATs, or Kafka. If you need to log CRUD operations, you can do so by enabling notifications to one of the three services. However, Nutanix currently does not manage these services and you should bring up your own Syslog, NATs, or Kafka servers, and enable event notifications to one of these endpoints.
- Updating the notification configuration can take up to 5 minutes to reflect.
- When you try to add a Kafka endpoint, if the topic *OSSEvents* is not created in the Kafka cluster, then the system will create it. But if the topic *OSSEvents* is already created, then you need to validate if the topic is created as per the configuration set in the Kafka server.

About this task

To configure events notifications, do the following:

Procedure

1. Log on to the Prism Central web console.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 944

2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the object store to view its performance.
   The object store opens in a new window.
4. Click **Settings** > **Notification Endpoints**.
   The **Notification Endpoints** page appears.

   This page allows you to configure the endpoints by entering the endpoint server details. The available endpoints are **Syslog**, **Nats-streaming**, and **Kafka**. You can enable any one of these endpoints or all of them.

   Note: When you add a valid notification endpoint (that is, Syslog or Nats-streaming or Kafka endpoint fields, or all are in the correct format), the operation is successful even if the endpoint is not connected, or the endpoint is not Syslog or Nats-streaming or Kafka. If there is an error while adding the endpoint, the object store list page displays the error message.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 945

5. In the **Syslog** tab, turn on the **Enable** toggle button to configure Syslog as the endpoint.

> **Important:** Syslog server should be up and running when performing the endpoint configuration in your Objects instance.

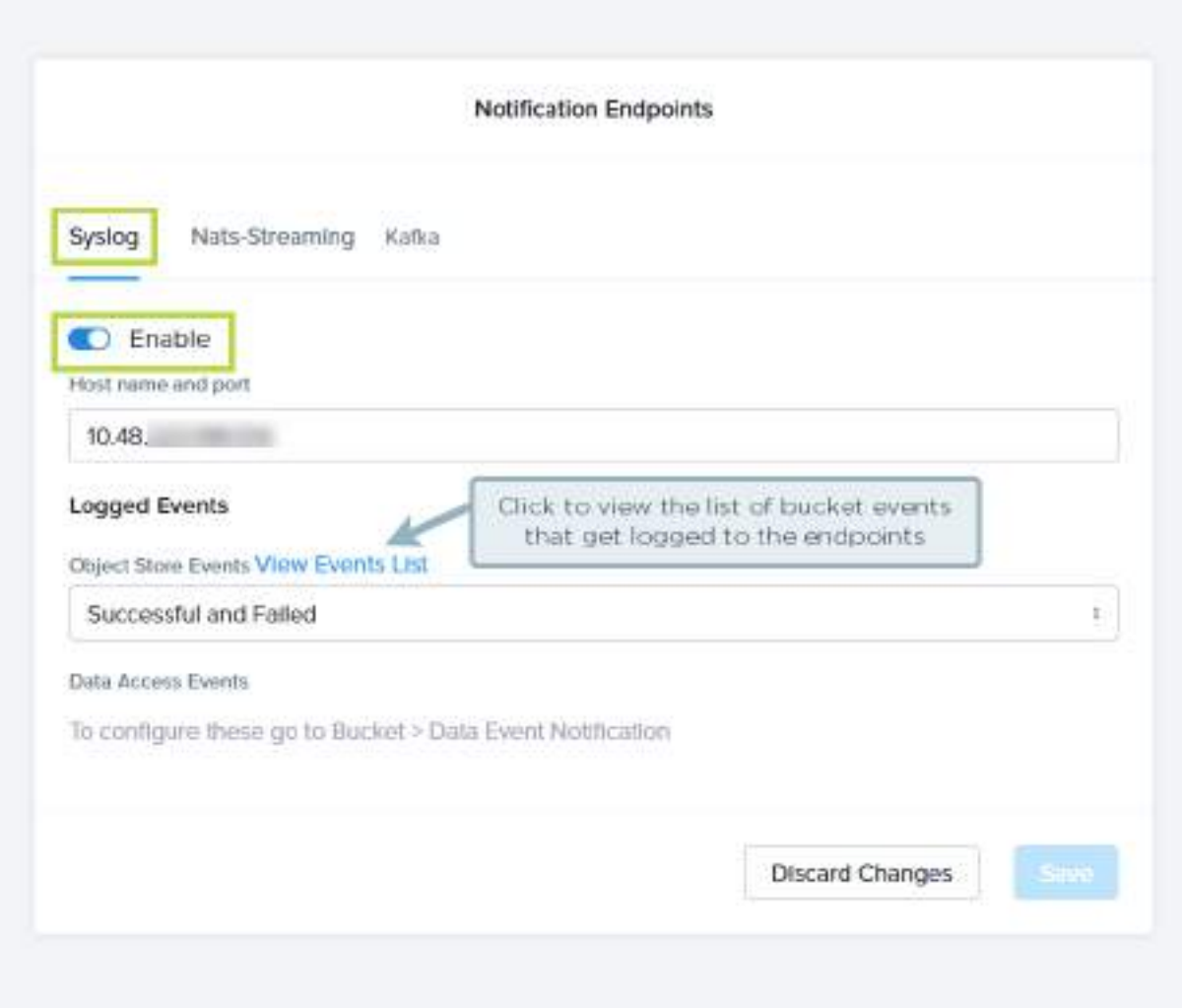


Figure 155: Notification Endpoints: Syslog

a. In the **Host name and port** box, enter the host name and port number of your Syslog server in the *Host name:Port* format.

b. In the **Logged Events** section, select one of the following object store events for which you want to enable notifications. By default, **Successful only** option is selected.

- **Successful and Failed**: Logs both successful and failed object store events.
- **Successful only**: Logs only successful object store events.
- **Failed only**: Logs only failed object store events.
- **None**: Logs none of the object store events.

> **Note:** You can click **View Events List** link to view the list of bucket events that get logged to the endpoints.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 946

6. In the **Nats-streaming** tab, turn on the **Enable** toggle button to configure Nats-streaming as the endpoint.

   Important: Nats-streaming server should be up and running when performing the endpoint configuration in your Objects instance.

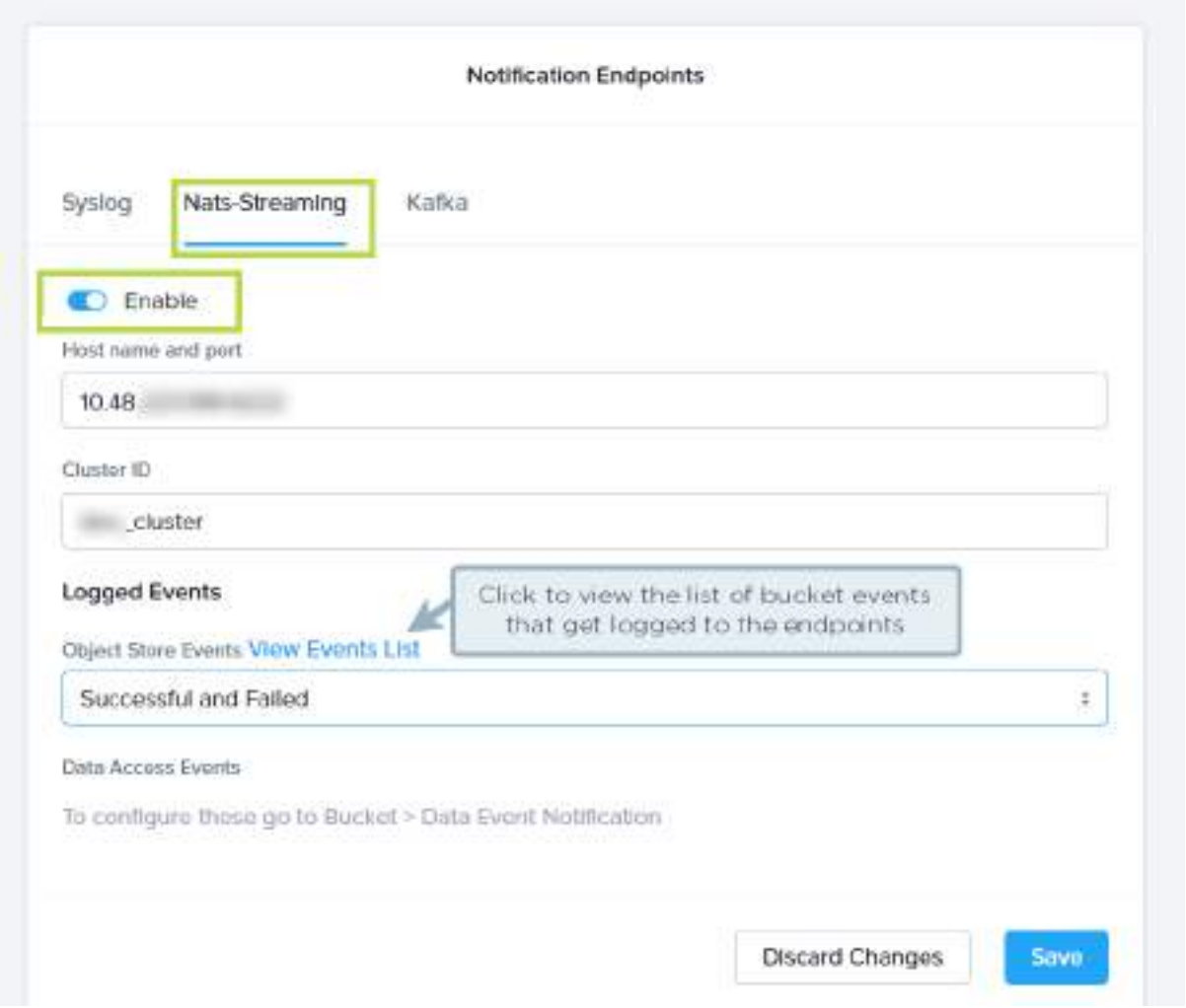


Figure 156: Notification Endpoints: Nats-Streaming

   a. In the **Host name and port** box, enter the host name and port number of your NATS streaming server in the *Host name:Port* format.

   b. In the **Cluster ID** box, enter the cluster ID of the server that you used to start the NATS server.

   c. In the **Logged Events** section, select one of the following object store events for which you want to enable notifications. By default, **Successful only** option is selected.

      - **Successful and Failed**: Logs both successful and failed object store events.
      - **Successful only**: Logs only successful object store events.
      - **Failed only**: Logs only failed object store events.
      - **None**: Logs none of the object store events.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 947

Note: You can click **View Events List** link to view the list of bucket events that get logged to the endpoints.

7. In the **Kafka** tab, turn on the **Enable** toggle button to configure Kafka as the endpoint.

> **Important:** Kafka server should be up and running when performing the endpoint configuration in your Objects instance.

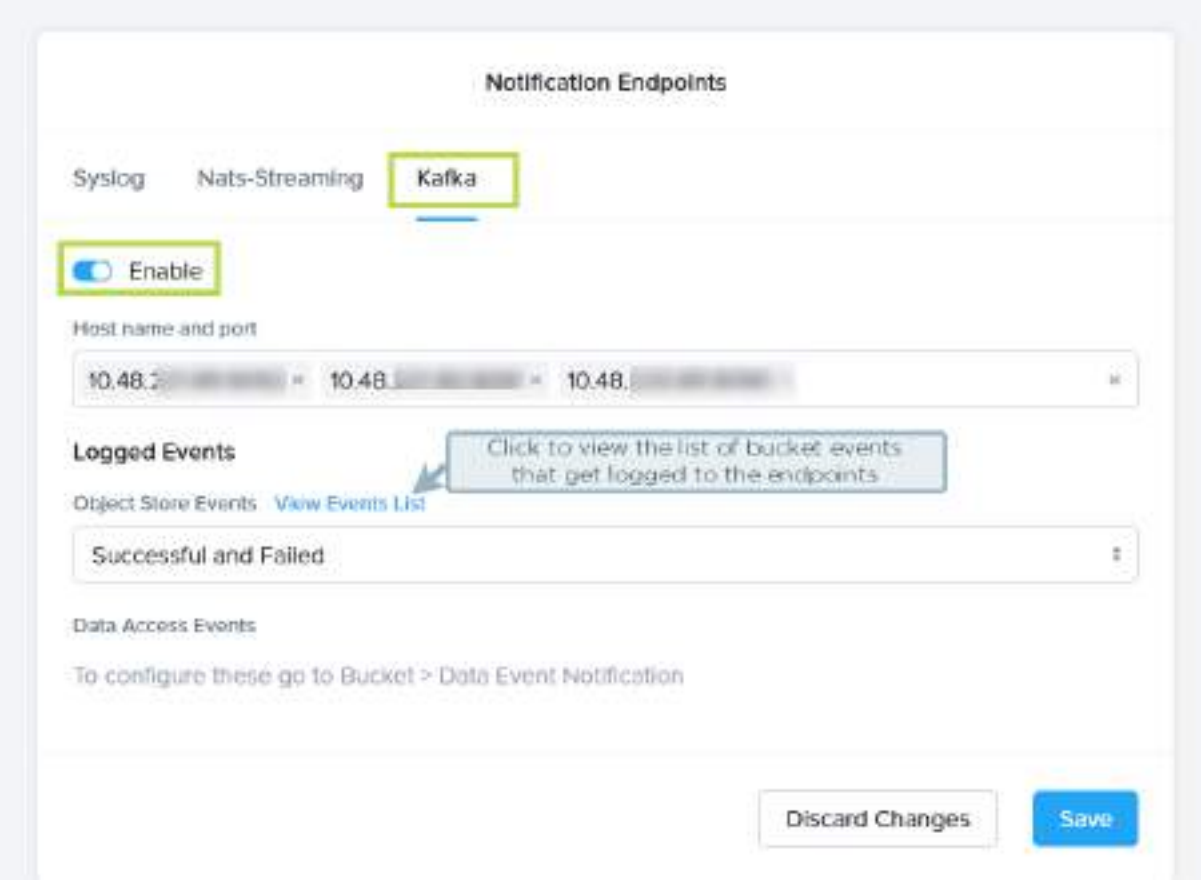


Figure 157: Notification Endpoints: Kafka

a. In the **Host name and port** box, enter the host name and port number of your Kafka streaming server in the *Host name:Port* format.

> **Note:** Up to 10 Kafka Brokers are supported for a Kafka endpoint.

For entering multiple brokers, hit space after entering a broker.

b. In the **Logged Events** section, select one of the following object store events for which you want to enable notifications. By default, **Successful only** option is selected.

- **Successful and Failed**: Logs both successful and failed object store events.
- **Successful only**: Logs only successful object store events.
- **Failed only**: Logs only failed object store events.
- **None**: Logs none of the object store events.

> **Note:** You can click **View Events List** link to view the list of bucket events that get logged to the endpoints.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 949

8. Click **Save** to complete the events notification configuration for Syslog, Nat-streaming, and Kafka.

   Notification is enabled for your Objects instance. Also, the status of the notification endpoint is shown in the **Notifications** column. For example, if the NATS endpoint gets disconnected due to network issues, a red icon appears in the **Notifications** column. Hovering over the red icon displays `Cannot connect to nats endpoint` message.

9. (Optional) To undo an endpoint configuration, do the following.

   a. Click **Settings** > **Notification Endpoints** to open the **Notification Endpoints** page.

   b. Clear the check box for the endpoint that you want to remove, and then click **Save**.

   c. In the **Data Event Notification** page, delete all the notification rules corresponding to the endpoint that you removed before adding a new notification rule to the bucket. For more information, see Creating Notification Rules for Data Events on page 235.

What to do next

You can now create notification rules for data events of the bucket, refer to Creating Notification Rules for Data Events on page 235.

Creating Notification Rules for Data Events

To keep track of the data events that get completed successfully, you need to create notification rules for the buckets.

Before you begin

A non-admin user can create notification rules for data events only after the administrator creates an access control policy on a role in Prism Central for the non-admin user. The specific role must have the following minimum permissions and the non-admin user must be assigned to specific objects instances:

- View Notification Endpoint
- Edit Buckets
- View Buckets
- View Object Store

Note:

- Administrators and non-admin users are Prism Central users with the following roles:
  - Administrator—A Super Admin or a Prism Admin in Prism Central.
  - Non-admin user—A Prism Central user without any administrator privileges.

  For more information about the built-in roles in Prism Central, see Built-in Role Management in the *Security Guide*.
- Users with Edit Bucket permission can create notification rules for data events on all buckets available in the Object stores that are assigned to the respective users.

About this task

To create a notification rule for a bucket, do the following.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 950

Procedure

1. Log on to the Prism Central web console.
2. In the Application Switcher, click **Objects**.
3. In the object stores table, click the name of the object store to view its performance.
   The object store opens in a new window.
4. Click the **Buckets** tab, and then from the list of buckets, select the bucket for which you want to create a notification rule.
5. Click **Data Event Notification**.
   The **Data Event Notification** page appears.
6. Click **Create Rule** to open the **Create Rule** page.

   Note: Configuring an endpoint is required to create notification rules. Configure endpoints that can be used to log both bucket events and data events. See Configuring Events Notification on page 229.

   If a rule is already created for that bucket, click **+ Add Rule** to add a new rule on the **Create Rule** page.

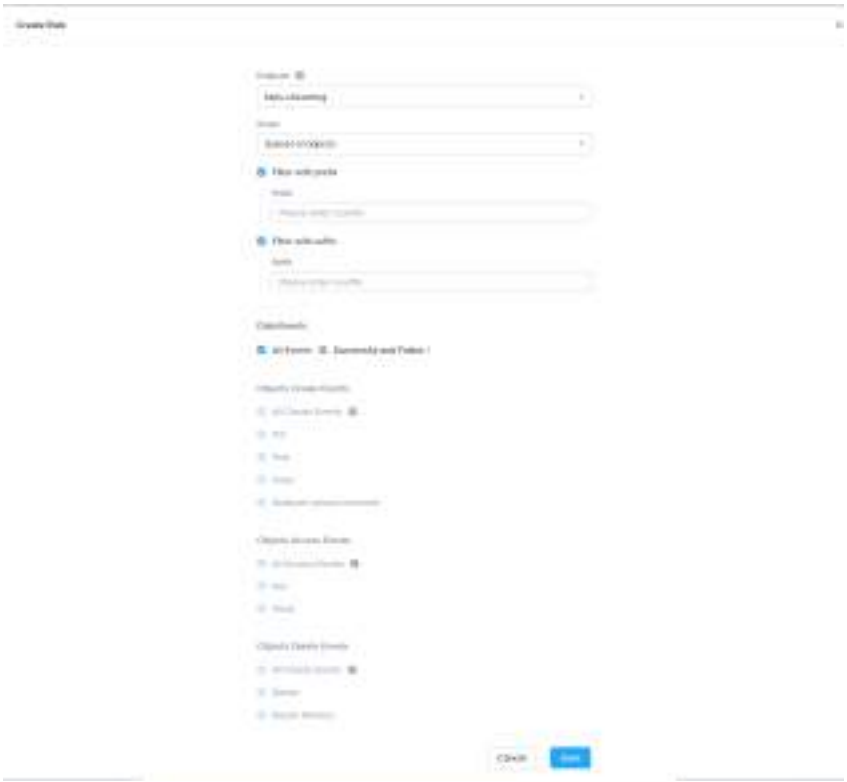


Figure 158: Create Rule

7. In the **Create Rule** page, do the following.

   a. In the **Endpoint** list, select the endpoint where you want the data events for this bucket to get logged. The endpoints you enable will be listed here.

      To update endpoints for your Objects instance, see Configuring Events Notification.

   b. In the **Scope** list, select **All Objects** or **Subset of objects**.

      - If you select **All Objects**, the notification rule you are creating applies to all the objects.
      - Select **Subset of objects** to apply the notification rule to specific objects. You can filter Objects by entering a prefix, suffix, or both. Objects with the prefix and suffix you specified get filtered and the rule applies to those objects.

        Note:

        - You cannot proceed without providing a suffix or prefix for the scope Subset of objects.
        - You can enter only one prefix and suffix. You can create another rule with a different suffix and prefix.
        - The suffix-prefix pair in two rules corresponding to the same event should not be overlapping. For example, any given Object name *xyz.jpg* should be selected by a maximum of one rule corresponding to the given event type.

   c. In the **Data Events** section, click the **All Events** check box to select all data events, or select a check box next to the name of the events listed under **Objects Create Events**, **Objects Access Events**, and **Objects Delete Events**, and choose from the following that you want to get logged to the endpoint.

      - **Successful and Failed**: Logs both successful and failed object store events.
      - **Successful only**: Logs only successful object store events.
      - **Failed only**: Logs only failed object store events.

        Note: When you select the **All Events** check box, all the Objects Create Events, Objects Access Events, and Objects Delete Events will be selected.

8. Click **Save** to complete, and then click **Done** to close the **Create Rule** page.

   The notification rule you created appears in the list of data events notification rules on the **Data Event Notification** page. You can click **All Events** or ***Number*** **Events** in the Events column to view

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 952

the configured data events for that bucket. For example, click **8 Events** to view the 8 data events configured.

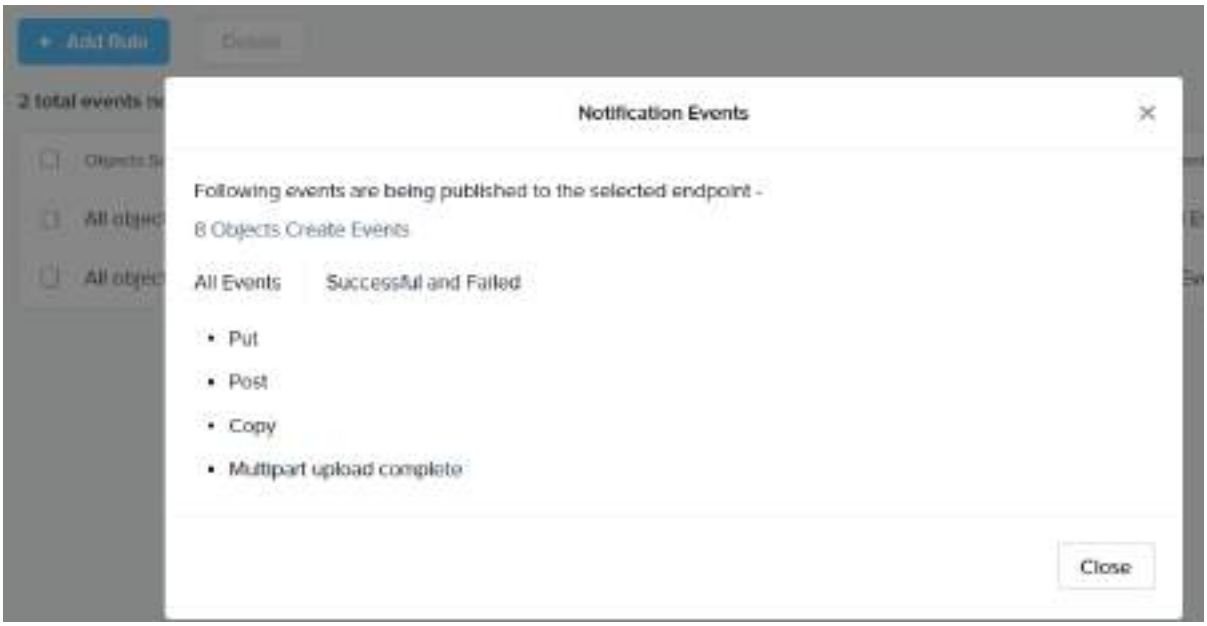


Figure 159: Configured Notification Events

Also, you can delete a notification rule. In the **Data Event Notification** page, select a notification rule from the list, and then click **Delete**.

After you create a notification rule for a bucket, the status in the **Notifications** column changes to **Enabled**.

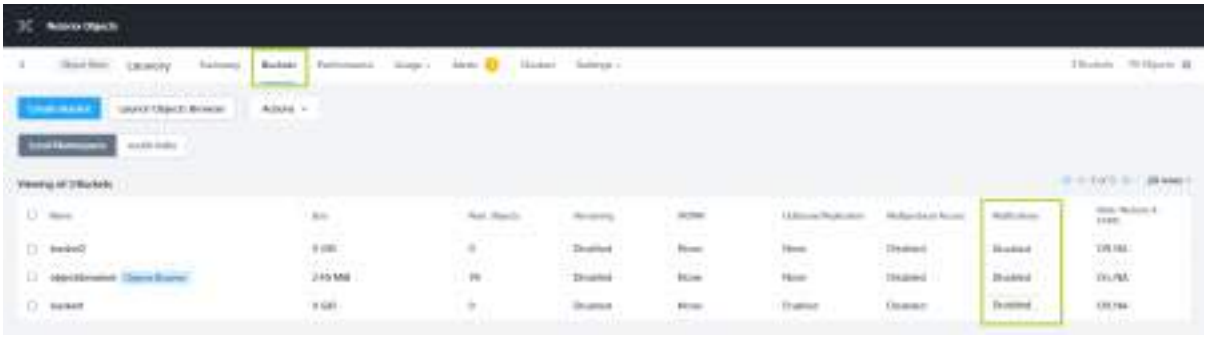


Figure 160: Notification Rule - Enabled for Data Events

CRUD OPERATIONS BY USING S3 APIS

You can create and manage buckets and objects by using the S3 APIs, which are then visible in Prism Central.

Authentication

You can send requests to Objects by using the REST API or the Amazon Web Services Software Development Kit (AWS SDK) wrapper libraries that wrap the underlying S3 REST API. Every interaction with Objects is authenticated. In this authentication process, the identity of the requester who is trying to access Objects is verified with a signature value. The signature value is generated from the AWS access keys (access key ID and secret access key) of the requester. This AWS access keys and endpoint URL is provided by the administrator to the user.

If you are using the AWS SDK, the libraries compute the signature from the keys you provide. However, if you make direct REST API calls, the signature is computed from the request.

For creating the buckets and objects, you need the following information from the administrator:

- Endpoint URL (Static IP address and the Port number)
- Access key ID
- Secret access key

Once you get this information, you can import the SDK libraries, create a session and a client, and then you can start making the requests (for example, creating buckets and objects).

Note: Objects supports the following:

- Signature Version 2 and Signature Version 4 (regular and pre-signed)
- Streaming signed payloads for PUT requests with Signature Version 4

Supported and Unsupported APIs

This section describes Objects support for Amazon S3 API. The object store service is available on the following ports:

- **HTTP**: 80
- **HTTPS**: 443

Note:

- Transport Layer Security (TLS) 1.2 is supported on Objects.
- Support for all CBC ciphers, except `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384`, for S3 protocol access over secure connection port 443 is deprecated.

  If you are using RSA certificate, the following ciphers are allowed.

  ```
  TLS/1.2
  IANA : TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (OpenSSL : ECDHE-RSA-AES256-GCM-SHA384)
  ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 954

```
IANA : TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (OpenSSL : ECDHE-RSA-AES128-GCM-
SHA256)
```

If you are using EC certificate, the following ciphers are allowed.

```
TLS/1.2
IANA : TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (OpenSSL : ECDHE-ECDSA-AES256-
GCM-SHA384)
IANA : TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (OpenSSL : ECDHE-ECDSA-AES128-
GCM-SHA256)
```

Supported APIs

The following table lists the supported S3 API methods.

Note:

- User-provided meta-data header names get stored in lower case.
- User-defined object meta-data is supported for `PUT Object` and `PUT Object - Copy` APIs and limited to 2 KB in size.
- For bucket tagging, tags starting with prefix `ntnx:` are reserved for internal services and not allowed by external clients.

Table 25: Supported S3 APIs and Parameters

Supported S3 APIs	Request Parameters/Request Headers/Request Elements/Request Body
PUT Bucket	Common Headers on page 243 + CreateBucketConfiguration, LocationConstraint (By default, LocationConstraint “us-east-1” is only supported.)
PUT Bucket Lifecycle	Common Headers on page 243 + Content-MD5 + AbortIncompleteMultipartUpload, And, Date, Days, DaysAfterInitiation, Expiration, Filter, ID, Key, LifecycleConfiguration, NoncurrentDays, NoncurrentVersionExpiration, NoncurrentVersionTransition, Prefix, Rule, Status
PUT Bucket Policy	Common Headers on page 243 + JSON string containing the policy contents containing the policy statements
PUT Bucket versioning	Status, VersioningConfiguration
Complete Multipart Upload	Common Headers on page 243 + CompleteMultipartUpload, Part, PartNumber, ETag

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 955

Supported S3 APIs	Request Parameters/Request Headers/Request Elements/Request Body
PUT Object - Copy	Common Headers on page 243 + x-amz-copy-source, x-amz-metadata-directive, x-amz-copy-source-if-match, x-amz-copy-source-if-none-match, x-amz-copy-source-if-unmodified-since, x-amz-copy-source-if-modified-since, x-amz-tagging, x-amz-tagging-directive, x-amz-meta-, x-amz-object-lock-legal-hold, x-amz-object-lock-mode, x-amz-object-lock-retain-until-date
DELETE Objects	Single query string parameter "delete" + Common Headers + Content-MD5, Content-Length, Delete, Quiet, Object, Key, VersionId
GET Object	Common Headers on page 243 + Range, If-Modified-Since, If-Unmodified-Since, If-Match, If-None-Match, x-amz-object-lock-legal-hold, x-amz-object-lock-mode, x-amz-object-lock-retain-until-date
HEAD Object	Common Headers on page 243 + Range, If-Modified-Since, If-Unmodified-Since, If-Match, If-None-Match, x-amz-object-lock-legal-hold, x-amz-object-lock-mode, x-amz-object-lock-retain-until-date
List Multipart Uploads	Common Headers on page 243 + delimiter,max-uploads, key-marker, prefix, upload-id-marker
List Object Versions	Common Headers on page 243 + delimiter, key-marker, max-keys, prefix, version-id-marker
GET Bucket (List Objects) Version 1	Common Headers on page 243 + delimiter, marker, max-keys, prefix
GET Bucket (List Objects) Version 2	Common Headers on page 243 + delimiter, max-keys, prefix, list-type, continuation-token, fetch-owner, start-after
List Parts	Common Headers on page 243 + uploadId, max-parts, part-number-marker
PUT Object	Common Headers on page 243 + Content-Length, Content-MD5, Expect, x-amz-tagging, x-amz-meta-, x-amz-object-lock-mode, x-amz-object-lock-retain-until-date, x-amz-object-lock-legal-hold
INITIATE Multipart Upload	Common Headers on page 243 + x-amz-meta-, x-amz-tagging, x-amz-object-lock-legal-hold, x-amz-object-lock-mode, x-amz-object-lock-retain-until-date
UPLOAD Part	Content-Length, Content-MD5, Expect
Upload Part - Copy	x-amz-copy-source, x-amz-copy-source-range, x-amz-copy-source-if-match, x-amz-copy-source-if-none-match, x-amz-copy-source-if-unmodified-since, x-amz-copy-source-if-modified-since

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 956

Supported S3 APIs	Request Parameters/Request Headers/Request Elements/Request Body
PUT Bucket Object Lock Configuration	Common Headers on page 243 + ObjectLockEnabled Rule
DELETE Bucket	Common Headers on page 243 + Bucket
Delete Multiple Objects	Common Headers on page 243 + Bucket, Delete, Quiet, Objects, Key, VersionId
GET Object Retention	Common Headers on page 243 + Bucket, Key, VersionId
PUT Object Retention	Common Headers on page 243 + Bucket, Key, VersionId, Retention, Mode, RetainUntilDate
PUT Object Legal Hold	Common Headers on page 243 + Bucket, Key, versionId, LegalHold, Status
GET Object Legal Hold	Common Headers on page 243 + Bucket, Key, versionId
Select Object Content	Expression, ExpressionType, InputSerialization, CSV, AllowQuotedRecordDelimiter, Comments, FieldDelimiter, FileHeaderInfo, QuoteCharacter, QuoteEscapeCharacter, RecordDelimiter, OutputSerialization, CSV

Note: The maximum size limit of a multipart object is 16 TiB. This limit is different from the standard S3 API limit of 5 TiB.

For more information about objects tagging API, refer to Buckets and Objects Tagging APIs Overview on page 244.

For more information about S3 Select API, refer to S3 Select API Overview on page 246.

Pre-signed URLs can be generated for Objects. For more information about generating the pre-signed URLs, see *Signing and authenticating REST requests* section in the *Amazon Simple Storage Service Developer Guide*.

Note: You can limit a presigned request by specifying an expiration time. You can set an expiration time of more than seven days.

The following table lists the supported APIs that use only Common Headers on page 243:

Supported APIs
GET Bucket lifecycle configuration
PUT Bucket lifecycle configuration
GET Bucket Object Lock Configuration
GET Bucket Location
GET Bucket Policy
GET Bucket versioning
GET Bucket ACL
GET Bucket notification configuration
GET Bucket cors

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 957

Supported APIs
GET Bucket website
GET Bucket replication
PUT Bucket cors
PUT Bucket notification configuration
PUT Bucket website
PUT Bucket replication
DELETE Bucket cors
DELETE Bucket website
DELETE Bucket Lifecycle
DELETE Bucket replication
DELETE Object
HEAD Bucket
LIST Bucket
ABORT Multipart Upload

Common Headers

You can use the following headers while making requests:

Table 26: List of Common Headers

Authorization
Content-Length
Content-Type
Content-MD5
Date
Expect
Host
x-amz-content-sha256
x-amz-date
x-amz-security-token

For more information about common headers, refer to *the Common Request Headers* section in the *Amazon Simple Storage Service API Reference Guide*.

Unsupported APIs

The following table lists the unsupported S3 API methods:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 958

Table 27: Unsupported S3 APIs

Unsupported S3 APIs
GET Bucket accelerate configuration
GET Bucket analytics configuration
GET Bucket encryption
GET Bucket inventory configuration
GET Bucket logging
GET Bucket metrics configuration
GET Bucket requestPayment
List Bucket Analytics Configurations
List Bucket Inventory Configurations
List Bucket Metrics Configurations
PUT Bucket accelerate configuration
PUT Bucket acl
PUT Bucket analytics configuration
PUT Bucket encryption
PUT Bucket inventory configuration
PUT Bucket logging
PUT Bucket metrics configuration
DELETE Bucket analytics configuration
DELETE Bucket inventory configuration
DELETE Bucket metrics configuration
DELETE Bucket encryption
DELETE Bucket Policy
Copy
GET Object ACL
PUT Object ACL
Restore Object

Buckets and Objects Tagging APIs Overview

A tag is a label that you assign to a bucket or an object, and it consists of a key and a value pair that you can define.

The tagging APIs feature allows you to add, retrieve, and remove tags for your buckets and objects.

Buckets Tagging

- Retrieving bucket metadata also returns the number of tags associated with the bucket, if any.
- The maximum number of tags allowed per bucket is 50.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 959

- Tag keys can be up to 128 Unicode characters in length, and tag values can be up to 256 Unicode characters in length.
- Tag keys and values are case-sensitive.

Objects Tagging

- Retrieving objects metadata also returns the number of tags associated with the object, if any.
- Tagging is also supported with a few other Object APIs.
- The maximum number of tags allowed per object is 10.
- Tag keys can be up to 128 Unicode characters in length, and tag values can be up to 256 Unicode characters in length.
- Tag keys and values are case-sensitive.

API Operations Supported for Buckets and Objects Tagging

Objects supports APIs for tagging both buckets and objects. Tag-based bucket lifecycle policy management and object listing are not supported.

Bucket Tagging API Operations

Nutanix Objects supports the following bucket tagging API operations.

> **Note:** For bucket tagging, tags starting with prefix `ntnx:` are reserved for internal services and not allowed by external clients.

- **PutBucketTagging**: Sets the tags for a bucket.

  The following two scenarios are involved:

  - You can add tags to a bucket with no tags associated with it.
  - You can replace the existing tags associated with the bucket.
- **GetBucketTagging**: Returns the tag set associated with the bucket..
- **DeleteBucketTagging**: Deletes the tags associated with a bucket.

For more information on bucket tagging, refer to the *PutBucketTagging* section of the *Amazon Simple Storage Service API Reference* guide.

Object Tagging API Operations

Nutanix Objects supports the following object tagging API operations.

- **PUT Object tagging**: Replace the tags associated with an object. You can add the tags in the request body.

  The following two scenarios are involved:

  - You can add tags to an object with no tags associated with it.
  - You can replace the existing tags associated with an object.
- **GET Object tagging**: Retrieves the tags associated with an object.
- **DELETE Object tagging**: Deletes the tags associated with an object.

The following Object APIs also support tagging:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 960

- GET Object (returns tag count, if any)
- PUT Object
- PUT Object-Copy
- Initiate Multipart Upload

S3 Select API Overview

S3 Select is a feature to select partial content of an object and returns the result.

With S3 Select feature, you can only fetch the content of interest. This allows applications to speed up their queries drastically as the size of the sub-set of object is smaller compared to the actual size of the entire object. S3 Select is supported on objects stored in CSV format and returns the result in CSV format.

> **Note:** S3 select does not support compression.

The `SelectObjectContent` API filters the contents of an object located in Nutanix Objects using an SQL statement. In the request, you must specify the SQL expression and data serialization format (CSV) of the object. Objects uses this format to parse object data into records, and returns only records that match the specified SQL expression. You must also specify the data serialization format (CSV) for the response.

Basic Command Support

Objects S3 Select feature support only the `SELECT` SQL command.

The S3 Select query operates on a single object. The primary commands involves data selection and filtering.

The following clauses are supported for the SELECT command.

- SELECT list: The `SELECT` list names the columns, functions, and expressions that you want the query to return.

  The following are supported:

  - Aggregate operators such as AVG, COUNT, MAX, MIN
  - Arithmetic operations (For example, +, /)
  - _1, _2 positional operators for CSV.
- FROM clause: Using `FROM` clause, you can select from arrays or objects within a JSON object. You can use `S3Object` as a basic reference.
- WHERE clause: The `WHERE` clause filters rows based on the *condition*. A condition is an expression that has a Boolean result.

  The following conditions are supported:

  - AND, NOT, OR operators
  - Comparision (For example, <, >=)
  - Pattern matching (For example, LIKE, %)
- LIMIT clause: The `LIMIT` clause limits the number of records that you want the query to return based on *the number*.

The following is the general syntax of a `SELECT` query.

```
SELECT fields FROM S3Object WHERE condition LIMIT num
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 961

Note: The specific parameters differ based on the format and schema of the object.

For more information about the supported SQL functions, refer to Supported SQL Functions on page 247.

Requirements

The following is the requirement for using S3 SELECT:

- You must have `s3:GetObject` permission for the object you are querying.

Limitations

The following are limitations for using S3 SELECT:

- The maximum length of a SQL expression is 256 KB.
- The maximum length of a record in the input or result is 1 MB.
- Complex operations like sub-queries or joins are not supported.

Supported SQL Functions

S3 Select supports the following SQL functions.

Table 28: Type of Supported Functions

Type of Functions	Functions with Parameters
Aggregate	**avg (X)**: Returns the average value of all X within a group. String and BLOB values that are not numbers are interpreted as 0. **count (X) or count(*)**: Returns a count of the number of times X is in a group. The count(*) function (with no arguments) returns the total number of rows in the group. **max(X)**: Returns the maximum value of all values in the group. It is the value that is returned last in an ORDER BY on the same column. **min(X)**: Returns the minimum value of all values in the group. This is the first value that appears in an ORDER BY of the column. **sum(X)**: Returns sum of all values in the group.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 962

Type of Functions	Functions with Parameters
Conditional	**CASE**: A CASE expression is similar to IF-THEN-ELSE. The optional expression that occurs in between the CASE keyword and the first WHEN keyword is called the *base* expression. There are two forms of the CASE expression: • **A CASE with a base expression**: The base expression is evaluated just once and the result is compared against the evaluation of each WHEN expression from left to right. The result of the CASE expression is the evaluation of the THEN expression that corresponds to the first WHEN expression for which the comparison is true. Or, if none of the WHEN expressions evaluate to a value equal to the base expression, the result of evaluating the ELSE expression, if any. If there is no ELSE expression and none of the WHEN expressions produce a result equal to the base expression, the overall result is NULL. • **A CASE without a base expression**: Each WHEN expression is evaluated and the result treated as a boolean, starting with the leftmost and continuing to the right. The result of the CASE expression is the evaluation of the THEN expression that corresponds to the first WHEN expression that evaluates to true. Or, if none of the WHEN expressions evaluate to true, the result of evaluating the ELSE expression, if any. If there is no ELSE expression and none of the WHEN expressions are true, then the overall result is NULL. A NULL result is considered untrue when evaluating. **coalesce(X,Y,...)**: Returns a copy of the first argument, or NULL if all arguments are NULL. Coalesce() must have at least 2 arguments. **nullif(X,Y)**: Returns its first argument if the arguments are different and NULL if the arguments are the same. This function searches its arguments from left to right for an argument that defines a collating function and uses that collating function for all string comparisons.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 963

Type of Functions	Functions with Parameters
Conversions	**CAST**: A CAST expression of the form *CAST(expr AS type-name)* is used to convert the value of *expr* to a different storage class specified by *type-name*. The following are the Conversion Processing ways for the different *type-name*: • Casting a value with no affinity converts into a BLOB. Casting to a BLOB first casts the value to TEXT, then interprets the resulting byte sequence as a BLOB instead of TEXT. • Casting a BLOB value to TEXT, the sequence of bytes that make up the BLOB is interpreted as text encoded using the database encoding. • Casting a BLOB value to a REAL, the value is first converted to TEXT. • Casting a BLOB value to INTEGER, the value is first converted to TEXT. • Casting a TEXT or BLOB value into NUMERIC yields either an INTEGER or a REAL result.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 964

Type of Functions	Functions with Parameters
Date	**date(time-value, modifier, modifier, ...)** **time(time-value, modifier, modifier, ...)** **datetime(time-value, modifier, modifier, ...)** All the date and time functions take a time value as an argument. The time value is followed by zero or more modifiers. The date() function returns the date in the `YYYY-MM-DD` format. The time() function returns the time in the `HH:MM:SS` format. The datetime() function returns in the `YYYY-MM-DD HH:MM:SS` format. **strftime(format, time-value, modifier, modifier, ...)** The strftime() function takes a format string as its first argument. It returns the formatted date according to the format string specified as the first argument. The following is a list of valid strftime() substitutions: • %d - day of month: 00 • %f - fractional seconds: SS.SSS • %H - hour: 00-24 • %j - day of year: 001-366 • %J - Julian day number • %m - month: 01-12 • %M - minute: 00-59 • %s - seconds since 1970-01-01 • %S - seconds: 00-59 • %w - day of week 0-6 with Sunday==0 • %W - week of year: 00-53 • %Y - year: 0000-9999 • %% - %

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 965

Type of Functions	Functions with Parameters
String	**length(X)**: Returns the following based on the value of X: • For a string value, returns the number of characters (not bytes) in X prior to the first NULL character, • For a blob value, returns the number of bytes in the blob. • For a NULL value, returns NULL. • For a numeric value, returns the length of a string representation of X. **lower(X)**: Returns a copy of string X with all ASCII characters converted to lower case. **Note:** The default lower() function works for ASCII characters only. **substring(X,Y,Z)**: Returns a substring of input string X that begins with the Y-th character and which is Z characters long. Returns the following based on different scenarios: • If Z is omitted, returns all characters through the end of the string X beginning with the Y-th. • If Y is negative, then the first character of the substring is found by counting from the right rather than the left. • If Z is negative, then the Z characters preceding the Y-th character are returned. • If X is a string, then the indices refer to actual UTF-8 characters. • If X is a BLOB, then the indices refer to bytes. **ltrim(X,Y)**: Returns a string formed by removing any and all characters that appear in Y from the left side of X. If the Y argument is omitted, ltrim(X) removes spaces from the left side of X. **rtrim(X,Y)**: Returns a string formed by removing any and all characters that appear in Y from the right side of X. If the Y argument is omitted, rtrim(X) removes spaces from the right side of X. **trim(X,Y)**: Returns a string formed by removing any and all characters that appear in Y from both ends of X. If the Y argument is omitted, trim(X) removes spaces from both ends of X. **upper(X)**: Returns a copy of input string X in which all lower-case ASCII characters are converted to their upper-case equivalent.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 966

ERROR RESPONSES

This section provides reference information about Objects errors responses and codes. When Objects request returns an error, the client receives an error response. The format of the error response is API specific; however, all the error responses have common elements.

REST Error Responses

When an error occurs, the header information contains the following: Content-Type: application/xml; An appropriate status code.

Table 29: REST Error Responses

Name
Code
Error
Message
RequestId
Resource

For more information about Error Responses, refer to the *REST Error Responses* section in the *Amazon Simple Storage Service API Reference Guide*.

List of Error Codes

The following table lists the error codes:

Table 30: Error Codes

Error Code	HTTP Status Code
AccessDenied	403 Forbidden
AuthorizationHeaderMalformed	400 Bad Request
BadDigest	400 Bad Request
BucketAlreadyExists	409 Conflict
BucketAlreadyOwnedByYou	409 Conflict
BucketNotEmpty	409 Conflict
EntityTooSmall	400 Bad Request
EntityTooLarge	400 Bad Request
IncompleteBody	400 Bad Request
InlineDataTooLarge	400 Bad Request
InternalError	500 Internal Server Error
InvalidAccessKeyId	403 Forbidden

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 967

Error Code	HTTP Status Code
InvalidArgument	400 Bad Request
InvalidBucketName	400 Bad Request
InvalidBucketState	409 Conflict
InvalidDigest	400 Bad Request
InvalidLocationConstraint	400 Bad Request
InvalidObjectState	403 Forbidden
InvalidPart	400 Bad Request
InvalidPartOrder	400 Bad Request
InvalidPolicyDocument	400 Bad Request
InvalidRange	416 Requested Range Not Satisfied
InvalidRequest	400 Bad Request
InvalidURI	400 Bad Request
KeyTooLongError	400 Bad Request
MalformedACLError	400 Bad Request
MalformedPOSTRequest	400 Bad Request
MalformedXML	400 Bad Request
MaxMessageLengthExceeded	400 Bad Request
MaxPostPreDataLengthExceededError	400 Bad Request
MetadataTooLarge	400 Bad Request
MethodNotAllowed	405 Method Not Allowed
MissingContentLength	411 Length Required
MissingRequestBodyError	400 Bad Request
NoSuchBucket	404 Not Found
NoSuchBucketPolicy	404 Not Found
NoSuchKey	404 Not Found
NoSuchLifecycleConfiguration	404 Not Found
NoSuchUpload	404 Not Found
InvalidVersion	404 Not Found
NotImplemented	501 Not Implemented
OperationAborted	409 Conflict
PermanentRedirect	301 Moved Permanent
PreconditionFailed	412 Precondition Failed
Redirect	307 Moved Temporarily
RequestIsNotMultiPartContent	400 Bad Request
RequestTimeout	400 Bad Request
RequestTimeTooSkewed	403 Forbidden

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 968

Error Code	HTTP Status Code
SignatureDoesNotMatch	403 Forbidden
ServiceUnavailable	503 Service Unavailable
SlowDown	503 Slow Down
TemporaryRedirect	307 Moved Temporarily
UnexpectedContent	400 Bad Request

For more information about the List of Error Codes, refer to the *List of Error Codes* section in the *Amazon Simple Storage Service API Reference Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 969

INTEGRATION WITH BACKUP APPLICATIONS

Objects is ideal for cost-effective, scale-out storage. It provides a fully distributed, API-accessible storage platform that integrates directly into applications or is used for backup, archiving, and data retention. Objects offers you a seamless way to switch from your traditional backup to object store backup. You can also perform multipart uploads. Objects supports integration with back up applications such as Commvault, HYCU, Veeam and Veritas.

> **Note:** Some backup vendors have configurable size limits if larger than 5 TiB VM images need to be backed up (For example, HYCU). The backup appliance configuration needs to be changed in order to take advantage of the larger size limit in Nutanix Objects.

For more information about Commvault Integration, refer to *Commvault with Nutanix* guide on the Nutanix Support Portal.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 970

TROUBLESHOOTING OBJECTS

This section explains how to troubleshoot issues that you might encounter while using Objects.

Handling Deployment Failure

In case you encounter any deployment failure, contact Nutanix Support at https://portal.nutanix.com/.

Shutting Down Objects VMs

This section describes the steps to perform a graceful shutdown of Objects VMs on AHV or ESXi.

Before you begin

Make sure all read and write operations are stopped from the application before shutting down the VM.

About this task

> **Warning:** Ensure that you only perform shutdown operations as described in this procedure. Do not perform any destructive actions such as deleting a VM.

To shut down Objects VMs, do the following:

Procedure

1. Log on to the Prism Central web console, and select **Objects** in the Application Switcher.
2. Copy the Object Stores cluster name.

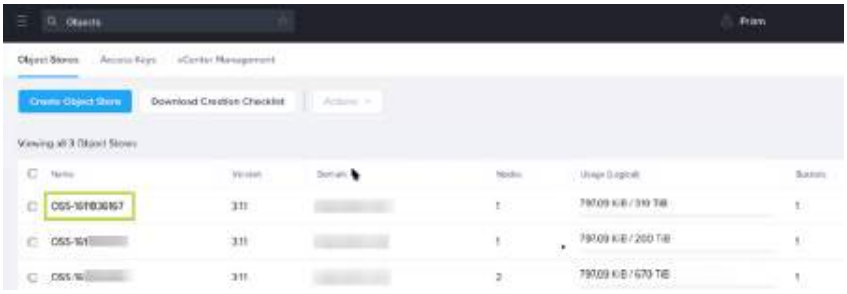


Figure 161: Object Store Cluster

3. SSH into any CVM on the Prism Element cluster where the object store is deployed.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 971

4. To view the list of VMs, do any one of the following:

   » **AHV**: To view the list of VMs, run the following command.

   ```
   nutanix@NTNX-18FM6F370127-A-CVM:xx.xx.xxx.xx:~$ acli vm.list |grep '<objectstore-name>' -i
   ```

   For example, `nutanix@NTNX-18FM6F370127-A-CVM:xx.xx.xxx.xx:~$ acli vm.list |grep 'OSS-1611836167' -i`, where `OSS-1611836167` is the object store name.

   ```
   nutanix@NTNX-18FM6F370127-A-CVM:XX.XX.XXX.XX:~$ acli vm.list |grep 'OSS-1611836167' -i

   oss-1611836167-898db8-default-0 6596b630-cacd-48bd-90b5-b4f1698e260a

   oss-1611836167-898db8-ijpsvgbict-envoy-0 c25b5fd8-2787-46b6-b3b4-c982f6ddf1b9
   ```

   » **ESXi**: To view the list of VMs in vCenter, click **Hosts and Clusters** tab, expand the ESXi cluster.

   The list of VMs appear.

   To find the primary and secondary MSP clusters, run the command `mspctl cluster list`. If the *cluster_type* value is `primary_msp`, then the cluster is a primary MSP cluster. Rest clusters are secondary.

   > **Note:** It is recommended to shut down the envoy VMs first, and then proceed to shut down the worker VMs. Also, ensure that the primary cluster is shut down at last as it hosts all the common services such as IAM.

5. To shut down the VMs, do any one of the following:

   » **AHV**: Run the following command:

   ```
   acli vm.shutdown <vm name>
   ```

   » **ESXi**: Right click the VM, and then click **Power** > **Power Off**.

   > **Note:** First shut down the envoy VMs.

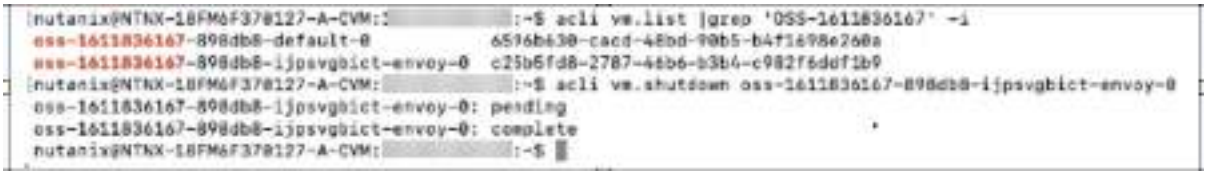
   

   Figure 162: Shutting Down the VMs: AHV

   For AHV, you can check the status of the VM from the Prism Central web console. Click the **Hamburger icon** > **Virtual Infrastructure** > **VMs** and confirm that the status of the VM is shown as `Off` in the **Power State** column.

   For ESXi, you can check the status of the VM from the vCenter. Click the **Hosts and Clusters** tab, and expand the cluster where the VM is listed, and confirm that the status of the VM is shown as `Off`.

6. Perform Step 5 for all the VMs within the cluster.

What to do next

You can also start the Objects VMs. Refer to Starting the Objects VMs on page 258.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 972

Starting the Objects VMs

This section describes the steps to start the Objects VM after performing a graceful shutdown of Objects VMs on AHV or ESXi.

About this task

> **Warning:** Ensure that you only perform power on operations as described in this procedure. Do not perform any destructive actions such as deleting a VM.

To start the Objects VMs, do the following:

Procedure

1. Log on to the Prism Central web console, and select **Objects** in the Application Switcher.
2. Copy the Object Stores cluster name.

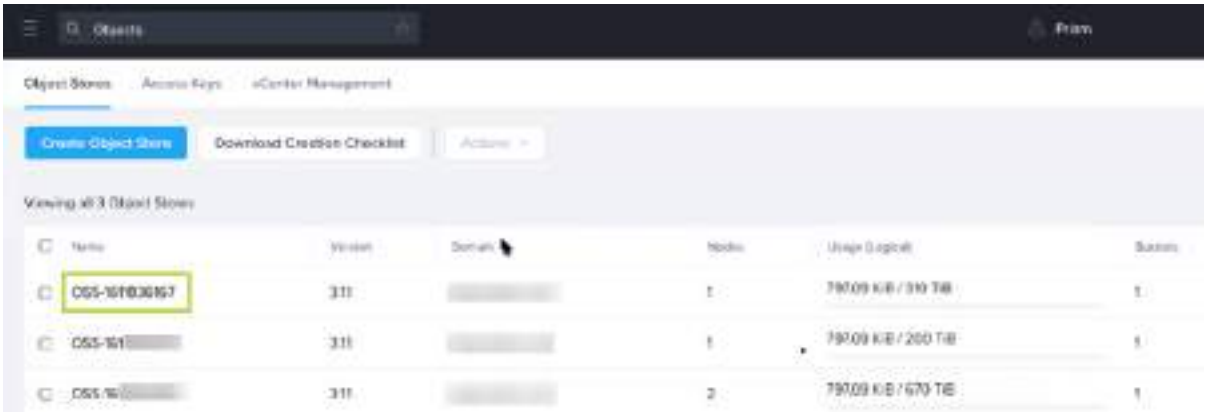


Figure 163: Object Store Cluster

3. SSH into any CVM on the Prism Element cluster where the object store is deployed.
4. To view the list of VMs, do any one of the following:

   » **AHV**: To view the list of VMs, run the following command.

   ```
   nutanix@NTNX-18FM6F370127-A-CVM:xx.xx.xxx.xx:~$ acli vm.list |grep '<objectstore-name>' -i
   ```

   For example, `nutanix@NTNX-18FM6F370127-A-CVM:xx.xx.xxx.xx:~$ acli vm.list |grep 'OSS-1611836167' -i`, where `OSS-1611836167` is the Object Store name.

   ```
   nutanix@NTNX-18FM6F370127-A-CVM:XX.XX.XXX.XX:~$ acli vm.list |grep 'OSS-1611836167' -i

   oss-1611836167-898db8-default-0 6596b630-cacd-48bd-90b5-b4f1698e260a

   oss-1611836167-898db8-ijpsvgbict-envoy-0 c25b5fd8-2787-46b6-b3b4-c982f6ddf1b9
   ```

   » **ESXi**: To view the list of VMs in vCenter, click **Hosts and Clusters** tab, expand the ESXi cluster.

   The list of VMs appear.

   To find the primary and secondary MSP clusters, run the command `mspctl cluster list`. If the *cluster_type* value is `primary_msp`, then the cluster is a primary MSP cluster. Rest clusters are secondary.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 973

5. To start the VMs, do any one of the following:

   » **AHV**: Run the following command:

   ```
   acli vm.on <vm name>
   ```

   » **ESXi**: Right click the VM, and then click **Power** > **Power On**.

   Note: First start the worker VMs.

6. Check the following to ensure that the VMs are powered on.

   - For AHV, in the Prism Central web console, go to the **VMs** page. Select the VM that you powered on using the acli and perform the **Launch Console** action. You will view the login prompt if the VM is powered on.

     For ESXi, you can check the status of the VM from the vCenter. Click **Hosts and Clusters** tab, and expand the cluster where the VM is listed, and confirm that the status of the VM is shown as `On`.

   - In the Prism Central web console, go to **Entity Menu** > **Services** > **Objects**. Check for the following points for your Objects cluster:

     - Statistics are visible in the Buckets and Objects columns.
     - Click on the corresponding Objects cluster to check if it is reachable. After the Object Store page opens, check if the various statistics are visible. For example, Performance, Usage Summary, and so on.
     - In the Alerts page, ensure that there are no active alerts. If there are active alerts, wait for a few minutes. If the alerts persist, contact Nutanix Support.
     - Perform read and write operations to ensure that the object cluster is running.

Detection of Slow Connections

Nutanix Objects can detect slow-performing client connections to Objects.

Any client connection must be able to read or write data at the rate of 2 MiB in every 600 seconds window (translates to approximately 4 KiB/s throughput). A client connection that is not able to transfer 2 MiB data in 600 seconds window will be treated as a slow connection.

Any slow connection will be terminated immediately to avoid Denial of Service (DoS) attacks and better manage the resources on the server.

Note: Up to 1000 active connections are accepted by each Objects endpoint. The slow-performing client connections can potentially consume all slots and cause Denial of Service (DoS).

Prism Element Clusters or Subnets Not Listed in the User Interface

You might see that the **Cluster** drop down or the **Subnets** drop-down shows empty list or an error message when no Prism Element clusters or subnets are available for deployment respectively. Or you might see that no Prism Element clusters are listed during the addition of multi-cluster to the Object Store.

The following are the possible causes for the Prism Element clusters or subnets to not appear in the user interface:

- No other Prism Elements are registered to the Prism Central.
- Prism Element was just registered but the sync between the Prism Element and the Prism Central is not complete yet.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 974

- The logged in user does not have access to any Prism Element.
- The admin has just created an access policy granting user access to a Prism Element.
- The logged in user does not have access to any subnets on the allowed Prism Element.
- The admin has just created an access policy granting user access to a Subnet.

> **Note:** If you are just registered to Prism Element, or you have been just granted access, try again in 5 minutes.

Object Stores Not Listed While Creating a Replication Rule

You might see that while creating a replication rule for a bucket, the **Object Store** drop-down under **the Destination** section shows an empty list.

The following are the possible causes for the object stores to not appear in the user interface:

- The logged in user does not have permission to view the object store.
- The deployment of the object store is not in **a Complete** state.
- The object store version is lower than Objects 3.0 version.

Manually Updating the DNS Server for an Objects Cluster

When the DNS servers are updated in the managed network that is used by Objects deployments, they are not automatically updated in the MSP VMs for these Objects deployments. For updating them, you have to either restart the network service or restart the VMs. So, to overcome this issue, you can manually update the DNS servers for each of the Objects clusters using the managed network.

About this task

To manually update the DNS servers for an Objects cluster, do the following:

Procedure

1. From the Prism Element CLI, update the name servers in the AHV managed networks.

   ```
   nutanix@PCVM:~$ acli net.update_dhcp_dns network_name servers=new server list
   ```

   For example,

   ```
   nutanix@NTNX-10-44-15-64-A-PCVM:~$ acli net.update_dhcp_dns OssNet
    servers=10.40.64.16
   ```

2. Update `etc/resolv.conf` manually on the Objects cluster with the new name servers.

   ```
   nutanix@PCVM:~$ mspctl cluster ssh cluster --all --cmd "sudo chattr -i /etc/
   resolv.conf"
   ```

   For example,

   ```
   nutanix@NTNX-10-44-15-64-A-PCVM:~$ mspctl cluster ssh dns-test-store --all --cmd
    "sudo chattr -i /etc/resolv.conf"
   ```

   a. Remove each old name server by running the following command.

   > **Caution:** Do not remove 127.0.0.1 entry.

   ```
   nutanix@PCVM:~$ mspctl cluster ssh cluster --all --cmd "sudo sed -i '/
   nameserver old_ip_address/d' /etc/resolv.conf"
   ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 975

For example,

```
nutanix@NTNX-10-44-15-64-A-PCVM:~$ mspctl cluster ssh dns-test-store --all --cmd
 "sudo sed -i '/search /i nameserver 10.40.64.16' /etc/resolv.conf"
```

b. For each name server, add entry in all nodes of the Objects clusters.

```
nutanix@PCVM:~$ mspctl cluster ssh cluster --all --cmd "sudo sed -i '/search /i
 nameserver new_ip_address' /etc/resolv.conf
```

For example,

```
nutanix@NTNX-10-44-15-64-A-PCVM:~$ mspctl cluster ssh dns-test-store --all --cmd
 "sudo sed -i '/search /i nameserver 10.40.64.16' /etc/resolv.conf"
```

```
nutanix@PCVM:~$ mspctl cluster ssh cluster --all --cmd "cat /etc/resolv.conf"
```

For example,

```
nutanix@NTNX-10-44-15-64-A-PCVM:~$ mspctl cluster ssh dns-test-store --all --cmd
 "cat /etc/resolv.conf"
```

3. Identify all the DNS pods.

```
nutanix@PCVM:~$ mspctl cluster ssh cluster_name
sudo kubectl get pods -A | grep -i dns
```

For example,

```
nutanix@NTNX-10-44-15-64-A-PCVM:~$ mspctl cluster ssh dns-test-store
================== 10.44.90.142 ==================
[nutanix@dns-test-store-16dcfd-default-0 ~]$ sudo kubectl get pods -A | grep -i dns
```

4. Restart all the DNS pods. For each pod, run the following command:

```
nutanix@PCVM:~$ mspctl cluster ssh <cluster_name>
kubectl delete pod -n namespace pod
```

For example, for pod `coredns-d9bfcdf7f-5xtc7`, run the following command:

```
nutanix@NTNX-10-44-15-64-A-PCVM:~$ mspctl cluster ssh dns-test-store
================== 10.44.90.142 ==================
[nutanix@dns-test-store-16dcfd-default-0 ~]$ kubectl delete pod -n kube-
system coredns-d9bfcdf7f-5xtc7
```

5. Restart the *dnsmasq systemd* service.

```
nutanix@PCVM:~$ mspctl cluster ssh cluster --all --cmd "sudo systemctl restart
 dnsmasq"
```

For example,

```
nutanix@NTNX-10-44-15-64-A-PCVM:~$ mspctl cluster ssh dns-test-store --all --cmd
 "sudo systemctl restart dnsmasq"
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 976

COPYRIGHT

Copyright 2024 Nutanix, Inc.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Nutanix and the Nutanix logo are registered trademarks of Nutanix, Inc. in the United States and/or other jurisdictions. All other brand and product names mentioned herein are for identification purposes only and may be trademarks of their respective holders.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 977

v3.1 | April 2023 | RA-PC21

REFERENCE ARCHITECTURE

Nutanix Hybrid Cloud Reference Architecture

NUTANIX
YOUR ENTERPRISE CLOUD

Copyright

Copyright 2023 Nutanix, Inc.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Nutanix and the Nutanix logo are registered trademarks of Nutanix, Inc. in the United States and/or other jurisdictions. All other brand and product names mentioned herein are for identification purposes only and may be trademarks of their respective holders.

Contents

1. Introduction....5
Vision for Private, Hybrid, and Multicloud....5
Design Objectives....7
Audience....11
Design Decisions....11
How To Use This Reference Architecture?....11

2. Architecture Overview....13
Physical Layer....13
Virtualization Layer....18
Management Layer....19
Business Continuity Layer....20
Automation Layer....22
Security and Compliance Layer....23

3. High-Level Design Considerations....27
Choosing A Datacenter Architecture....27
Choosing a Hypervisor....35
Choosing a Cluster Deployment Model....37
Choosing How You Will Scale....42
Choosing a Control Plane....43
Choosing the Right Licensing and Support....46
Choosing the Right Hardware for Your Workload Types....51

4. Detailed Technical Design....55
Required Software Versions....55
Physical Layer Design....56
Virtualization Layer Design....120
Management Layer Design....127
Security Layer Design....134
Automation Layer Design....148
Operations Design....153

5. Multidatacenter Design for Nutanix Core and Business Continuity and Disaster Recovery....160

Choosing the Right Business Continuity and Disaster Recovery Solution....160
Multidatacenter Design....162
Replication Options....164
Disaster Recovery Decision Tree....173
ROBO Patterns....187
Control Planes....190

6. Incorporating Optional Nutanix Products and Services....205
Prism Operations....206
Nutanix Cloud Clusters for Hybrid and Multicloud Operations....214
Nutanix Flow for Microsegmentation....225
Nutanix Files for Integrated File Services....232
Nutanix Objects for Integrated Object Storage....245
Nutanix Mine for Integrated Backup....257
Calm Application Orchestration....262
Karbon for Kubernetes and Container Support on Nutanix....272
Era for Database as a Service....281

7. Conclusion....292

Appendix....293
Table of Design Decisions....293

List of Figures....304

List of Tables....309

1. Introduction

Vision for Private, Hybrid, and Multicloud

The Nutanix vision for cloud computing environments started in the datacenter with innovative solutions for private cloud, which greatly reduced the complexity and effort required to deploy and manage software-defined storage, compute, and networking infrastructure. In recent years, Nutanix's vision has expanded to include architectures for hybrid and multicloud that offer more alternatives to optimize costs.

Which type of cloud to use for a specific use case depends on a variety of characteristics of multi-tiered applications. These can be summarized in terms of:

- Use Case: web servers, application servers, databases, and so on
- Workload Type: virtual machines (VMs) or containers
- Storage Format: block, object, file
- Security Policies: requirements that could rule out the option to host workloads on particular public clouds
- Unique Requirements: items like machine learning hardware or media transcoding that can only be met by the unique features of one specific Public Cloud offering (for example serverless computing, analytics, PaaS, and so on)

These characteristics ultimately shape an organization's cloud architectures and drive the decisions regarding where to host each application tier in a particular service.

Historically, the hosting architecture for multitiered applications didn't change without a labor-intensive migration. Nutanix innovation gives IT organizations the flexibility to dynamically place workloads. The Nutanix distributed architecture natively includes the ability to provision the same application blueprints in four different cloud configurations.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 982

Table 1: Cloud Configurations

Cloud Configuration	Description
Private	Hosted on prem on AHV and/or VMware.
Hybrid	Some hosted on prem on AHV and/or vSphere and some hosted in AWS, Azure, or GCP.
Public (natively)	Hosted in AWS, Azure, or GCP as a native public cloud service offering.
Public (bare metal)	Hosted as bare metal in AWS running Nutanix Acropolis Operating System (AOS).

Nutanix further extends these cloud configurations by enabling the following four architectural principles:

Table 2: Architectural Principles

Architectural Principle	Description
Application Mobility	Multi-tiered applications can be aligned across all cloud providers to maximize architectural symmetry and promote application mobility.
Increased Standardization	Use of the same hardened OS gold image and business process orchestration (e.g. ITSM integration, approvals, emails, showback/ chargeback, etc.) across all cloud configurations.
Policy-Based Security Governance	Hosted in AWS, Azure, or GCP as a native public cloud service offering.
Policy-Based Cost Governance	Optimize cost by hosting workloads on the platform that meets the requirements of the service and has the lowest Total Cost of Ownership (TCO).

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 983

All of these principles contribute to an advanced hybrid and multicloud strategy that simplifies IT, stretches budgets, and accelerates time to value. This document provides the architecture and design-driven decisions to help our customers realize this strategic vision.

Figure 1: Nutanix Hybrid and Multicloud Strategy

Design Objectives

The objective of this document is to define, explore, and develop key design decisions required when implementing private, hybrid, or multicloud solutions based on the Nutanix platform. The objective can be further broken down as follows:

- To identify and enumerate the key design decisions that need to be documented in order to support a robust design methodology and practice.
- To explore each design decision, evaluating key viable options, tools, and methods for implementation and management so that organizations can make informed decisions relating to their specific design requirements.

Since simplicity is a key principle of all Nutanix products, some requirements may be met through native platform architecture without the need for superfluous design decisions, which are often required by competing platforms. The objective of this document is therefore not to educate readers about Nutanix features and functions, even though this may naturally occur as a side

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 984

benefit. In these cases, this document will explain how these requirements are addressed by Nutanix-native features.

The design objectives of this document for the Hybrid Cloud implementations are as follows:

Table 3: Design Objectives of this Document for Private Cloud Implementations

Design Objectives	Description
Key objective	The platform is capable of hosting and provisioning workloads.
Workload Types	Virtual Machines and containers
Scope of deployment	Greenfield deployment that is adaptable to brownfield deployments with workload migrations.
Cloud type	Hybrid cloud
Number of regions	• Two regions. Region 1 provides two availability zones for resiliency. Region 2 provides long-term backup retention for recovery from disasters impacting all of Region 1. • Services must be available across two availability zones during normal production. Services must be available within one availability zone during disaster recovery. • A minimum distance of 300km between Region 1 (primary) and Region 2 (DR). • Provide running workloads and disaster recovery services in same region.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 985

Design Objectives	Description
Availability	• SLA 24/7 • Uptime 99.999% across availability zones › Applies to certain production workloads › Scheduled downtime not included › 99% uptime required during disaster recovery scenario • RPO – 0 min across availability zones › Applies to certain production workloads › RPO = 0 can be achieved at the application layer for some services but the infrastructure layer must support RPO = 0 • RTO – 5 min across availability zones. › Applies to certain production workloads
Disaster Recovery	• DR RPO = 60 min between primary availability zones and DR availability zone • DR RTO = 24h between primary availability zones and DR availability zone • Best effort RTO in the region where production workloads are running and the disaster recovery capabilities fails.
Minimum number of nodes per cluster	3 nodes.
Maximum number of workloads	Unlimited number of workloads dependent on the pod based constructs described herein.
Types of Clusters	Management, Workload, Storage Heavy, Edge Clusters.
Virtualization	• Nutanix AHV and VMware ESXi hypervisors. • While Nutanix supports Microsoft Hyper-V, it is not considered in this design.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 986

Design Objectives	Description
Management Plane	Nutanix Prism Element, Nutanix Prism Central, and VMware vCenter.
Scope	• Sizing recommendations and methodology for the amount of software-defined storage, compute and networking. • Physical implementation of storage, compute, and networking. • Logical configuration of clusters. • Scalability methods and recommendations. • Automation relating to cluster build, expansion, and lifecycle management. • Management and operations aspects such as capacity management, reporting, upgrades, backup and restore, monitoring and alerting, and logging.
Authentication, authorization, and access control	Microsoft Active Directory users and groups tied to Role Based Access Control.
Security Policy & Enforcement	• Least privilege access policies will be implemented so that end-users and administrators will need to be members of groups in order to be able to perform secure aspects of their job function. • Certificates are signed by a trusted certificate authority (CA). • Hardening of platform associated with hypervisor, control plane, and data plane. • Security policy definition and enforcement of drift away from defined policies and checksum verification. • Separation of traffic classes such as management and application.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 987

Audience

This document for Multi Datacenter design is intended for infrastructure architects, infrastructure administrators, and infrastructure operators who want to deploy and manage datacenters based on Nutanix Enterprise Cloud, to address requirements for availability, capacity, performance, scalability, business continuity, and disaster recovery.

Design Decisions

This document makes recommendations and guides the reader to appropriate decisions where possible. In cases where a design decision is required, this document describes possible options.

Table 4: Design Decision Example

NET-001	Title Of Design Decision
Justification	Justification to support why the decision was made.
Implication	Additional implications as a result of the design decision.

Note: Appendix I: Table of Design Decisions includes a list of all the design decisions described throughout this document.

How To Use This Reference Architecture?

This document is subdivided into five major sections as follows:

Architectural Overview

Introduces key Architecture concepts that will be discussed throughout this design.

Design Considerations

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 988

Discusses key design considerations that will vary for each customer. Customers will be required to make decisions that will influence the design and build of their end-solution.

Detailed Design

Identifies key design decisions and in most cases determines the optimal configuration and decision that will be used for validating the design. For design decision, alternate options may be discussed along with pros and cons. For good reasons, Customers may choose to deviate from the decisions made in this document. The decisions made in this section are recommended by Nutanix, however they are by no means meant to be the only method, and Nutanix recognizes that alternate decisions may be appropriate depending on specific requirements.

Multi-site Design, Disaster Recovery and Business Continuity

Articulates considerations for designing across multiple data centers, and the related DR/BC architecture.

> Note: This section does not provide detailed operational guides or runbooks.

Incorporating Optional Nutanix Services

Describes the design considerations for additional services that can optionally be deployed in a Nutanix environment to address specific requirements. The list of capabilities covered includes: management automation, Nutanix deployment in public cloud, advanced security capabilities, file and object data services, integrated backup options, application orchestration, container support, and database-as-a-service (DBaaS).

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 989

2. Architecture Overview

This section describes the high-level Nutanix architecture, including major concepts and design elements that anyone designing a Nutanix deployment should understand. If you are already familiar with Nutanix hyperconverged infrastructure (HCI) and Nutanix software, you can skip this section.

The diagram below shows the high-level architecture covered in this document. This overview explains the elements in each layer. Later sections will explore the design decisions necessary for each layer.

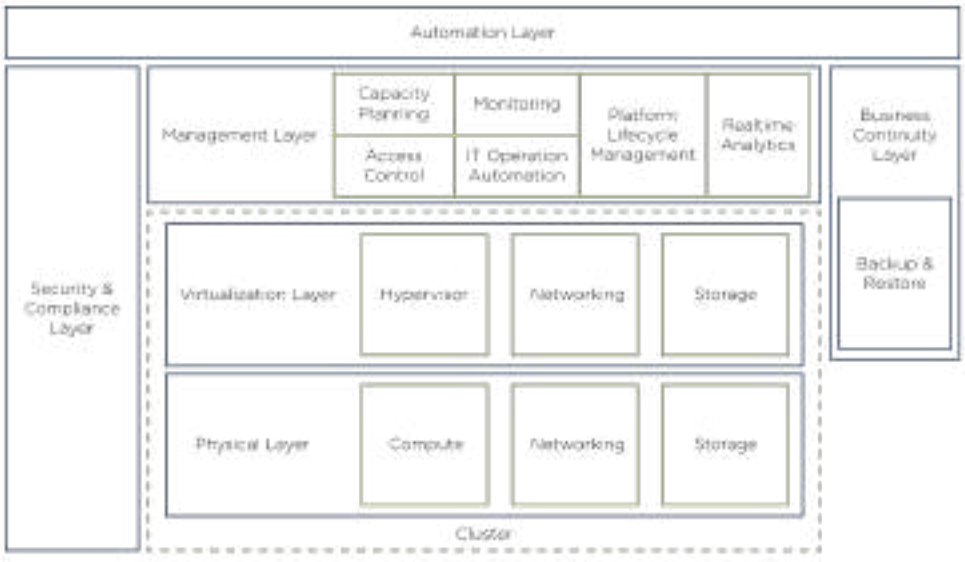


Figure 2: Architecture Overview

Physical Layer

Because the Nutanix Enterprise Cloud architecture is based on hyperconverged infrastructure, the physical layer is significantly different than it would be in a traditional datacenter architecture. Understanding the differences will allow you to make the best hardware choices for your Nutanix deployment.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 990

Hyperconverged Infrastructure

Nutanix HCI converges the datacenter stack including compute, storage, storage networking, and virtualization, replacing the separate servers, storage systems, and storage area networks (SANs) found in conventional datacenter architectures and reducing complexity. Each node in a Nutanix cluster includes compute, memory, and storage, and nodes are pooled into a cluster. The Nutanix Acropolis Operating System (AOS) software running on each node pools storage across nodes and distributes operating functions across all nodes in the cluster for performance, scalability, and resilience.

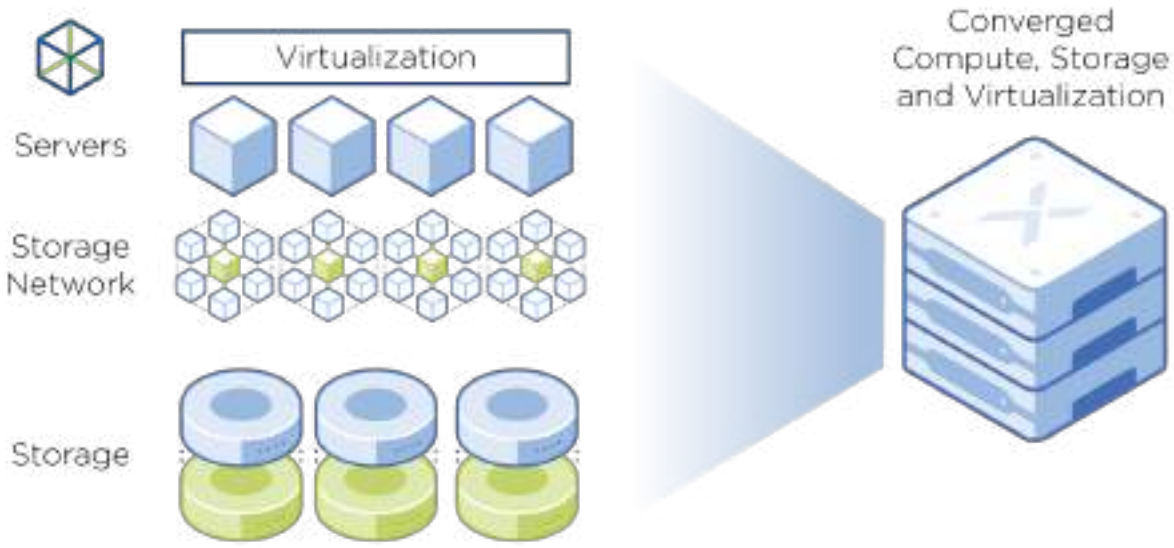


Figure 3: Hyperconverged Infrastructure

A Nutanix node runs an industry-standard hypervisor and the Nutanix Controller VM (CVM). The Nutanix CVM provides the software intelligence for the platform and is responsible for serving IO to running VMs.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 991

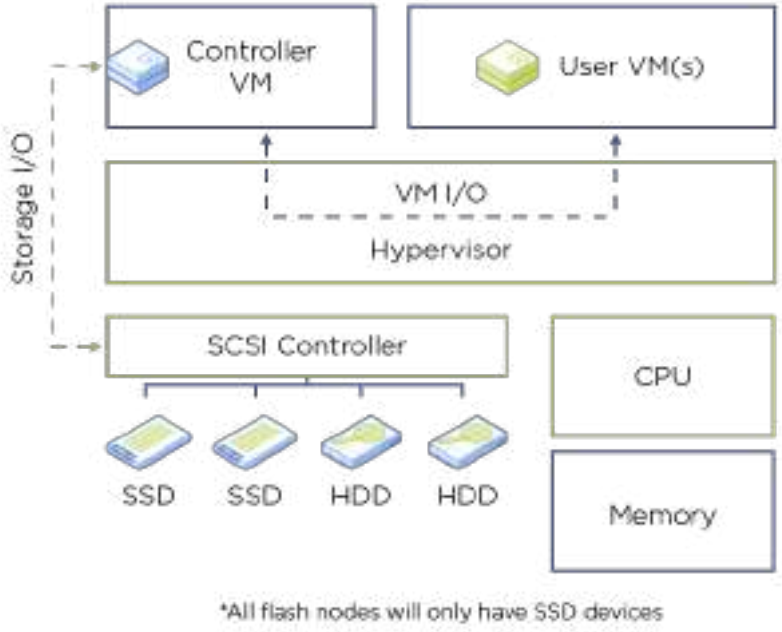


Figure 4: A Nutanix Node

Hardware Choice

Nutanix Enterprise Cloud provides significant choice when it comes to hardware platform selection. Available options include:

- Nutanix NX appliances.
- OEM appliances from leading vendors such as Dell, Lenovo, HPE, IBM, and Fujitsu.
- Other third-party servers from a wide range of vendors.

The Nutanix Support Portal contains the most up-to-date information on supported systems.

Hardware is available in a variety of chassis configurations from various vendors. Options range from multi-node chassis for high density to single-node rackmount chassis.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 992

Figure 5: Chassis Configurations

Nutanix commonly refers to all of these chassis configurations as a block.

Compute

Sizing systems to meet compute needs in a Nutanix environment is similar to other architectures. However, it's important to ensure that your design provides enough compute (CPU/RAM) to support the CVM.

Storage

Nutanix nodes offer a range of storage configurations:

- Hybrid nodes combine flash SSDs for performance and HDDs for capacity.
- All-flash nodes utilize traditional flash SSDs.
- NVMe nodes utilize NVMe SSDs.

Different node types can be mixed in the same cluster. More information is provided in the document Product Mixing Restrictions.

For data resiliency, Nutanix uses replication factor (RF), maintaining 2 or 3 data copies. This approach enables a Nutanix cluster to be self-healing in the event of a drive, node, block, or rack failure. In a Nutanix cluster consisting of multiple blocks, RF can enable block awareness. Data copies are distributed across blocks to protect against the failure of an entire block. In configurations spanning multiple racks, RF can similarly provide rack awareness with resilience to a rack outage. For more information on Nutanix data resiliency, please refer to the Nutanix Bible.

Compression, deduplication and erasure coding (EC-X) can be enabled to increase data efficiency and save capacity.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 993

Data locality and intelligent tiering ensure that the data associated with a VM is preferentially stored on that VM's local node. Active data is stored on the fastest media, delivering performance and eliminating the need for ongoing performance tuning.

Networking

Fast, low-latency and highly available networking is a key element of this document. The distributed storage architecture relies on the performance and resilience of the physical network. A good design provides high performance while maintaining simplicity.

In the detailed design section of this document we address common network topologies, selection of physical switches, and recommended connections between hosts and the physical network.

Cluster Design

A Nutanix cluster is the management boundary of the storage provided to a group of workloads. A Nutanix deployment can be architected to support either (a) mixed workloads in a single Nutanix cluster; or (b) dedicated clusters for each workload type in a block and pod design.

Designs that choose dedicated clusters may include any of the following cluster types:

Management clusters

Designed to run VMs that support datacenter management such as:

- Nutanix Prism Central.
- VMware vCenter.
- Active Directory Domain Controllers.
- Other management workloads, such as DNS, DHCP, NTP, Syslog.

Management clusters reside in the management workload domain. In this document, a management cluster occupies a separate rack or is distributed across multiple racks.

Workload clusters

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 994

Reside in a virtual infrastructure workload domain and run tenant virtual machines. You can mix different types of compute clusters and provide separate compute pools to address varying SLAs for availability and performance.

Storage clusters

Storage-only clusters provide dedicated data services to tenants. These are typically deployed for use cases focused on Object, File, or Block-level storage.

Edge/ROBO clusters

Reside at an edge and/or ROBO deployment to run virtual machines or ROBO workloads. These are typically distinguished from normal workload clusters by their small size and limited external bandwidth.

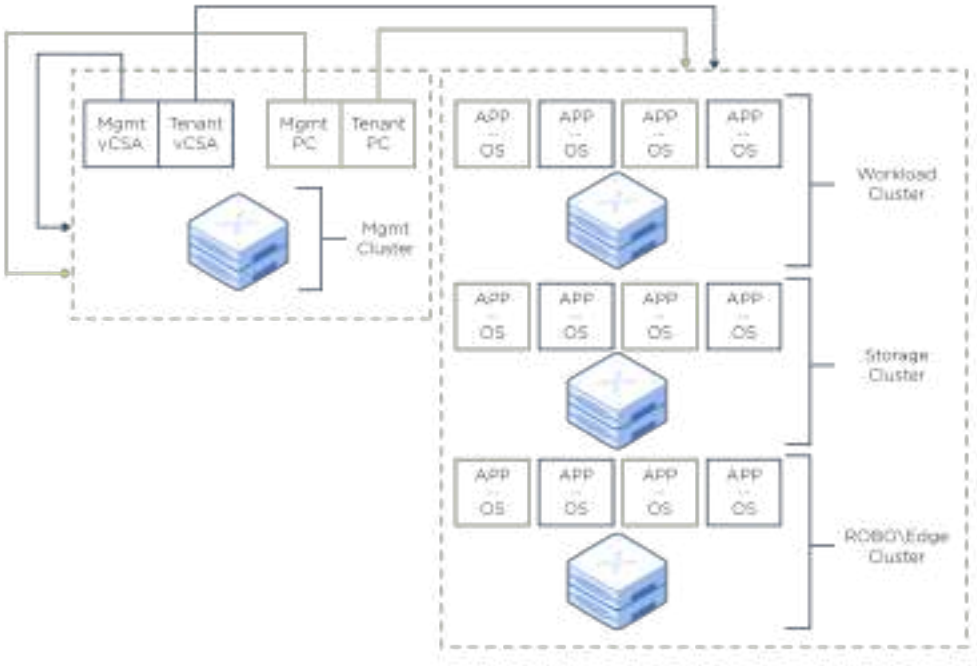


Figure 6: Cluster Design

Virtualization Layer

The virtualization layer sits logically above the physical layer, controlling access to compute, network, and storage resources. This document provides a choice between two hypervisors: Nutanix AHV and VMware ESXi. Both are enterprise-

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 995

grade hypervisors, filling a similar set of requirements and use cases. Nutanix AHV is included at no additional cost with every Nutanix node.

> Note: Nutanix HCI supports Microsoft Hyper-V, however this document does not describe deployment of this hypervisor.

Management Layer

The management layer is a key differentiator for Nutanix.

Nutanix Prism provides simplified end-to-end management for Nutanix environments. Prism combines multiple aspects of datacenter management into a single consumer-grade design that provides complete infrastructure and virtualization management, operational insights, and troubleshooting. Prism largely eliminates the need for separate management tools. All Prism functionality is also accessible via REST API.

The Prism family consists of three products that extend core capabilities:

Prism Element

The core Nutanix management platform enables management and monitoring at the cluster level for all infrastructure (compute, storage, networks) and virtualization. Key functionality of Prism includes:

- Full VM, storage, and hypervisor management.
- Network visualization.
- Role-based access control (RBAC).
- Nutanix 1-click upgrades. Prism orchestrates and streamlines platform upgrades, keeping track of the changes. Can upgrade all Nutanix software and firmware running in a Nutanix environment plus the ESXi hypervisor.

Prism Central

Enables management and monitoring of multiple Nutanix Prism Element clusters from a central interface.

Prism Pro and Ultimate

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 996

Adds advanced capabilities to the Prism platform, including performance anomaly detection, capacity planning, custom dashboards, reporting, advanced search capabilities, and task automation.

The Prism family of products are an integral part of a Nutanix cluster and do not require separate infrastructure. Prism Central runs as a separate VM, or as a cluster of 3 VMs for additional scale and resilience. More details on Nutanix management are provided later. Nutanix deployments that use the AHV hypervisor can be fully managed by Prism.

Nutanix deployments that use VMware vSphere should also include VMware vCenter Server. This is the centralized monitoring and resource management software for VMware virtual infrastructure. It performs a number of tasks, including resource provisioning and allocation, performance monitoring, workflow automation, and user privilege management.

Automated IT Operations

Prism Pro allows administrators to automate routine operational tasks, reducing administrator effort and time while increasing the quality of results. To provide this automation, Nutanix X-Play enables “if-this-then that” (IFTT) features that allow admins to create Playbooks that define automation actions that run when a particular trigger occurs.

The most common type of trigger is alert-based, where a system-defined or user- defined alert causes an action to occur. An alert could be something as simple as crossing a designated CPU or memory threshold. Other triggers can be manual; the associated playbook does not take action until an admin explicitly tells it to. With a manual trigger, an admin selects an entity such as a VM, and the specified playbook executes against it. Manual triggers allow the admin to control when and where the automation takes place. (See the section Prism Operations for more information on automation with Prism.)

Business Continuity Layer

Nutanix HCI is built with resiliency in mind including redundancy for power and other hardware components and the ability to architect resiliency for entire

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 997

datacenters. Nutanix provides multiple ways to provide business continuity including backup/restore and disaster recovery:

There are five main categories where Nutanix provides native protection, via hypervisor, third-party software, or a combination:

- Hardware
  - Self-healing from disk failure
  - Redundancy of key components
- Node
  - Node failure resiliency
  - Non-disruptive upgrades
- Data
  - Tunable redundancy
  - Nutanix Mine provides secondary storage integration and works with leading backup vendors.
- VM
  - VM-centric Protection
  - High Availability (HA)
  - ADS/DRS
  - Eco-system integration such as Nutanix Mine
- Datacenter/Site
  - Multidatacenter replication including ROBO
  - Multisite replication including ROBO
  - Cloud Connect
  - Metro Availability or synchronous replication
  - NearSync
  - Asynchronous replication
  - Nutanix Disaster Recovery as a Service (DRaaS)

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 998

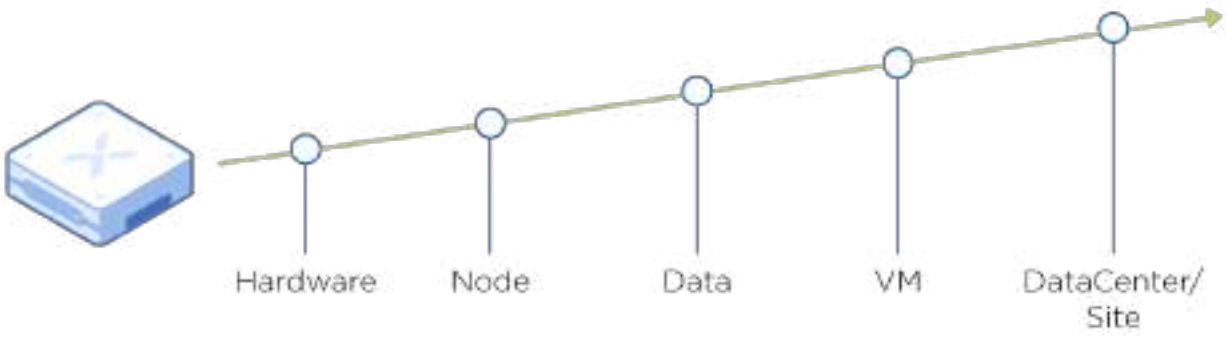


Figure 7: Business Continuity Layer

This document describes the configuration and use of Nutanix-native capabilities. Other solutions mentioned may be added to the completed design but are beyond the scope of this document.

For a list of supported third-party backup solutions see Nutanix Technology Alliance Partners.

Automation Layer

Automation and orchestration are increasingly recognized as critical to IT success. By simplifying infrastructure management across the entire lifecycle, automating operations, and enabling self-service, Nutanix helps you deploy datacenter infrastructure that delivers a high degree of scalability, availability, and flexibility.

Nutanix improves efficiency with meaningful automation, self-service, and integration with development pipelines.

- Flexible task automation: Nutanix Prism Pro provides a low-code/no-code, visual approach to task automation, enabling any administrator to build, maintain, and troubleshoot automations. Common admin tasks, like adjusting resources allocated to a VM in response to a constraint, are easily automated. Even the most complex, multi-step procedures can be turned into one- click operations.
- Self-service with no loss of control: Enterprise teams want self-service access to infrastructure and services to accelerate time to market. With Nutanix Calm, you can create blueprints that model applications and tasks and

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 999

publish them to an internal marketplace or add them to a growing collection of pre-integrated, blueprints on the Nutanix Marketplace. Application owners and developers can request IT services from the marketplace whenever needed. (See the section Calm Application Orchestration for more information.)

- Simplified development: Nutanix eliminates the complexity of test and development automation, allowing developers and administrators to work more efficiently. Your team can deploy and maintain a fully automated CI/CD pipeline with continuous application deployment across on-premises and cloud locations.

DevOps is a way to standardize processes and improving communication and collaboration between development and operations teams in an enterprise organization. DevOps methodology is not discussed in this design, but the constructs and the logical components included are elements that will help you develop/improve your DevOps strategy.

Security and Compliance Layer

Designing for your security requirements is paramount to delivering robust solutions. This is another area where this document is well differentiated from conventional datacenter architectures.

Figure 8: Designing for Security and Compliance

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1000

The Nutanix security approach is not predicated on having hundreds of different configuration options that you must set to achieve a secure environment. Nutanix takes a security-first approach including a secure platform, extensive automation, and a robust partner ecosystem. There are additional configuration options available if you need to add an extra layer of security based on business and or technical requirements.

Nutanix enables you to maintain a continuous security baseline to meet regulatory requirements more easily. Powerful security automation, called Security Configuration Management Automation (SCMA), monitors the health of storage and VMs, automatically healing any deviations from this baseline.

Nutanix provides customers with the ability to evolve from point-in-time security baseline checking to a continuous monitoring/self-remediating baseline to ensure all CVM/AHV hosts in a cluster remain baseline compliant throughout the deployment lifecycle. This new innovation checks all components of the documented security baselines (STIGs), and if found to be non-compliant, sets it back to the supported security settings without customer intervention.

In addition, data-at-rest encryption features and a built-in Key Management Server (KMS) further add our robust security capabilities.

These security features are discussed later in the Detailed Design section, and you can find more information online in the Nutanix Bible.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1001

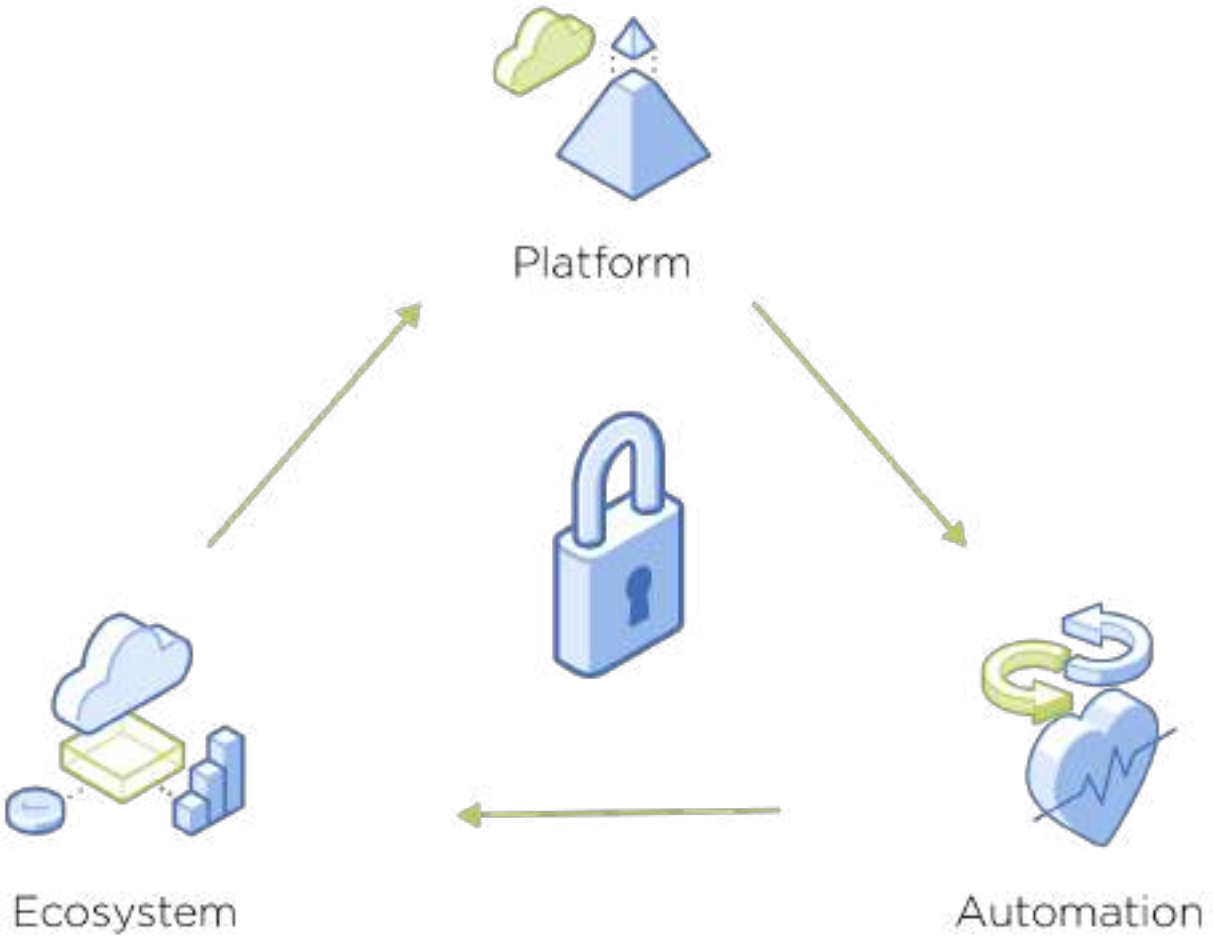


Figure 9: Nutanix Security

Nutanix incorporates security into every step of its software development process, from design and development to testing and hardening. Nutanix security significantly reduces zero-day risks. One-click automation and a self-healing security model ensure ongoing security maintenance requires much less effort.

Nutanix provides the following international security standards:

- 508 Compliant
- FIPS 140-2 Level 1
- National Institute of Standards and Technology (NIST) 800-53

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1002

- TAA Compliant

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1003

3. High-Level Design Considerations

A key feature of Nutanix Enterprise Cloud is choice. Nutanix customers have the flexibility to choose their preferred hardware vendor, CPU architecture, hypervisor, and more. This design is intended to help guide you to the best choices for your organizational needs.

There are a number of high-level design decisions that must be made before proceeding to a detailed technical design. This section provides the information necessary to help you make the following decisions:

- Choosing a datacenter architecture.
- Choosing a hypervisor.
- Choosing a cluster deployment model.
- Choosing a hardware platform.

Choosing A Datacenter Architecture

What availability must be delivered and what type of failures must the design protect against. These are key input requirements for a design since they will have an immediate impact on regions, availability zones, and data centers required plus budget.

Area and Availability Definitions

Region

A region is a geographical area with one or more availability zones (AZs). Regions are independent from each other so that failures in one region should not affect another region. Typical examples would be US east coast, US west coast, Europe north, Europe south, Asia east, Asia south.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1004

Figure 10: Regions

Availability Zone

A region holds one or more availability zones. Each availability zone contains one or more data centers.

Availability zones are implemented such that normal failures (such as a power plant failure) in one zone will not affect another. Natural and manmade disasters such as catastrophic earthquakes and nuclear strikes may disable more than one availability zone in a region.

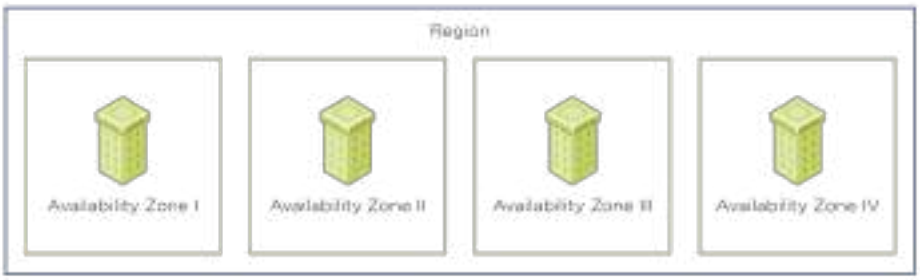


Figure 11: Availability Zones

Datacenter

Datacenters host hardware, management, and end user applications/services including network routers, network switches, firewalls, load balancers, physical servers running Nutanix software, and potentially third-party hypervisor(s).

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1005

Figure 12: Datacenters

Datacenter Architectures

Nutanix provides built-in capabilities to provide support for a multi datacenter operating model, independent of the datacenters implementation architecture which usually can be divided into single location and multiple locations.

The different datacenter location models discussed can be leveraged using private or public implementation models, or a combination of the two typically referred to as a hybrid strategy.

Single Location

- Active
  - Applications are active within the datacenter
  - Backups are stored in the same datacenter as where the applications are running.
  - Long time archiving at offsite location
  - Limited protection against datacenter failure.

Figure 13: Single Location

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1006

Multiple Locations

- Active – Active
  - Applications are active in both datacenters during normal production.
  - Both sites can provide disaster avoidance and disaster recovery for each other.

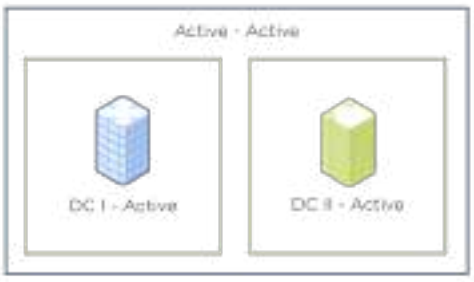


Figure 14: Multiple Locations

- Active – Passive
  - Applications are typically running from one datacenter only during normal production.
  - To make failover easier and more predictable the passive datacenter typically runs a limited number of infrastructure services during normal production.
  - The passive site provides disaster avoidance and disaster recovery functionality for the active site.

Figure 15: Active - Passive

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1007

- Active-Active-Passive
  - Applications are active in two datacenters during normal production.
  - The active datacenters provide disaster avoidance for each other.
  - To make failover easier and more predictable the passive datacenter typically runs a limited number of infrastructure services during normal production.
  - The passive site provides disaster recovery functionality.

Figure 16: Active - Active - Passive

Remote Office/Branch Office Architectures

In addition to a multiple datacenter model Nutanix can be used to provide business continuity for remote office branch office (ROBO) implementation models with a datacenter as a fan-in/central starting point. including e.g.:

- Datacenter – ROBO
  - Multiple ROBO sites replicating data to the datacenters.
  - Datacenter acts as disaster recovery for the ROBO sites.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1008

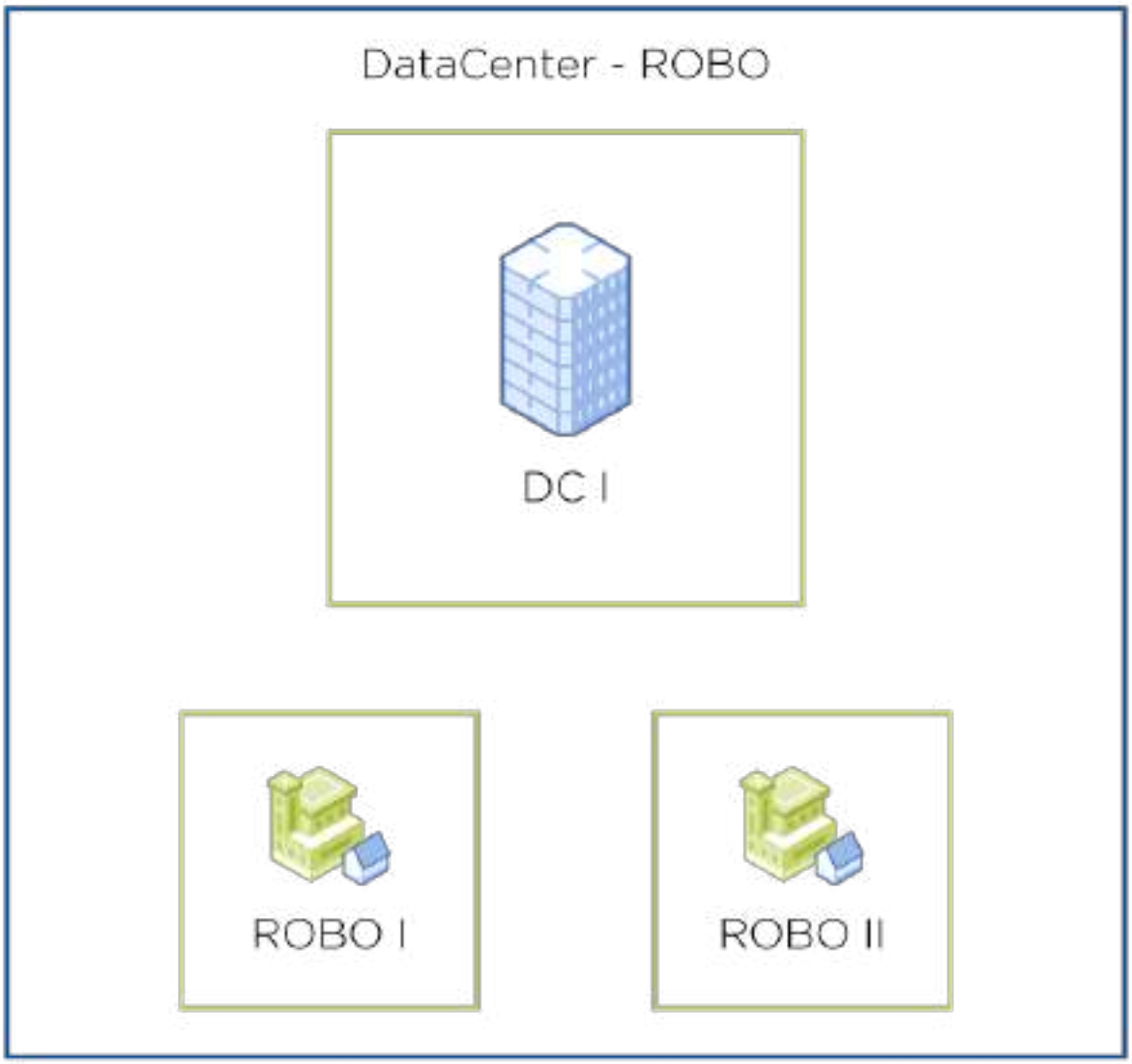


Figure 17: Datacenter ROBO

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1009

- Chain structure with Datacenter-ROBO-ROBO
  - › Datacenter acts as disaster recovery for the closest ROBO site or sites
  - › The first tier ROBO site/sites connected to the datacenter acts as disaster recovery sites for the next chain of ROBO sites. Some organizations use the term “regional data center” for these locations.

Figure 18: Chain structure with Datacenter-ROBO-ROBO

ROBO designated sites are typically a small footprint and differentiated from datacenters due to low bandwidth & high latency connections between datacenters and the ROBO sites. For larger customers, there will also be a proportionally high number of clusters/sites relative to the VM count.

Data can be replicated to more than one location for more advanced needs. An example of this policy might use NearSync between branches located in the same availability zone, and Asynchronous to a datacenter in another region

When choosing a ROBO architecture, keep in mind the restrictions that are most impactful:

- 100 millisecond or less latency between prism central and each cluster under management
- A scaled-out prism central can handle 300 clusters under management

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1010

- Accurate NTP access
- WAN restricted topology vs open internet access

Table 5: Number of Regions to be used

Region-001	NUMBER OF REGIONS TO BE USED
Justification	
Implication	

Table 6: Number of Availability Zones to be used

AZ-001	NUMBER OF AVAILABILITY ZONES TO BE USED
Justification	
Implication	

Table 7: Number of Datacenters to be used

DC-001	NUMBER OF DATACENTERS TO BE USED
Justification	
Implication	

This following table maps out the capabilities which can be applied to the different datacenter plus datacenter & ROBO architectures based on RPO and RTO requirements.

Table 8: RPO and RTO requirements

Nutanix Feature	RPO	RTO	Protect Against	Environment(s)
Time Stream / VM Snapshot	Minutes	Minutes	Minor Incident	Single Nutanix Cluster
Cloud Connect	Hours	Hours	Minor Incident	External Cloud

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1011

Nutanix Feature	RPO	RTO	Protect Against	Environment(s)
Asynchronous / Remote Replication	Minutes	Minutes	Major Incident	Multiple Nutanix Clusters
NearSync replication	Seconds	Minutes	Major Incident	Multiple Nutanix Clusters
Synchronous Replication	Zero	Minutes	Major Incident	Multiple Nutanix Clusters
Metro Availability	Zero	Near Zero	Major Incident	Multiple Nutanix Clusters

Typically, the multiple Nutanix clusters specified in the Environments column are placed in different datacenters but can be placed in same datacenter but in different fire zones.

Nutanix provides a variety of Node options and cluster sizes. Make sure to respect the current limitations:

- AOS Snapshot Frequency for Nutanix Nodes
- Single-Node Replication Target Requirements and Limitations

Choosing a Hypervisor

Nutanix supports a range of server virtualization options including: Nutanix AHV, VMware vSphere, and Microsoft Hyper-V. This design covers the deployment of either Nutanix AHV or VMware vSphere.

Nutanix AHV is included with AOS and delivers everything you'd expect from an enterprise virtualization solution: high performance, flexible migrations, integrated networking, security hardening, automated data protection and disaster recovery, and rich analytics. With robust, integrated management features, AHV is a lean virtualization solution.

A significant advantage of AHV as part of this validated design is the elimination of virtualization as a separate management silo and all of the complexity that entails. When designing a vSphere environment, for example, decisions must be made about the number of vCenters, the type of deployment

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1012

mechanism, how to enable HA, and so on. Extensive ongoing training is often required for internal staff or consultants in order to effectively design, deploy, and upgrade the environment. AHV avoids these challenges.

AHV enables:

- Checkbox high availability configuration (vs. complex percentage or slot size config)
- No virtual SCSI devices required (vs. manually configured multiple SCSI devices for maximum performance).
- Distributed networking by default (vs. deciding between Standard or Distributed Switch).
- Automatic CPU Masking (vs. manual in vSphere).
- No need for Host Profiles.
- Fewer design choices.
- Simple control plane lifecycle.
- Simplified 1-click upgrades.
- Single support path.

VMware vSphere is a proven virtualization platform used by many organizations and has a robust ecosystem. It is a complex platform with many design choices and settings to tune; it often requires the purchase of additional licenses.

When deciding which hypervisor to use in your deployment, the choice comes down to which solution best meets your business and technical requirements and your budget. Key areas to consider when choosing a hypervisor include:

- Operating system support (including legacy and current OSes).
- Third-party virtual appliance support.
- Security/hardening baseline.
- Integration with third party products (backup, software-defined networking, anti-virus, security tools, etc.).
- Availability of automation tools.
- Staff skill set and training (architecture, administration, daily operations).

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1013

- Scalability of the solution.
- Licensing costs and model (AHV adds no licensing costs to a Nutanix deployment).
- Integration with the existing environment.
- Migration of existing VMs.
- Hypervisor and management plane technical features and performance.
- Simplicity or complexity of the solution.
- Features or products that support only one hypervisor or the other.
- Satisfaction with existing hypervisor platform(s).
- ROI/TCO of the full stack.
- Simplified support model (i.e. single support vendor vs multiple).
- Time to Deploy/Time to Value.

Freedom of choice is a key tenet of Nutanix. After considering these factors, it is likely that one hypervisor platform stands out as the best option for your deployment. No matter which hypervisor you choose, the solution is backed by world-class Nutanix support and a full ecosystem of node types. (Hardware selection is discussed in the section Platform Considerations).

Table 9: Choose a Hypervisor

VRT-001	CHOOSE NUTANIX AHV OR VMWARE ESXI AS THE HYPERVISOR FOR YOUR DEPLOYMENT
Justification	
Implication	

Choosing a Cluster Deployment Model

When designing Nutanix clusters for your deployment, there are several important design considerations:

- Choosing whether to deploy a separate management cluster?

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1014

- Choosing whether your cluster(s) will run mixed workloads or be dedicated to a single workload?

Separate Management Clusters

A separate management cluster is not a requirement of this design. If you are planning a smaller-scale deployment, it doesn't always make sense to design, purchase, and operate a separate cluster for a limited set of management VMs.

However, the infrastructure applications and services that run on a management cluster are critical. At a larger scale, there are several reasons to separate these management workloads:

- Availability: Separating management workloads on their own cluster(s) makes it easier to ensure they are always available.
- Security: you may wish to more strictly control access to management clusters and workloads, including additional controls such as firewalls, dedicated networks, more stringent role-based access (RBAC), and possibly others. While this can be accomplished on mixed clusters, it is easier to monitor and manage these additional security controls on a separate physical cluster.
- Operations: RBAC prevents those that are not authorized from interacting with important management services. Physical separation prevents any accidental or malicious actions that could compromise the availability or performance of important infrastructure services.
- Performance: Performance is just as important for infrastructure services as any other workload. Having a dedicated management cluster(s) simplifies troubleshooting of performance issues and reduces the potential for hard to diagnose workload conflicts. It eliminates the possibility that changes in the management space will affect application workloads and vice versa. In a highly elastic cloud environment, there may be workload expansions that occur via self-service or automated events. Depending on whether resource control policies are in effect, this can cause resource contention in a shared cluster.

Note: You do not need a separate management cluster for each use case or environment unless you have strict security or compliance requirements that make it necessary. This means that a

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1015

single management cluster can support multiple use cases such as: EUC deployments, private cloud, and general server virtualization environments.

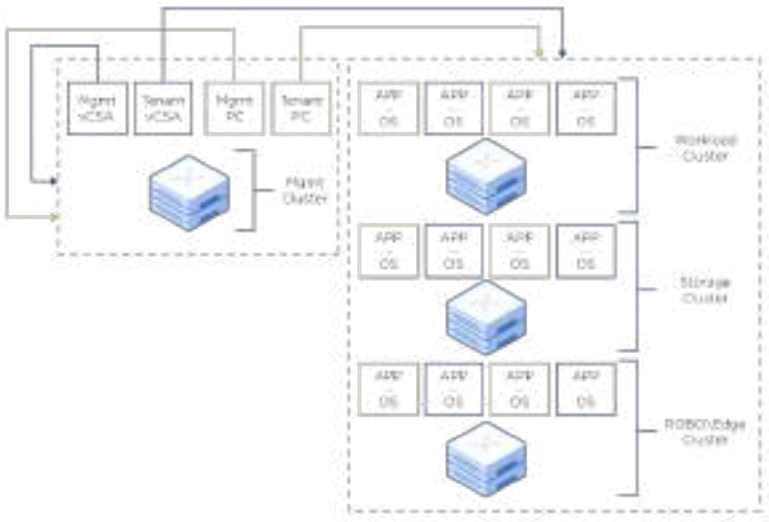


Figure 19: Separate Management Clusters

Should You Deploy Two Management Clusters?

In large-scale deployments, the management cluster can be split to create separate failure domains. With two management clusters, you can place redundant components into each cluster, enabling a higher level of availability. Should there be an issue with one of the management clusters, the other remains available to service requests.

Table 10: Management Cluster Architecture

PFM-001	**MANAGEMENT CLUSTER ARCHITECTURE: DEPLOY A SEPARATE MANAGEMENT CLUSTER OR SHARE A CLUSTER WITH OTHER WORKLOADS. WHEN CHOOSING A SEPARATE MANAGEMENT CLUSTER, CONSIDER A REDUNDANT CONFIGURATION.**
Justification	
Implication	

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1016

Will You Deploy Dedicated or Mixed Clusters?

The decision whether to mix workloads within a cluster or to dedicate a cluster for each type of workload is usually a question of scale. For example, if you have 200 general server VMs, a small Exchange deployment, and 10 average-sized database VMs, mixing the workloads in a single cluster is common and can be easily managed. However, if any or all of these workloads increase by 5-10x, the complexity of sizing and operating the mixed environment goes up dramatically.

Operating large-scale mixed environments creates a number of unique challenges. You have to decide whether you are willing to manage the challenges of mixed workloads or dedicate clusters for each workload. Here are the main factors to consider:

- Performance and capacity: The resource demands of different applications can vary widely. You need to understand the needs of each application when mixing workloads since the chance for conflicts to occur is increased. There may also be wildly different performance and capacity needs between applications which could require different node configurations within a single cluster. Unless you are going to isolate certain workloads to particular nodes, each node within a cluster needs to be able to handle the average daily mix of applications that might be running on it.
- VM resource-sizing requirements: The CPU and memory sizing for general server VMs, VDI VMs, business-critical application VMs, etc. can vary widely. While it's fairly easy to account for memory sizing, CPU sizing is more complex. Each of these workloads consumes different amounts of CPU, and may require much different levels of CPU overcommit, if any.

If you have large groups of VMs with widely different resource requirements, it's typically better to build clusters to contain more uniformly sized VMs. From a hypervisor HA standpoint, you may require additional resources within a mixed cluster to ensure the ability to failover. This can also increase the day 2 operational support effort, since it may require manually tuning HA settings and increased monitoring to ensure HA resources remain in compliance.

- Software licensing: The most common reason for dedicated clusters is software licensing. There are a variety of reasons why using dedicated

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1017

clusters make sense from a licensing standpoint. Here are two common examples:

  - Operating system licensing: Windows and Linux vendors may offer "all-you-can- eat" license models for licensing at the host level. Therefore, it makes more sense to have clusters dedicated to either Windows or Linux VMs, to minimize licensing costs.
  - Database licensing: Database licenses are frequently based on either CPU cores or sockets. These licenses can be expensive, and you often have to license all the nodes in a cluster to enable DB VMs to run on every node. Once again, you probably don't want to run other workloads on the cluster since that reduces the return on your license investment.

In addition, you may want to run nodes hosting database workloads on different hardware than nodes hosting general server VMs. For instance, having fewer CPU cores running at a higher clock speed may reduce your overall licensing costs while still providing the necessary compute power.

This is provided for informational purposes only, please refer to your licensing agreement with Microsoft for more information.

- Security: In many projects, security constraints are an overriding factor. When it comes to the security of mixed vs dedicated clusters, there are a few design considerations that are important to consider as you decide whether logical or physical separation is adequate to address your security requirements:
  - Operations: RBAC is the primary means of controlling access and management of infrastructure and VMs in a mixed cluster. Dedicated clusters prevent non-ap proved parties from gaining any access whatsoever.
  - Networking: A mixed cluster typically relies on separate VLANs and firewall rules per workload to control access. A dedicated cluster would only have the required networks presented to it for a single workload and would likely limit who and what has network access. Both approaches can control and limit access to cluster resources, but dedicated goes a step further by providing complete physical network isolation for those that require it.

If you are able to address the performance/capacity, resource-sizing, licensing, and security constraints discussed above, it is possible to successfully

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1018

design and operate clusters of any size to run mixed workloads. The key is to thoroughly understand the requirements of each workload and size with that knowledge.

Recommendation

At scale, it is our recommendation to use dedicated clusters to the greatest extent possible for the reasons discussed above. Utilize mixed workload clusters where it fits.

Including Storage-Only Nodes in Clusters

Storage-only nodes contribute storage capacity and I/O performance within a cluster. Storage only nodes are available for clusters running either AHV or ESXi. Storage-only nodes can be any node type, but typically are configured with just enough CPU and memory resources to run the CVM since there aren't any application VMs running on these nodes. These nodes are a member of the AOS cluster but are not visible to the hypervisor cluster for non-storage functions, so the hypervisor won't schedule other VMs to run on them.

Table 11: Mixed or Dedicated Workloads Per Cluster

PFM-002	MIXED OR DEDICATED WORKLOAD PER CLUSTER
Justification	
Implication	

Choosing How You Will Scale

This document clearly lays out the Nutanix opinionated design for deploying HCI clusters and building a private or hybrid cloud for any type of workload. A challenge in any design, whether you're starting with one cluster or dozens, is how to scale the environment to reach your goal. To accomplish this, you need an overarching architectural plan that creates a repeatable process that can be followed by the organization. Defining this in advance removes confusion and simplifies future deployment. An overarching architectural plan allows you to track progress and ensure compliance with the design.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1019

For this design, we recommend that an at-scale deployment should include:

- A control plane.
- A block and pod architecture.

Choosing a Control Plane

Within your design there should be a primary control plane where the majority of daily operational tasks are performed. In this design:

- The primary control plane is Prism Central.
- VMware vCenter is also required for those using VMware ESXi.

Each of these control planes has a maximum size that dictates the number of VMs, nodes, and clusters that can be managed by an instance.

Block and Pod Architecture

A repeatable architecture is needed to ensure safe and efficient scaling. This design uses the pod and block architecture because it's both familiar and easily consumed. We have adapted it to support Nutanix deployments. This section explains the different parts of the architecture and how they can be used to scale a deployment to any level.

What is a Pod?

In this design, a pod is a group of resources that are managed by a single Prism Central instance. The diagram below shows a single pod containing four building blocks. A pod is not bound by physical location limitations; all of its resources could be at a single site or at multiple sites. Examples of multiple sites include: a traditional multi-datacenter design, a hybrid cloud design,or a ROBO architecture.

Building Block

In this design, a build block is equivalent to a Nutanix cluster. Each of the clusters can run a single dedicated workload or mixed workloads. There is no need for building blocks to be uniform within your design.

Recommendation

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1020

For each workload:

- Establish whether it will have a dedicated cluster or share a mixed cluster with other applications.
- Define the maximum size of this type of building block. While building blocks for different workloads do not need to be the same, they certainly can be.
- Determine the maximum size of a building block based on:
  - The scale at which you will deploy workloads.
  - The need for failure domains.
  - Operational considerations such as upgrade timing.

These topics are discussed later in the Detailed Technical Design section of this document.

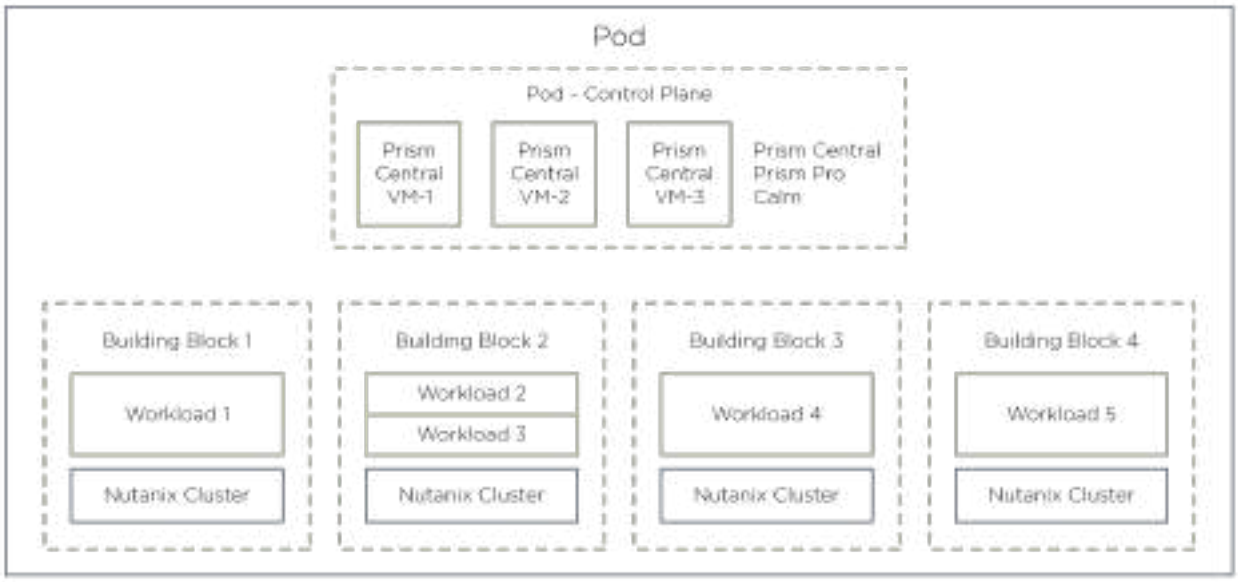


Figure 20: Block and Pod Architecture

Scaling the Block and Pod Architecture

You can scale an individual pod up to the maximums that Prism Central supports for the AOS version you are deploying. For the AOS version specified in this document, a scale out Prism Central deployment with large sized VMs can manage up to:

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1021

Prism Central Limits (assumes Scale-Out PC configuration):

- 25,000 VMs
- 200 clusters
- 1,000 nodes

If any of these limits are reached, a pod is considered full. For example, with an EUC deployment, the VM limit will likely be reached first since you typically have high VM density resulting in large numbers of VMs with fewer nodes and clusters. A large ROBO environment might hit the cluster count limit because you tend to have many sites each with a small cluster and a few VMs.

At very large scale (e.g. thousands of nodes), it can make sense to have pods dedicated to each workload, but for environments that have Nutanix deployed for multiple workloads, a pod will typically contain multiple applications.

Once a pod reaches a scaling limit, start a new pod with at least one building block. The new pod scales until it also reaches a scaling limit, and so on.

The building blocks within a pod scale in a similar fashion. A building block is started, and workloads are migrated onto it until it reaches its determined max size, and a new building block is started. New building blocks can be as small as 3 nodes, the minimum to start a Nutanix cluster, or any size up to the max size you've specified for that building block.

The starting size for each building block and the increments for scaling them are organizational decisions:

- For smaller or more agile organizations, starting small and scaling incrementally often makes sense.
- Larger organizations may prefer to deploy a new building block fully populated and migrate workloads onto it as schedules dictate.
- Although 3 nodes is the minimum size for a cluster, using 4 nodes provides a higher level of redundancy during maintenance and failure conditions.
- For ROBO and edge use cases, the starting size can be as small as one, two, or three nodes depending on requirements.

The diagram below illustrates a simple VDI building block example. With VDI it is easy to think in terms of number of users and the node count in a cluster. In

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1022

this example, the building block is a 16-node cluster supporting 1,500 users. This works out to 100 users per node plus an additional node for HA. With the first building block full, a request for an additional 500 users requires a new building block to be started. This building block is then scaled up to its max size before starting a third.

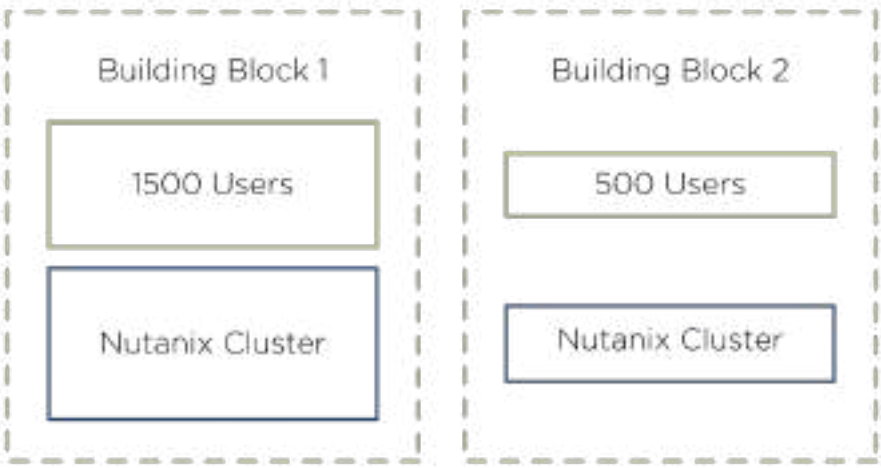


Figure 21: Example VDI Building Block

By having well established and documented design decisions for pod size and building block size, the architecture and operational teams are free to keep scaling without the need to revisit decisions to satisfy each resource expansion request.

Choosing the Right Licensing and Support

Now that you've chosen a hypervisor, decided on mixed or dedicated workloads, and established your block and pod architecture, you can make informed hardware decisions. When evaluating the different Nutanix platform options available, there a few key decision points:

- Choosing Your Software licensing and Support.
- Choosing Your Platform Vendor.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1023

Software Licensing and Support Considerations

Nutanix nodes are available in two different purchasing/licensing options: appliances or software-only:

- Appliances are available directly from Nutanix or through our OEM relationships.
  - Appliance based licensing is referred to as “life of device licensing”, meaning it’s only applicable to the appliance it was purchased with.
  - The manufacturer of the appliance takes all support calls for software and hardware issues. For example, if you choose Dell appliances, Dell will take all support calls and escalate to Nutanix for software support as needed. With Nutanix NX appliance all support calls go directly to Nutanix.
- The Software Only option de-couples software and support licensing from the underlying hardware. This enables:
  - License portability. The same license can continue to be used when the underlying hardware is changed, such as a hardware vendor change or a node refresh. (note: licenses are portable for like-for-like hardware replacements. If the hardware specification of the nodes change, then there might be the need for additional licenses.).
  - Deployment on additional supported hardware platforms. Hardware is per our qualified list of platforms, which can be found on the Hardware Compatibility List (HCL).
  - Direct software support from Nutanix while the server vendor provides hardware support.
  - Another type of Software Only Licensing is the Core-Licensing option, which is best for those customers who prefer the benefits of the software-only model but want hardware from a specific OEM server vendor. Core licensing enables customers to purchase software only licenses and buy hardware from any of the appliance vendors. For example, XC-Core utilizes Dell XC OEM appliances but de-couples software and hardware support.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1024

Table 12: Nutanix Software Licensing Level

PFM-003	SELECT NUTANIX SOFTWARE LICENSING LEVEL
Justification	
Implication	

Vendor Considerations

When it comes to selecting a hardware vendor, there are a number of factors to evaluate:

- Brand loyalty. This can be a strong factor in an IT buying decision. There may be purchasing commitments or discounts in place at an organizational level driving this loyalty, or you may simply have been happy with past experiences.
- Support Quality. The quality of the support experience can also be a factor in your hardware evaluation. For hardware failures, makes sure the hardware vendor responds quickly and can provide parts reliably within the contracted response time. The overall support experience is important. A vendor should be easy to contact, be responsive to requests, and provide resolution in a timely manner.
- Hardware Quality. The reliability and quality of hardware is of obvious importance. Today's servers are all very similar internally; they use many of the same components with just a few proprietary components for each vendor. The reliability of the leading server vendors is pretty similar so your decision may be contingent on your organization's past experiences.
- Operational Experience. When it comes to the ongoing operational experience, what does it take to carry out day 2 operations to support the lifecycle of the physical server and the vendor toolset (if any). This includes: monitoring server health, reporting and upgrading firmware, and monitoring for component issues and failures. Virtually all of the server vendors offer tools for these activities and when combined with the power of AOS and Prism, the experience is pretty similar. Nutanix Lifecycle Manager (LCM) offers firmware reporting and management for all Nutanix appliance options.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1025

- Configuration Options. Physical configuration options may weigh strongly in choosing among server vendors, and in choosing a model type for each workload. Factors include:
  - Number of sockets.
  - CPU options.
  - Number of storage bays.
  - Network connectivity options.
  - Storage media options. While there is generally a level of parity between server vendors, a particular vendor may offer something the others do not, or one vendor may offer the latest options more quickly when new components are released. You may require or prefer a specific type of network card or need nodes with a large number of storage bays. Storage considerations, such as the number of SSD/NVMe options available, RDMA capabilities, and support for large-capacity media may be important for specific workload requirements.
- Physical form factor. This is another common decision point since it can affect the amount of space consumed in a rack, the power draw, the number of network connections, and the number of internal expansion slots. Availability of internal expansion slots may limit the number and type of network cards that can be deployed, and whether a node is capable of accepting GPU cards and the number of GPU cards it's capable of supporting. When it comes to different form factors, there are:
  - High-density chassis that offer either four or two physical nodes in 2U of rack space. These are popular options for a variety of workloads that do not require extensive internal expansion or a large number of storage bays.
  - Standard rackmount servers, typically with a 1U or 2U chassis and one physical server per chassis. These provide much wider capabilities in the number of storage bays available, the number of internal expansion slots available, and may also support more memory.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1026

Table 13: Physical Node Vendor

PFM-004	SELECT PHYSICAL NODE VENDOR
Justification	
Implication	

Mixed Configurations and Node Types

Nutanix clusters allow significant flexibility in terms of the node types and configurations you can utilize in a single cluster. This allows clusters to be operated and expanded over time without artificial constraints. A cluster can be expanded with different node configurations to accommodate new workloads or when previous nodes are no longer available.

Considerations include:

- Node models. Mixing node models within a cluster is a fairly regular occurrence. While it's possible to have the same CPU, memory and storage configuration in two different node types, it's not required in order to mix them in the same cluster.
- CPU configurations. Mixing nodes within a cluster with different CPU configurations such as core count, clock speed, or CPU generation is supported. This can be to address changing application requirements, inventory availability, financial constraints, time of purchase, or other factors.

While there is no limit to the drift between configurations, it's a commonly accepted best practice to keep the core counts and memory configuration of nodes within a cluster at similar levels. Using different CPU generations in the same cluster can limit the feature set / functionality of newer CPUs. The lowest common denominator is the level of the oldest CPU generation within a cluster. Having mostly uniformly configured nodes in a cluster makes it easier for humans to double check the HA and capacity planning recommendations of automated tools.

- Storage media. Having nodes with different storage configurations is also supported. Variations at the storage layer can include varying the size or number of SSDs or adding all-flash nodes to a hybrid cluster.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1027

When introducing a storage configuration within a cluster that dramatically increases the amount of storage, you must ensure there is ample failover capacity to rebuild the largest node. For example, suppose the existing nodes in a cluster have 10TB of capacity each and you want to add node(s) with 40TB of capacity. Initially, it's best to add a pair of these 40TB nodes. Subsequent large-capacity-node additions can then be done one at a time.

Choosing the Right Hardware for Your Workload Types

When it comes to sizing Nutanix clusters for different application workloads there are many options. Most workloads can successfully run on any of the Nutanix and OEM models available, but some models and configurations may be a better fit than others.

Once you know the requirements of your workload(s) you can use the Nutanix Sizer to determine the best configuration for your cluster(s).

Nutanix Sizer is a web-based application that is available to Employees, partners and select customers. Sizer allows for the architect to input application and workload requirements and the node and cluster configurations are automatically calculated.

Different hardware platforms offer different characteristics to address differences in workloads. The following sections provide guidance on model selection, and performance considerations.

Model Types

The various Nutanix and OEM appliance models and hardware compatibility list (HCL) servers provide the flexibility to identify the right solutions to meet financial, space, and performance requirements for different projects. There may be differences in terms of the number and types of models available, but the same level of flexibility is generally available from all vendors. Some vendors offer fewer models but allow greater configuration flexibility.

Generally speaking, there are four different groups that servers fall into, translating to different use cases:

- General workloads and EUC: These are by far the most popular nodes deployed in Nutanix clusters. They can handle the vast majority of workloads

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1028

including: general server virtualization, business-critical applications, VDI, and most others. There are a mix of form factors available.

- ROBO and Edge: These are similar to the general workload options, with the exception that they may offer few options for CPU and storage as they are optimized for these edge use cases.
- Storage dense: For workloads that require large amounts of storage capacity, storage-dense nodes offer a larger number of storage bays and dense media options, possibly with fewer CPU options. The physical configuration of these nodes is optimized for workloads such as Nutanix Files, Nutanix Objects, or to be utilized as storage-only nodes.
- High performance: The most demanding workloads and business-critical applications (BCA) may require additional CPU resources and storage performance. For these workloads there are nodes offering additional CPU configurations in terms of core count and clock speed, as well as quad-socket configurations. It's common for these models to offer as many as 24 storage bays to allow for more flash devices or hard drives for workloads that can utilize the added performance characteristics.

Each of the above model alternatives offer one or several of the available physical form factors along with the density and performance characteristics discussed.

Nutanix software does not require any complex tuning or configuration to support the different workloads, but there are plenty of hardware options to tailor your selections to different use cases.

Performance Considerations

Nutanix and AOS meet the performance demands of different workloads without continuous performance tuning. The Nutanix HCI storage fabric is powerful and intelligent enough to handle nearly any type of workload.

However, different cluster design and configuration options still yield performance benefits. Selecting the appropriate node model and configuration to meet application and solutions requirements is an important design decision. The primary design considerations for performance are:

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1029

- Number of drives. The number of hard disk drives (HDDs) or flash devices in a node can dramatically affect its performance characteristics. However, simply picking the node with the most device bays won't improve the performance of every workload.
  - Write-heavy workloads benefit from additional storage devices to provide performance and consistency. Other workload characteristics such as read/write ratio and I/O size should also be considered.
  - Workloads such as VDI typically have minimal capacity requirements but higher IOPS demands. It's common to utilize nodes with partially populated storage bays and as few as 2 flash devices per node, providing the right amount of storage capacity while still exceeding performance demands.
- All Flash. All-flash configurations are available from Nutanix, OEMs, and supported third-party server vendors. All-flash clusters utilize only SSDs, and these configurations provide higher IOPS and a more consistent I/O profile. While all flash configurations have become common, they are not absolutely necessary for every workload and use case.
- NVMe. There are a number of new technologies available now and coming soon that offer additional performance capabilities. NVMe is the first of these to be widely available and offers a number of benefits over SSD. New flash technology allows NVMe devices to deliver higher levels of I/O with lower latencies.
- RDMA. To realize the full benefits of NVMe, nodes are typically configured with remote direct memory access (RDMA). RDMA allows one node to write directly to the memory of another node. This is done by allowing a VM running in the user space to directly access a NIC, which avoids TCP and kernel overhead resulting in CPU savings and performance gains.
- Size of flash tier. In hybrid configurations containing SSD and HDD devices, the bulk of the performance comes from the flash tier. Therefore, it's important to understand the workload being deployed on a hybrid cluster. The data an application accesses frequently is typically referred to as the working set. The flash tier in hybrid clusters should be sized to meet or exceed the size of the working set for all of the applications that will run on

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1030

the cluster. There is no penalty for having too much flash in a cluster but not having enough can result in inconsistent performance.

Table 14: Node Models

PFM-005	SELECT NODE MODEL(S) PER USE CASE
Justification	
Implication	

Note: As your organization works through the Detailed Technical Design elements in the following section, be prepared to revisit your model decisions to fine-tune CPU, memory, and storage configurations.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1031

4. Detailed Technical Design

With the necessary high-level design decisions made, including hypervisor, deployment model, and hardware platform and models, you can now plan the technical design for your Nutanix deployment.

This section provides technical guidelines for each layer of the design stack. Disaster recovery and business continuity guidelines are provided in chapter 5. Where possible, we've organized the sections so that you don't have to spend time reading material that doesn't apply. For instance, if you are not deploying VMware, you can skip all sections that are applicable only to it.

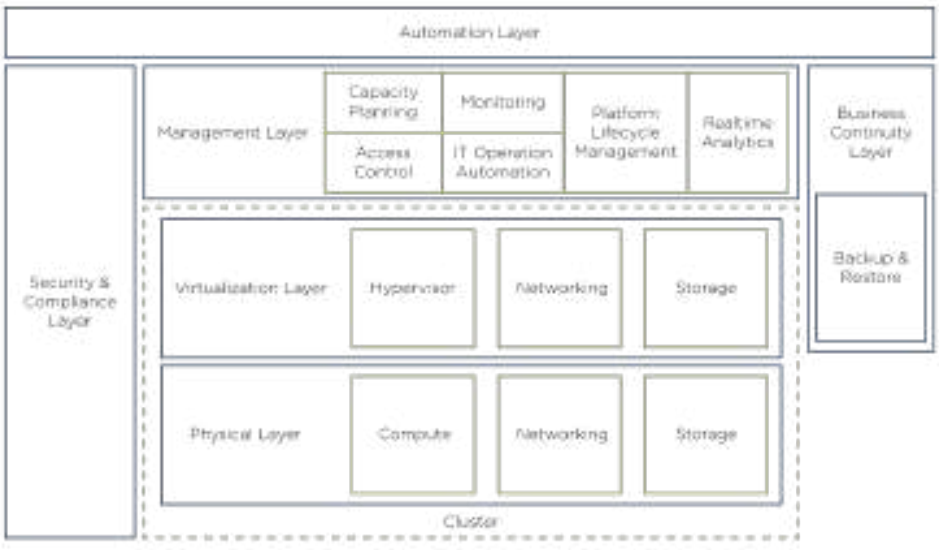


Figure 22: Planning the Technical Design

Required Software Versions

This design assume that you will be running the following software versions:

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1032

Table 15: Software Versions

Name	Version	Description
Prism Central	Latest version	Use latest version available (pc.2020.7 at the time of writing).
Nutanix AOS	Latest LTS	Use latest LTS available (5.15 at the time of writing).
Hypervisor Options		
Nutanix AHV	Latest LTS	Use latest LTS available (5.15 at the time of writing).
VMware vSphere	6.7 or 7.0	
VMware vCenter	6.7 or 7.0	Recommended for vSphere deployments.

Physical Layer Design

This section guides you through the process of designing all physical aspects of your Nutanix deployment, including:

- Compute and Storage Design.
- Networking.
- Choosing cluster size.
- Failure domain considerations.
- Designing workload domains and cluster layout.

Choosing the Optimum Cluster Size

This section provides guidance for cluster sizing. When designing a Nutanix cluster it's important to consider more than just technical limits and recommendations. There are other important considerations including: hardware vendor recommendations, security, and operational requirements that may dictate the optimal cluster size.

Review Nutanix Configuration Maximums for the latest limits.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1033

The following table provides a comprehensive list of the design considerations that pertain to cluster size.

> Note: These considerations apply to cluster sizing. Additional information for each area is provided in later sections.

Table 16: Cluster Size Design Considerations

AREA	LIMITING FACTOR(S)	CONSIDERATIONS
Operations/ manageability	Maintenance window	Define/validate your maintenance window and make sure the cluster upgrade process fits in the window. Example: • Maintenance window: 12h. • Full single node upgrade: at least 45m (Hardware, FW, AOS, and hypervisor). Time depends on hardware vendor. • Maximum cluster size: 12 -15 nodes.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1034

AREA	LIMITING FACTOR(S)	CONSIDERATIONS
Security & compliance	Security zones within an organization or business unit	Collect all relevant security and compliance requirements. Example: • Multiple security zones: Internet DMZ, PROD, test & dev, inner-DMZ • Every security zone may dictate different cluster sizes: › Internet-facing DMZ clusters usually have a smaller number of nodes and smaller number of workloads to minimize impact of a security breach or DDoS attack. › For example, Dev/Test clusters that have lower criticality may also have less strict change management policies and can therefore have a large numbers of hosts.
Vendor recommendations and limitations	• Hypervisor limitations • Management plane limitations • Vendor recommendations	Each product has limitations and vendor recommendations. Make sure you do not cross boundaries set by the vendor. See the vendor limitations/ recommendations table.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1035

AREA	LIMITING FACTOR(S)	CONSIDERATIONS
Business continuity	• RPO • RTO • Backup window	Collect BC/DR requirements, RPO, RTO, backup and restore time window, backup system performance statistics. Example: • RPO 24h • RTO 48h Ensure you can recover/restore from backup and restart workloads within 48h. A cluster where total storage capacity exceeds technical capabilities of the backup system could fail to meet desired RTO.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1036

AREA	LIMITING FACTOR(S)	CONSIDERATIONS
Workload considerations	• Application architecture • Application licensing • Application criticality	Verify application architecture with the application team/vendor, including HA, DR, scale-in vs scale-out, and performance requirements. Consider licensing model for each application and its implications. Example #1: Oracle or MS SQL licensing models are based on physical core count. Design clusters for database performance and capacity requirements to avoid cluster oversizing and minimize license costs. Example #2: Application has its own HA or DR If application can provide native HA and/or DR, RPO/RTO considerations described under Business Continuity (above) may not apply.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1037

AREA	LIMITING FACTOR(S)	CONSIDERATIONS
Networking	• Total available network switch ports. • Available network switch ports per rack.	Available physical ports per rack and rack row is important when choosing cluster size and number of clusters. Example: • 96 ports (10GbE) available per rack. • 48 ports (1Gbps) available per rack. • 2 x 10GbE uplinks per Nutanix host. • 1 x 1Gbps uplink for Out-of-Band management. Maximum nodes per rack is 48 (total capacity of the top-of-rack switches).
Datacenter Facility	• Available server rooms. • Total power and cooling. • Power and cooling per rack. • Available total rack units. • Available rack units per rack. • Floor weight capacity.	Power and cooling is one of the most important factors limiting Nutanix cluster size and node density. You have to ensure you do not exceed any hard limits when designing your cluster layout. When calculating power consumption and thermal dissipation use maximum values provided by vendor. Typical datacenter rack is 42RU. Some datacenters have racks up to 58RU.

Maximums and Minimums: AHV Deployments

The following table shows the maximum limits for management plane software components in AHV deployments.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1038

Table 17: Maximum Limits for Management Plane Software Components in AHV Deployments

Management Software	Maximum Number of Hosts	Maximum Number of VMs	Notes
Nutanix Prism Central	Up to 200 clusters or 25,000 VMs	1,000 nodes or	Assumes scale-out Prism Central

The following table provides Nutanix recommendations for the minimum and maximum number of nodes in a single Nutanix AHV cluster.

Table 18: Minimum and Maximum Number of Nodes in a Single AHV Cluster

Minimum Number of Nodes	Maximum Number of Nodes	Hypervisor	Recommendation
1	32	Nutanix AHV	Single and dual-node clusters are for ROBO only

Maximums and Minimums: VMware vSphere Deployments

The following table shows the maximum limits for management plane software components in VMware deployments.

Table 19: Maximum Limits for Management Plane Software Components in VMware Deployments

Management Software	Maximum Number of Hosts	Maximum Number of VMs	Notes
Nutanix Prism Central	Up to 200 clusters or 25,000 VMs.	1,000 nodes or	Assumes scale-out Prism Central
VMware vSphere vCenter	2,000 hosts	25,000 powered on	

The following table provides Nutanix recommendations for the minimum and maximum number of nodes in a single VMware cluster.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1039

Table 20: Minimum and Maximum Number of Nodes in a Single vSphere Cluster

Minimum Number of Nodes	Maximum Number of Nodes	Hypervisor	Recommendation
2	48	VMware vSphere ESXi	Dual-node clusters are for ROBO workloads only. Maximum number of nodes in single Nutanix cluster with VMware ESXi is limited by hypervisor version. For more details refer to VMware documentation.

Table 21: Number of Clusters

PFM-006	NUMBER <<TYPE AND SIZE>> OF CLUSTERS
Justification	
Implication	

Failure Domain Considerations

Failure domains are physical or logical parts of a computing environment or location that is adversely affected when a device or service experiences an issue or outage.

The device or services that are affected can greatly affect the size of the failure domain and its potential impact. For example, a router generally has a bigger failure domain than a wireless access point since more endpoints rely on a single router than a single access point. Identifying possible failure domains and keeping the size of failure domains small or manageable where possible, reduces the chance of widespread disruption.

Building redundancy within and across failure domains helps to mitigate the risks of failure.

When designing a Nutanix deployment, you can take steps to mitigate risk for each of the following failure domains:

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1040

- Drives
- Nutanix node
- Nutanix block
- Management plane
- Nutanix cluster
- Datacenter rack and server room
- Datacenter

Nutanix clusters are resilient to a drive, node, block, or rack failure, which is enabled by redundancy factor 2, the default. Redundancy factor 3 can enable simultaneous drive, node, block, or rack failures with the right architecture. After drive, node, block, or rack failure, a Nutanix cluster self-heals to reach the desired redundancy factor and rebuilds resilience for additional subsequent failures.

> Note: You can configure your Nutanix environment to be fault tolerant to node, block, and rack failures. This is described later in the Data Redundancy and Resiliency section. Mitigating the risks of network failure domains is described in the Networking section.

The Management Plane

One of the most important failure domains, and one that is often overlooked by architects, is the management plane. The more workload domains managed by a single management plane, the bigger the impact of a failure. When deploying the management plane, consider the following risk mitigations to reduce the impact of a failure.

Table 22: Management Plane Risk Mitigations

AREA	RISK MITIGATION
Availability	• Design and deploy management plane to be highly available. • At a minimum, design to meet the availability. requirements of the managed workload or service with the highest uptime requirement.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1041

AREA	RISK MITIGATION
Limit the impact	• Confine workload domain to a single datacenter or site. • Confine workloads domain to a defined security zone. • Ensure the API gateway is always available because other 3rd party integrations may rely on it (for example, third party backup vendor integration).
Access Control	Configure built-in RBAC to restrict access to management platform resources.

Note: The section Management Layer provides more details on management plane configuration.

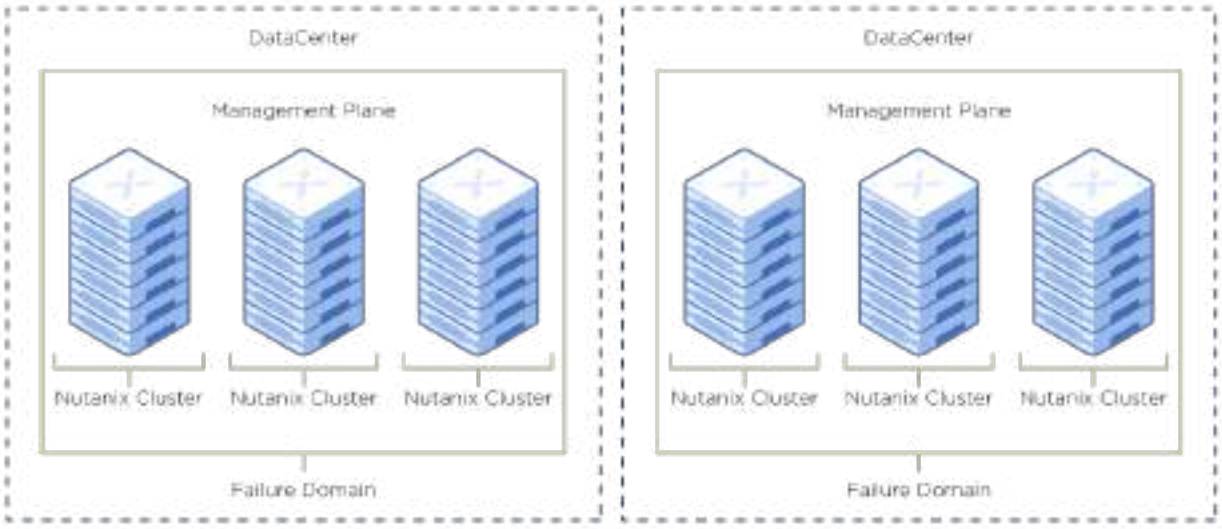


Figure 23: Management Plane Failure Domain

The Nutanix Cluster as a Failure Domain

When evaluating each Nutanix cluster as a failure domain, consider the risks and potential effects in terms of both the size of the cluster (as described above in Choosing the Optimum Cluster Size) and the workloads running in the cluster, including whether the cluster is running mixed or dedicated workloads.

Large clusters result in larger failure domains and potentially higher business impacts, since they typically host considerably more workloads. To mitigate

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1042

the risk of data unavailability or service disruption, design for redundancy at a cluster level to protect data and services, as described in the following table:

Table 23: Designing for Redundancy at the Cluster Level

AREA	RISK MITIGATION
Power	Redundant power from two different power supplies.
Networking	Redundant TOR switches. Redundant upstream connectivity to TOR switches from each Nutanix node.
Cluster	Leverage Nutanix scale-out architecture and data protection capabilities to replicate data to a second Nutanix cluster in the event that one cluster fails.
Application	Deploy application across multiple clusters.

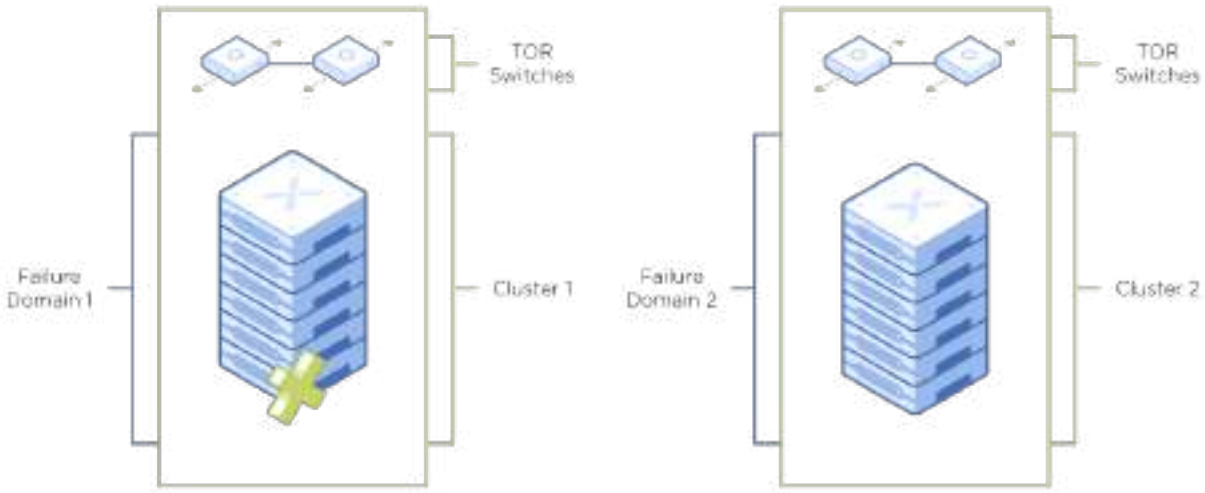


Figure 24: The Nutanix Cluster as a Failure Domain

Datacenter Rack and Server Room Failure Domains

When considering the datacenter rack failure domain, the primary mitigations are redundant power from two different power supplies to each rack, redundant TOR switches, and redundant network uplinks.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1043

When considering the datacenter server room failure domain, it is critical to examine all datacenter components to ensure they are not shared among multiple server rooms, as described in the following table:

Table 24: Datacenter Rack and Server Room Risk Mitigation

AREA	RISK MITIGATION
Power	Redundant power
Cooling	Independent cooling
Server Room	Provide redundant server room within separate firezone (in the same datacenter)
Application	Place application in multiple server rooms. For example, active directory domain controllers in separate server rooms.

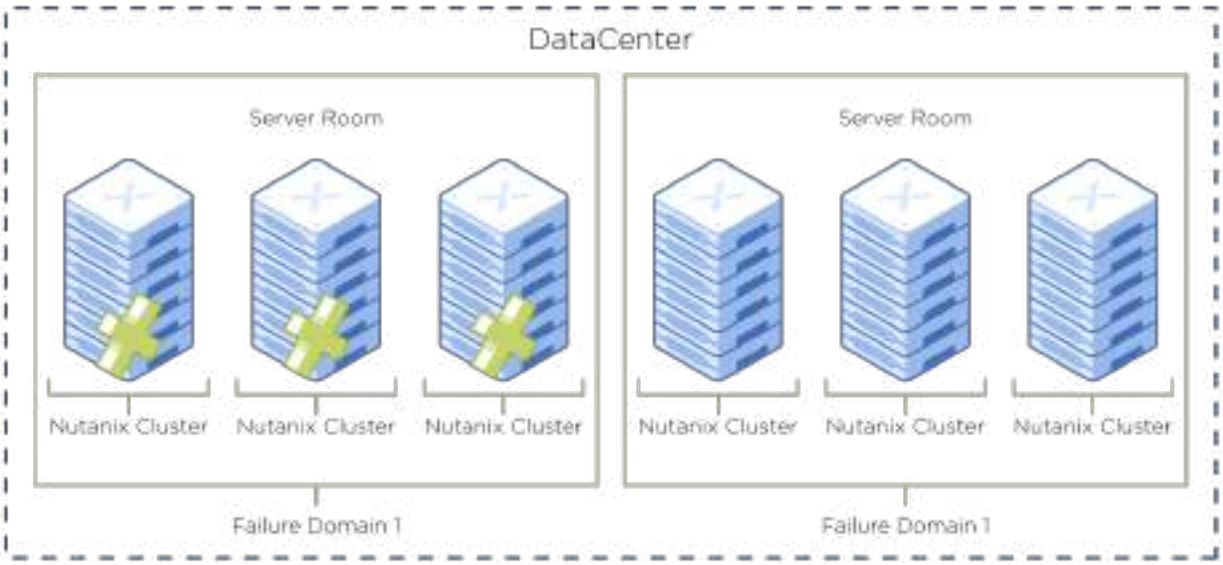


Figure 25: Datacenter Rack and Server Room Failure Domains

Datacenter Building

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1044

When considering the datacenter failure domain, it is critical to examine the redundancy of all connections to the outside to ensure they are not shared, as described in the following table:

Table 25: Datacenter Building Risk Mitigation

AREA	RISK MITIGATION
Power	Redundant power supply from different suppliers.
Cooling	Independent/redundant cooling system for each datacenter room.
Network Connectivity	Redundant networking connectivity between datacenter buildings from different providers Redundant internet connectivity from different ISP
Datacenter buildings/server room	Where possible, utilize multiple datacenter buildings and/or server rooms in separate datacenter buildings so a single server room does not affect all of production. Distribute multi-component services equally across datacenter server rooms.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1045

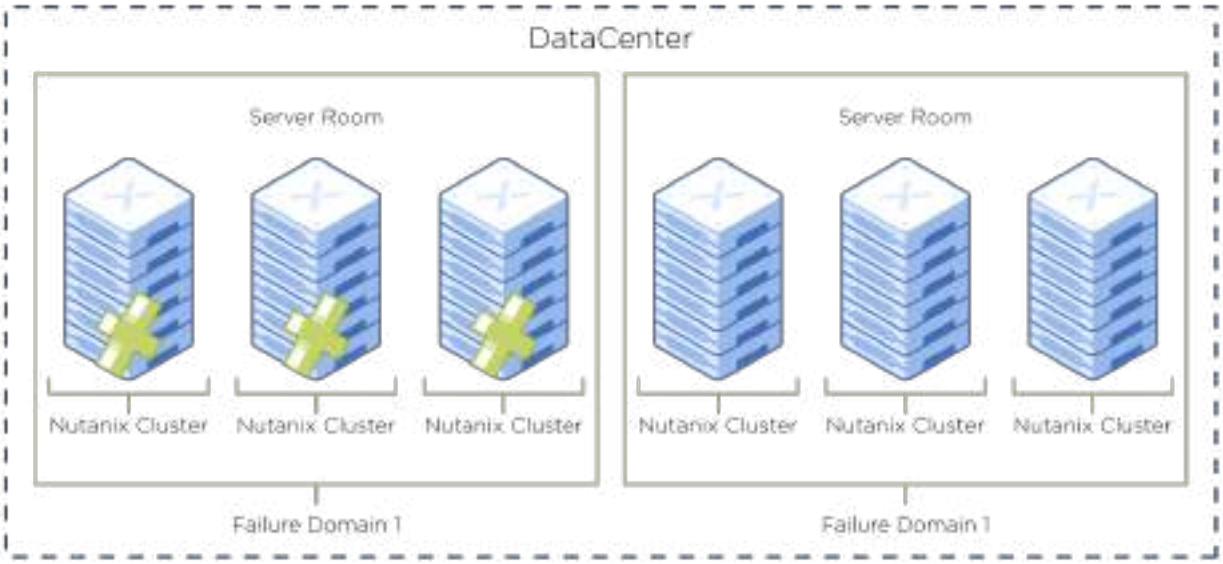


Figure 26: Datacenter Building Failure Domain

Designing Datacenter Locations

Based on typical enterprise requirements the logical implementation for DR across regions, availability zones and datacenters will use the following layout.

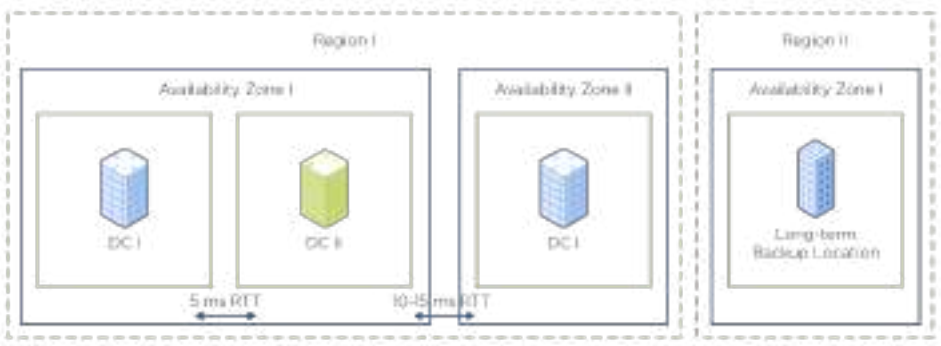


Figure 27: Designing Datacenter Locations

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1046

Regions

Table 26: Two region implementation for DR

REGION-001	TWO REGIONS ARE USED, SUCH AS: REGION 1 (PRIMARY REGION) RUNS ACTIVE WORKLOADS AND PROVIDES TWO AVAILABILITY ZONES FOR DISASTER RECOVERY AND REGION 2 (SECONDARY REGION) PROVIDES A LOCATION FOR LONG-TERM BACKUP RETENTION.
Justification	Regional separation of running workloads and disaster recovery capabilities plus long-term backup retention.
Implication	It may take a long time to restore services in or from Region 2 when Region 1 fails but the likelihood of an entire region failing is low.

Table 27: Single region implementation for DR

REGION-002	ONE REGION HOSTS PRIMARY AND DISASTER RECOVERY AVAILABILITY ZONES.
Justification	• Addresses the requirement to have active workloads and disaster recovery capabilities in a region separate from where the long-term backups are stored. • Services must be available in one region only based on end-user location • Staff only available in one region • Budget constraints • One region can host multiple datacenters within 100 km and provide RTT of maximum 5ms which will be required to meet infrastructure RPO 0. • One region can host datacenter separation of more than 200 KM which is required for disaster recovery purposes.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1047

REGION-002	ONE REGION HOSTS PRIMARY AND DISASTER RECOVERY AVAILABILITY ZONES.
Implication	• If Region 1 fails, the services has to be rebuilt from backups from outside Region 1. • Staff has to travel to Region 2 to build up the services from backups, or backups must be relocated to Region 1 when Region 1 becomes available after the failure, and the services must be rebuilt/restored.

Table 28: Long term retention backups are placed in Region 2

REGION-003	LONG TERM RETENTION BACKUPS ARE PLACED IN REGION 2.
Justification	Addresses the requirement to have long-term backups stored in a separate region from active workloads and provides disaster recovery capabilities in case of regional disasters.
Implication	• If Region 1 fails, the services has to be rebuilt from backups from outside Region 1. • Staff has to travel to Region 2 to build up the services from backups, or backups must be relocated to Region 1 when Region 1 becomes available after the failure, and the services must be rebuilt/restored.

Availability Zones

Table 29: Three availability zones in two regions

AZ-001	THREE AVAILABILITY ZONES IN TWO REGIONS WILL BE USED, SUCH AS: DC1 AND DC2 IN REGION 1 RUNNING WORKLOADS, AZ2 IN REGION 1 FOR DISASTER RECOVERY PURPOSES, AND AZ1 IN REGION 2 WHERE LONG-TERM BACKUPS ARE STORED.
Justification	Required to provide the separation required

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1048

AZ-001	THREE AVAILABILITY ZONES IN TWO REGIONS WILL BE USED, SUCH AS: DC1 AND DC2 IN REGION 1 RUNNING WORKLOADS, AZ2 IN REGION 1 FOR DISASTER RECOVERY PURPOSES, AND AZ1 IN REGION 2 WHERE LONG-TERM BACKUPS ARE STORED.
Implication	• Many availability zones to manage. • Multiple network connections to manage between availability zones.

Table 30: Two availability zones in Region 1

AZ-002	TWO AVAILABILITY ZONES IN REGION 1 WILL HOST PRIMARY WORKLOADS.REGION 2 DR SITE WILL HOST ANY WITNESS FUNCTIONALITY REQUIRED FOR SERVICE AVAILABILITY.
Justification	• Addresses the requirement to have applications available across multiple availability zones during normal production • Distance is more than 100km and provides RTT of less than 5ms meaning it is technically possible to meet an RPO = 0 requirement.
Implication	Network connections between availability zones are critical for service availability and are also exposed to more risk compared to intra-availability-zone connections.

Table 31: One availability zone in Region 1 to provide disaster recovery

AZ-003	ONE AVAILABILITY ZONE IN REGION 1 WILL BE USED TO PROVIDE DISASTER RECOVERY CAPABILITIES.
Justification	Addresses the requirement to provide disaster recovery across availability zones within the same region.
Implication	No availability zone redundancy during a disaster recovery scenario.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1049

Table 32: One availability zone in Region 2 hosts backups.

AZ-004	ONE AVAILABILITY ZONE IN REGION 2 HOSTS LONG-TERM BACKUPS.
Justification	Addresses the requirement to have long-term backups stored in a separate region from running workloads, and disaster recovery capabilities are provided.
Implication	Staff has to travel to Region 2 to build up the services from backups, or backups must be relocated to Region 1 when Region 1 becomes available after the failure, and the services must be rebuilt/restored.

Designing Workload Domains

This document uses workload domains as building blocks. Each workload domain consists of a set of Nutanix nodes that are managed by the same management instance (Nutanix Prism Central/VMware vCenter) and connected to the same network domain.

Workload Domain Architecture

A single workload domain can include different hardware and software combinations, have homogeneous ESXi or AHV nodes, or mix ESXi (running VMs) and AHV (not running VMs) in a single cluster. These can be configured to satisfy redundancy, performance, and capacity requirements.

Normally, single workload domains occupy a single rack. However, you can aggregate multiple workload domains in a single rack or span a single workload domain across multiple racks.

Workload Domain Rack Mapping

Mapping workload domains to datacenter racks is not one to one. While the workload domain is a repeatable building block, a rack is a unit of size. Workload domains and datacenter racks can have different characteristics; you map workload domains to datacenter racks according to the use case and rack specifications.

Nutanix Cluster Layout

Single Rack, Single Workload Domain

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1050

One workload domain can occupy a single datacenter rack. All nodes from a workload domain are connected to a single pair of TOR switches.

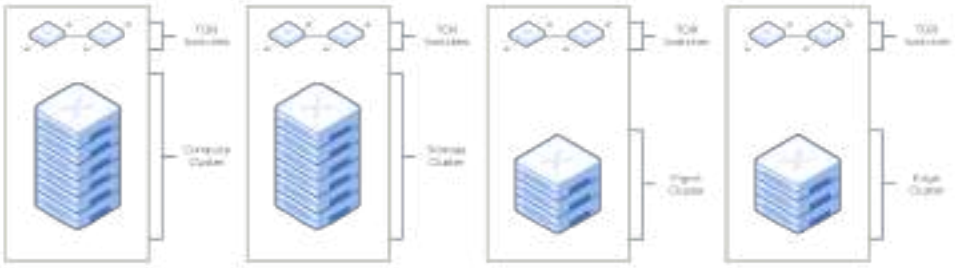


Figure 28: Single Rack Single Workload Domain

Single Rack, Multiple Workload Domains

One workload domain can occupy a single datacenter rack. All nodes from a workload domain are connected to a single pair of TOR switches.

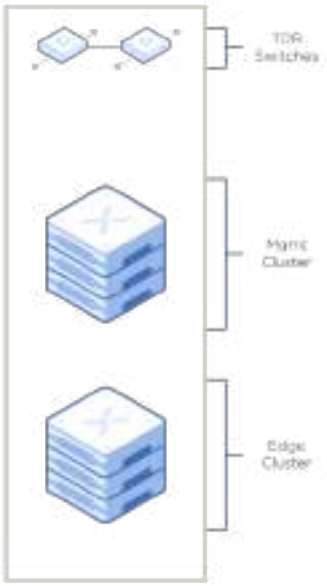


Figure 29: Single Rack, Multiple Workload Domains

Multiple Racks, Single Workload Domain

A single workload domain can span multiple racks. For example, to provide an additional level of data protection (using rack awareness/fault tolerance, see

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1051

the section Data Redundancy and Resiliency) or if a single workload domain is bigger than a single rack can contain.

© 2023 Nutanix, Inc. All rights reserved

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1052

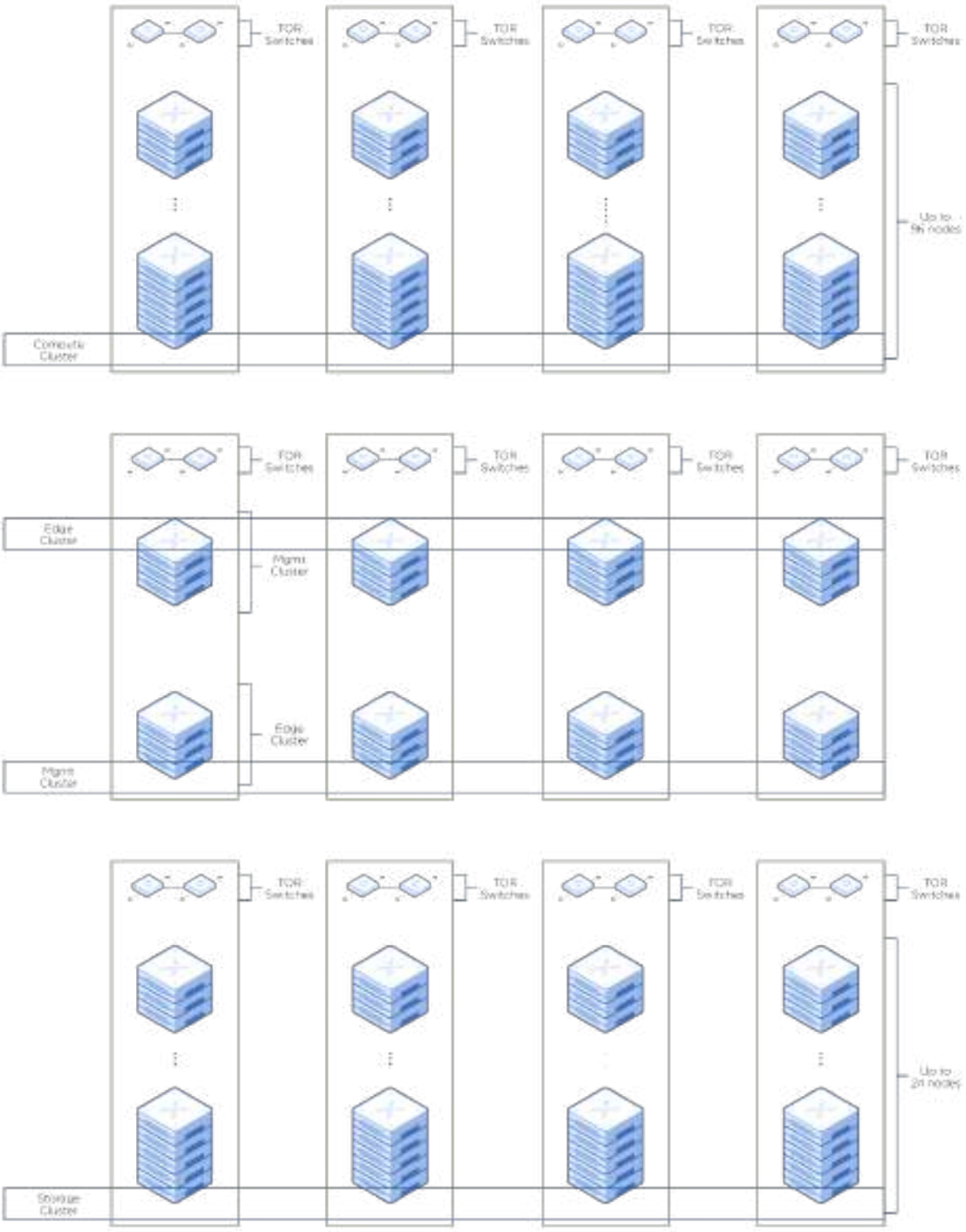


Figure 30: Multiple Racks, Single Workload Domain

© 2023 Nutanix, Inc. All rights reserved

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1053

Pros and Cons

A single workload domain can span multiple racks. For example, to provide an additional level of data protection (using rack awareness/fault tolerance, see the section:

Data Redundancy and Resiliency) or if a single workload domain is bigger than a single rack can contain.

Table 33: Pros and cons

	PROS	CONS
Single Rack/	• Default redundancy level. • Simple to consume.	May use rack space inefficiently.
Single Workload Domain	• Efficient space usage. • Default redundancy level. • Simple to consume.	Increases impact of rack failure.
Single Rack/ Multiple Workload Domains	• Efficient space usage. • Increases resiliency for each workload domain. • Decreases impact of rack failure.	Complexity.

Table 34: Workload Domains Spanning Single or Multiple Racks

PFM-007	DECIDE WHICH WORKLOAD DOMAINS WILL SPAN A SINGLE OR MULTIPLE RACKS
Justification	
Implication	

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1054

Networking

Well-designed networks are critical to a Nutanix deployment's resilience and performance.

A Nutanix cluster can tolerate multiple simultaneous failures because it maintains a set redundancy factor and offers features such as block and rack awareness. However, this level of resilience requires a highly available, redundant network connecting a cluster's nodes. Protecting the cluster's read and write storage capabilities also requires highly available connectivity between nodes. Even with intelligent data placement, if network connectivity between more than the allowed number of nodes breaks down, VMs on the cluster could experience write failures and enter read-only mode.

To optimize I/O speed, Nutanix clusters choose to send each write to another node in the cluster. As a result, a fully populated cluster sends storage replication traffic in a full mesh, using network bandwidth between all Nutanix nodes. Because storage write latency directly correlates to the network latency between Nutanix nodes, any increase in network latency adds to storage write latency.

Physical Switches

A Nutanix environment should use datacenter switches designed to handle high- bandwidth server and storage traffic at low latency. Do not use switches meant for deployment at the campus access layer. Campus access switches may have 10 Gbps ports like datacenter switches, but they are not usually designed to transport a large amount of bidirectional storage replication traffic. Refer to the Nutanix physical networking best practices guide for more information.

The deployment size and purpose also influence physical switch choice. Datacenter switches with large buffers are critical in a large AOS cluster that is going to grow beyond eight nodes or host storage-intensive applications. In smaller clusters or ROBO deployments that have fewer than eight nodes or do not host write-intensive applications, the switch may not experience buffer contention, and you can relax these switch restrictions. There are also some switch types you should never use for any Nutanix deployment because of oversubscription or other architecture choices; we list examples of these as well.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1055

Datacenter switches should have the following characteristics:

- Line rate: Ensures that all ports can simultaneously achieve advertised throughput.
- Low latency: Minimizes port-to-port latency as measured in microseconds or nanoseconds.
- Large per-port buffers: Accommodates speed mismatches from uplinks without dropping frames.
- Nonblocking, with low or no oversubscription: Reduces chance of drops during peak traffic periods.
- 10 Gbps or faster links for Nutanix CVM traffic: Only use 1 Gbps links for additional user VM traffic or when 10 Gbps connections are not available, such as in a ROBO deployment. Limit Nutanix clusters using 1 Gbps links to eight nodes maximum.

Switch manufacturers' datasheets, specifications, and white papers can help identify these characteristics. For example, a common datacenter switch datasheet may show a per-port buffer of 1 MB, while an access layer or fabric extension device has a per-port buffer of around 150 KB. During periods of high traffic, or when using links with a speed mismatch (such as 40 Gbps uplinks to 10 Gbps edge ports), a smaller buffer can lead to frame drops, increasing storage latency.

The following table is not exhaustive, but it includes examples of model lines that meet the above requirements for high-performance or large clusters. Models similar to the ones shown are also generally good choices.

Table 35: Examples of Recommended Switch Models

EXAMPLES OF HIGH PERFORMANCE SWITCH MODELS		
Arista 7050X3	Arista 7160	Arista 7170
Arista 7280	Cisco Nexus 9000	Cisco Nexus 7000
Cisco Nexus 7000	Dell S5200-ON	HPE FM3810
HPE FM3132Q	Juniper QFX-5100	Lenovo NE2580O

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1056

Mellanox SN2010	Mellanox SN2100	Mellanox SN2410

The following are examples of switches that do not meet high-performance datacenter switch requirements but are acceptable for ROBO clusters and clusters with fewer than eight nodes or low performance requirements:

Table 36: Examples of Robo Or Smb Switch Models

EXAMPLES OF ROBO OR SMB SWITCH MODELS		
Arista 7050	Arista 7150S	Cisco Nexus 3000
Cisco Catalyst 9000	Cisco Catalyst 3000	HPE FM2072

The following are examples of switches that are never acceptable for any Nutanix deployment:

Table 37: Switches that are not acceptable

SWITCH	REASON NOT RECOMMENDED
Cisco Nexus 2000 (Fabric Extender)	Highly oversubscribed with small per-port buffers.
10 Gbps expansion cards in a 1 Gbps access switch	10 Gbps expansion cards provide uplink bandwidth for the switch, not server connectivity.

Each Nutanix node also has an out-of-band connection for IPMI, iLO, iDRAC, or similar management. Because out-of-band connections do not have the same latency or throughput requirements of VM or storage networking, they can use an access layer switch.

Note: Nutanix recommends an out-of-band management switch network separate from the primary network to ensure management availability. Configure server-facing ports in the management network as access ports and do not use VLAN trunking for these ports. Access to this critical management network should be restricted.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1057

Table 38: Using a Large Buffer Datacenter Switch at 10GBPS or Faster

NET-001	USE A LARGE BUFFER DATACENTER SWITCH AT 10GBPS OR FASTER
Justification	Achieves high performance for critical storage and VM traffic converged on the same network fabric.
Implication	Requires data center switches that may be more expensive than campus or access layer switches.

Network Topology

In a greenfield environment, Nutanix recommends a leaf-spine network topology because it is easy to scale, achieves high performance with low latency, and provides resilience. A leaf-spine topology requires at least two spine switches and two leaf switches. Every leaf connects to every spine using uplink ports.

There are no connections between the spine switches or between the leaf switches in a conventional leaf-spine design. To form a Nutanix cluster it's critical that all nodes are in the same broadcast domain, thus in any leaf-spine design all leaf switches connecting nodes in a cluster should carry the Nutanix VLAN. This can be accomplished with physical connections between switches, using an overlay network, or using a pure layer 2 design. The following example shows a pure layer 2 design or overlay.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1058

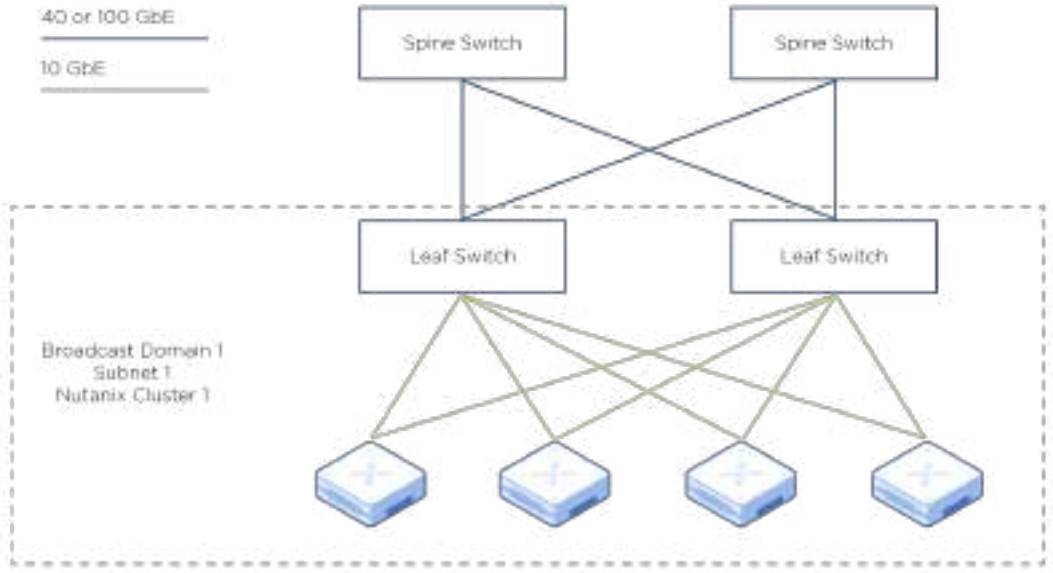


Figure 31: Pure Layer 2 Design

You may also choose a leaf-spine topology that uses links between switches to guarantee layer 2 connectivity between Nutanix nodes.

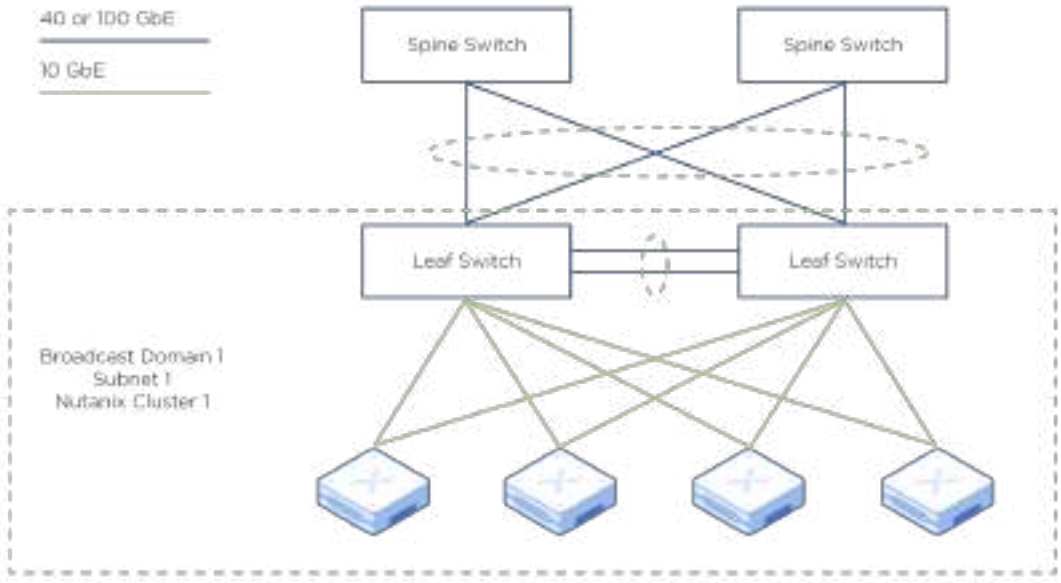


Figure 32: Leaf Spine Topology

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1059

Use uplinks that are a higher speed than the edge ports to reduce uplink oversubscription. To increase uplink capacity, add spine switches or uplink ports as needed.

The core-aggregation-access (or multi-tier) network design is a modular layout that allows you to upgrade and scale layers independently. Nutanix clusters perform well in the core-aggregation-access topology, but extra caution should be taken around scaling the Nutanix cluster.

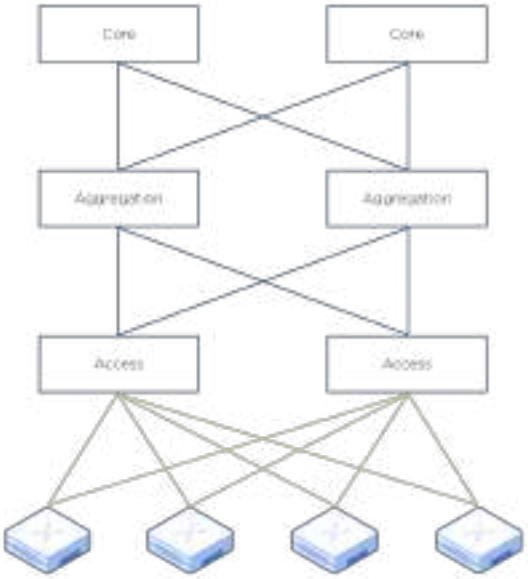


Figure 33: Core Aggregation Access Design

In pre-existing environments, you may not have full control over the network topology, but your design should meet the following requirements:

Guidelines:

- Networks must be highly available and tolerate individual device failures.
- Ensure that each layer of the network topology can tolerate device failure.
- Avoid configurations or technologies that do not maintain system availability during single device outages or upgrades such as stacked switches.
- Ensure that there are no more than three switches between any two Nutanix nodes in the same cluster. Nutanix nodes send storage replication traffic to

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1060

each other in a distributed fashion over the top-of-rack network. One Nutanix node can therefore send replication traffic to any other Nutanix node in the cluster.

- The network should provide low and predictable latency for this traffic. Leaf-spine networks meet this requirement by design. For the core-aggregation-access model, ensure that all nodes in a Nutanix cluster share the same aggregation layer to meet the three-switch-hop rule.

Oversubscription occurs when an intermediate network device or link does not have enough capacity to allow line rate communication between the systems connected to it. For example, if a 10 Gbps link connects two switches and four hosts connect to each switch at 10 Gbps, the connecting link is oversubscribed. Oversubscription is often expressed as a ratio—in this case 4:1, as the environment could potentially attempt to transmit 40 Gbps between the switches with only 10 Gbps available. Achieving a ratio of 1:1 is not always feasible.

Recommendation 1

- Keep the oversubscription ratio as small as possible based on budget and available capacity.

In a typical deployment where Nutanix nodes connect to redundant top-of-rack switches, storage replication traffic between CVMs traverses multiple devices.

Recommendation 2

- To avoid packet loss due to link oversubscription, ensure that the switch uplinks consist of multiple interfaces operating at a faster speed than the Nutanix host interfaces. For example, for nodes connected at 10 Gbps, interswitch connections should consist of multiple 10, 40, or 100 Gbps links.
- Connect all Nutanix nodes that form a cluster to the same switch fabric. Do not stretch a single Nutanix cluster across multiple, disconnected switch fabrics. A switch fabric is a single leaf-spine topology or all switches connected to the same switch aggregation layer. Every Nutanix node in a cluster should therefore be in the same L2 broadcast domain and share the same IP subnet.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1061

See section Security > Network Segmentation for service placement information and design decisions.

Recommendation 3

- Use native, or untagged, VLANs for the hypervisor host and CVM for ease of initial configuration. Ensure that this untagged traffic is mapped into the CVM and hypervisor VLAN only on the required switch ports to reduce risk.
- Use tagged VLANs for all guest VM traffic and add the required guest VM VLANs to all connected switch ports for hosts in the Nutanix cluster.
- Limit guest VLANs for guest VM traffic to the smallest number of physical switches and switch ports possible to reduce broadcast network traffic load.

Table 39: Using a Leaf-Spine Network Topology for New Environments

NET-002	USE A LEAF-SPINE NETWORK TOPOLOGY FOR NEW ENVIRONMENTS.
Justification	Achieves high performance for critical storage and VM traffic and is easy to scale.
Implication	Requires more network connections between switches and may require new network design.

Table 40: Populate Each Rack with Two 10GBE or Faster TOR Switches

NET-003	POPULATE EACH RACK WITH TWO 10GBE OR FASTER TOR SWITCHES
Justification	Simplifies the design, follows the leaf/spine model, and provides high performance and high availability to the network.
Implication	Increases rack space requirements, costs, and the number of leafs.

Table 41: Avoid Switch Stacking to Ensure Network Availability During Individual Device Failure

NET-004	AVOID SWITCH STACKING TO ENSURE NETWORK AVAILABILITY DURING INDIVIDUAL DEVICE FAILURE.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1062

Justification	Critical network infrastructure must be redundant between all CVMs in the same Nutanix cluster.
Implication	More network devices may be required to provide high availability and reduce single points of failure.

Table 42: Use No More Than Three Switches Between Two Nutanix Nodes in the Same Cluster

NET-005	ENSURE THAT THERE ARE NO MORE THAN THREE SWITCHES BETWEEN ANY TWO NUTANIX NODES IN THE SAME CLUSTER.
Justification	Storage latency is directly related to network latency, so the network distance between nodes in the same cluster must be reduced.
Implication	A Nutanix cluster cannot span multiple sites or switch fabrics, instead use data replication technologies instead to provide high availability between sites.

Table 43: Reduce Network Oversubscription to Achieve a Near-1:1 Ratio

NET-006	REDUCE NETWORK OVERSUBSCRIPTION TO ACHIEVE AS CLOSE TO A 1:1 RATIO AS POSSIBLE.
Justification	Dropped network packets or a congested network will immediately impact storage performance and must be avoided in the design phase.
Implication	Higher bandwidth paths must be created using more uplink paths of faster speed between switches.

Table 44: Configure CVM and Hypervisor VLAN on Server-facing Switch Ports

NET-007	CONFIGURE THE CVM AND HYPERVISOR VLAN AS NATIVE, OR UNTAGGED ON SERVER FACING SWITCH PORTS.
Justification	Newly added nodes use untagged traffic for discovery and will work out of the box, reducing manual server configuration.
Implication	Network switches must be configured to accept untagged frames on ports facing Nutanix servers and place the traffic into the CVM and hypervisor VLAN.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1063

Table 45: Use Tagged VLANs on Switch Ports for All Guest Workloads

NET-008	USE TAGGED VLANS ON THE SWITCH PORTS FOR ALL GUEST WORKLOADS.
Justification	Workloads should be separated from each other and from the CVM and hypervisor network using VLANs.
Implication	Multiple VLANs and IP subnets are required.

Broadcast Domains

Performing layer 3 routing at the top of rack, creating a layer 3 and layer 2 domain boundary within a single rack, is a growing network trend. Each rack is a different IP subnet and a different layer 2 broadcast domain. This layer 3 design decreases the size of the layer 2 broadcast domain to remove some common problems of sharing a large broadcast domain among many racks of servers, but it can add complexity for applications that require layer 2 connectivity.

In contrast, the traditional layer 2 design shares a single broadcast domain or VLAN among many racks of switches. In the layer 2 design, a switch and server in one rack share the same VLANs as a switch and server in another rack. Routing between IP subnets is performed either in the spine or in the aggregation layer. The endpoints in the same switch fabric have layer 2 connectivity without going through a router, but this can increase the number of endpoints that share a noisy broadcast domain.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1064

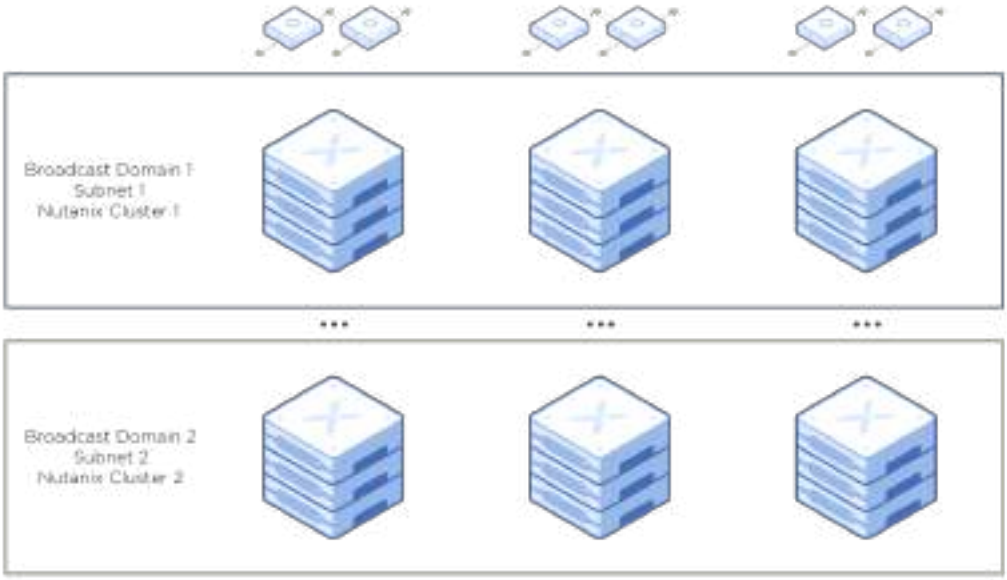


Figure 34: Layer 2 Network Design

Nutanix recommends a traditional layer 2 network design to ensure that CVMs and hosts can communicate in the same broadcast domain even if they are in separate racks. The CVM and host must be in the same broadcast domain and IP subnet.

If a layer 3 network design is chosen, there are two possible ways to make this work with a Nutanix deployment:

- Keep all Nutanix nodes in a cluster inside the same rack.
- Create an overlay network in the switch fabric that creates a virtual broadcast domain that is shared across racks for the Nutanix CVMs and hosts.

Keeping all of the Nutanix nodes in a single cluster in a single rack has the limitation of losing resilience against rack failure. Creating an overlay in the network fabric:

- Requires special configuration.
- May require specific network hardware to achieve.
- Increases configuration complexity.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1065

Spreading a broadcast domain across racks virtually may also raise concerns that the original intent of the layer 3 design, reducing broadcast domain scope, is now violated.

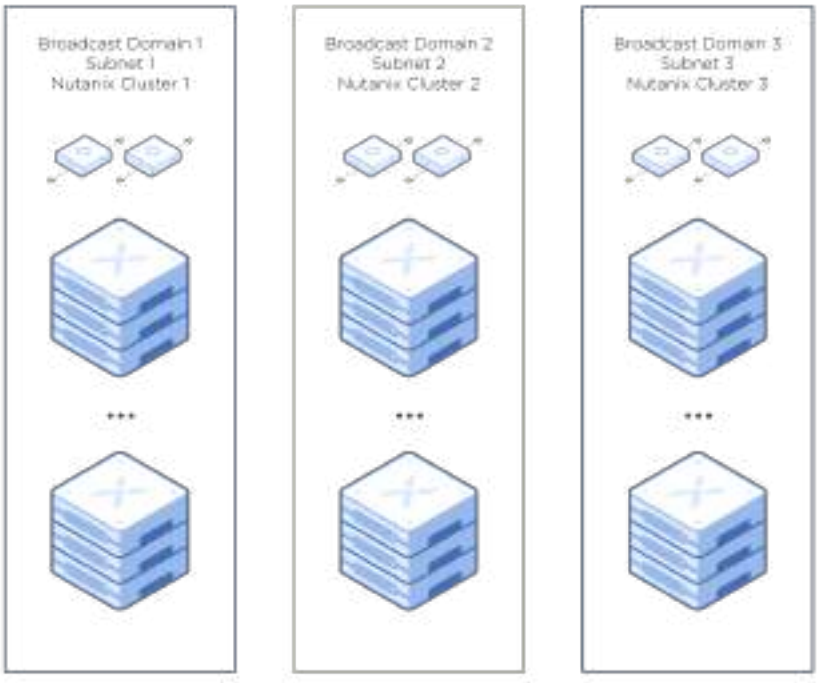


Figure 35: Layer 3 Network Design

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1066

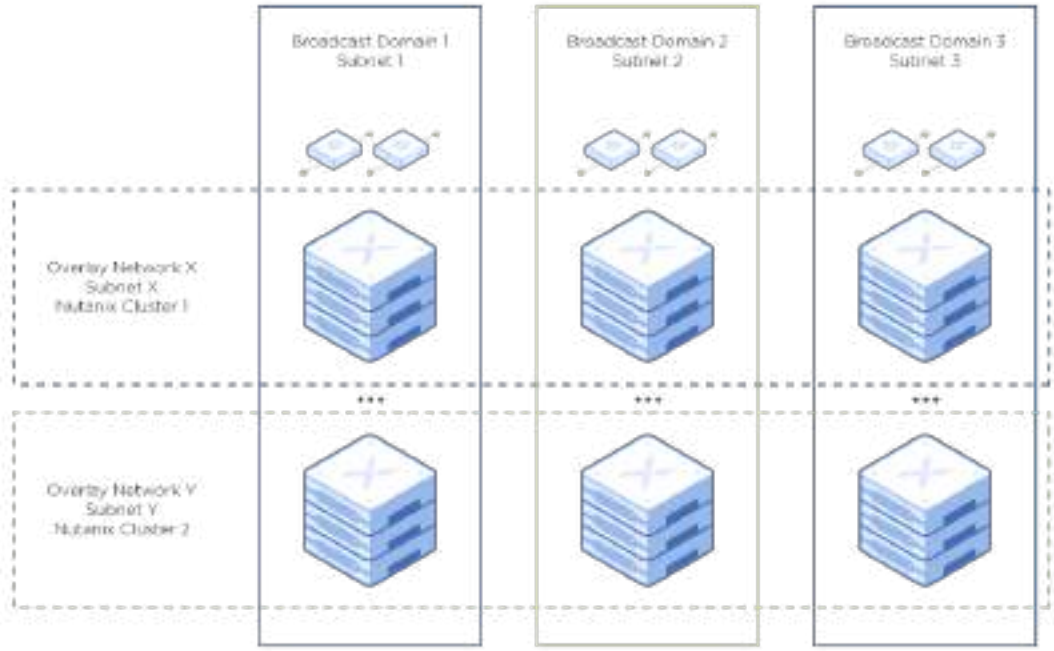


Figure 36: Layer 3 Network Design with Overlay

Table 46: Use a Layer 2 Network Design

NET-009	USE A LAYER 2 NETWORK DESIGN
Justification	Nutanix CVMs and hypervisor hosts must be in the same broadcast domain to function properly after a CVM becomes unavailable.
Implication	A broadcast domain failure or storm, can span multiple racks.

Scaling the Network

To scale the leaf-spine network:

- Add two leaf switches and a management switch for every rack.
- Add spine switches as needed.

Because there are no more than three switch hops between any two Nutanix nodes in this design, a Nutanix cluster can easily span multiple racks and still use the same switch fabric. Use a network design that brings the layer 2

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1067

broadcast domain to every switch that connects Nutanix nodes in the same cluster.

The following example shows a leaf-spine network using either an overlay or a pure layer 2 design, with no connections are required between leaf switches.

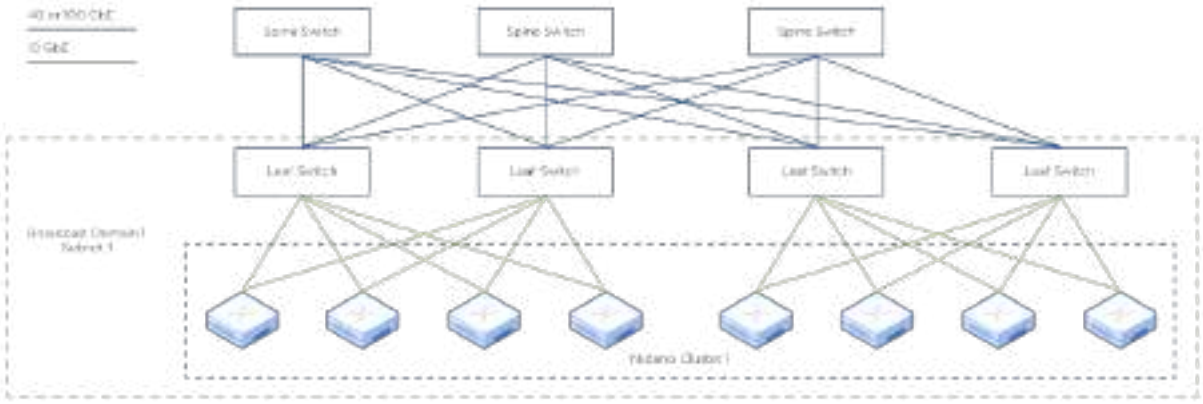


Figure 37: Logical View of Leaf Spine Scale

You may choose a leaf-spine design where a pair of leaf switches are connected using link aggregation. Discuss scale plans with the switch vendor when scaling beyond two spine switches in this design.

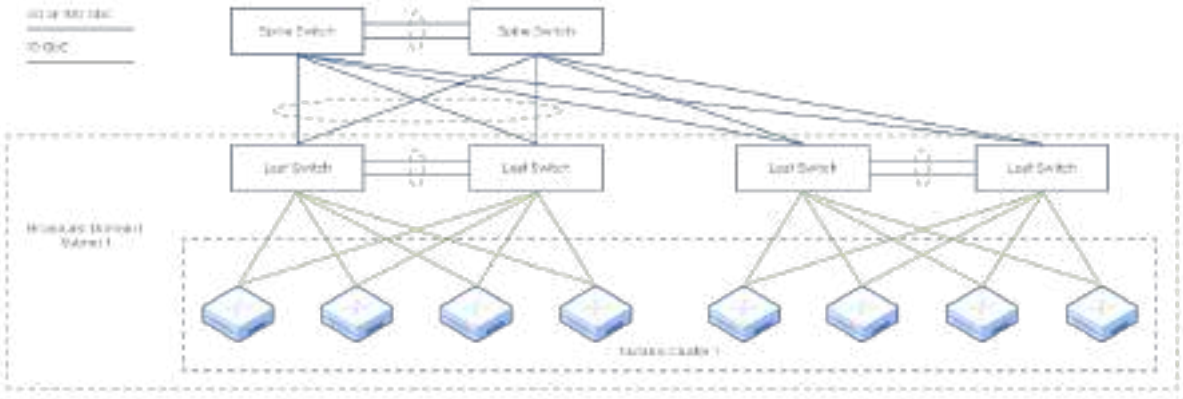


Figure 38: Leaf Switches Connected Using Link Aggregation

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1068

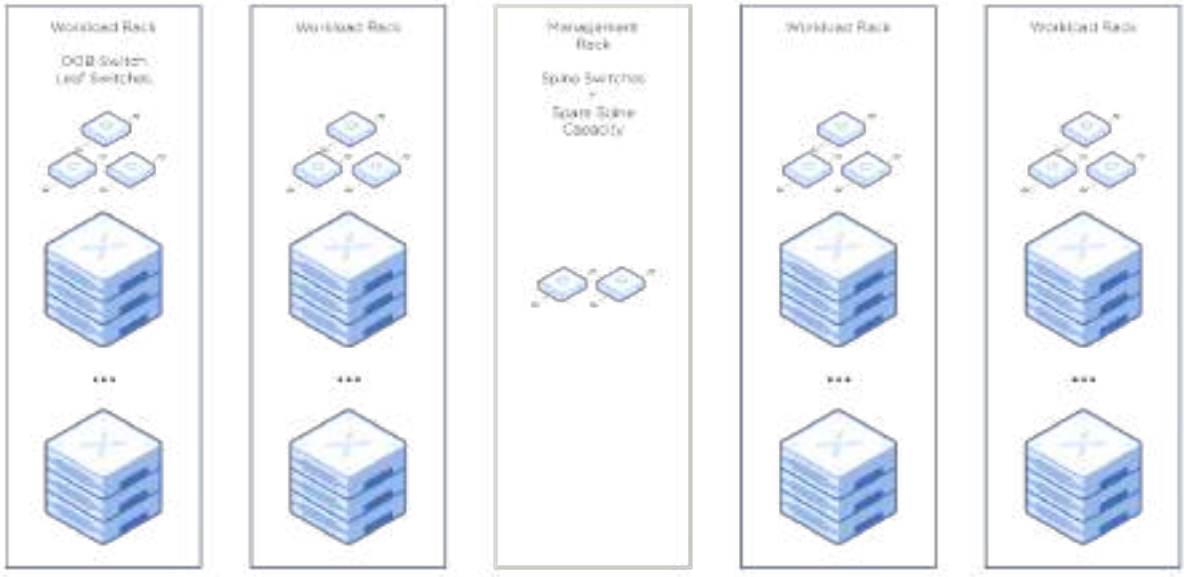


Figure 39: Rack Level View of Leaf Spine

Determining when to add new spine switches is a function of:

- How many ports the spine switch has.
- How many leaf switches (or racks) there are.
- How many connections are formed between each leaf and spine.

It's also important to take into account the throughput capacity of the switch and the throughput required between each rack.

In the previous example with 4 workload racks, assume you have 2 x 32-port spine switches with a single 100 Gbps connection to every leaf. Also assume each TOR leaf switch has 48 x 10 Gbps ports and 6 x 100 Gbps ports.

Spine switch port utilization is at 8 out of 32 ports on each spine, leaving capacity to grow up to 16 racks at each spine (32 spine ports divided by 2 ports per rack).

Each leaf would be using 1 out of the 6 available uplinks and each leaf can support up to 48 connected servers. However, at this point these two spine switches will be processing a lot of traffic and may be overloaded depending on their specifications.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1069

Calculating oversubscription ratios, if you assume that each rack has 24 x 10Gbps dual-connected servers with dual leaf switches, for a total of 240 Gbps bandwidth capacity at each leaf, oversubscription is 2.4:1. This design is oversubscribed and would not be recommended.

One way to reduce oversubscription is to add another 100Gbps uplink from each leaf to the existing spine switches. However, that reduces the total number of supported racks by half to 8, (32 spine ports divided by 4 ports per rack), so you must carefully consider which leaf and spine switches are selected and what scale you would like to achieve.

Another way to grow spine capacity is to add a spine switch, which would then require another uplink from every leaf, and greatly increase the total throughput of the switch fabric without reducing the number of racks supported. If you added another spine switch to bring the total to 3 spines, each leaf switch would add another 100Gbps uplink (reducing oversubscription), but each spine could still support 16 racks (32 spine ports divided by 2 ports per rack). With 6 uplinks on every leaf switch, you can support designs with up to 6 spines in this example.

Scaling the multi-tier network design may require adding another aggregation and access layer to the core. In this case, there would be more than three switch hops between the two access layers.

> Note: The guideline here is to ensure that you add Nutanix nodes in separate aggregation and access layers to separate clusters to keep the number of switch hops between nodes in the same cluster to three or fewer.

In the following figure, Cluster 1 connects to one aggregation layer and Cluster 2 connects to another.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1070

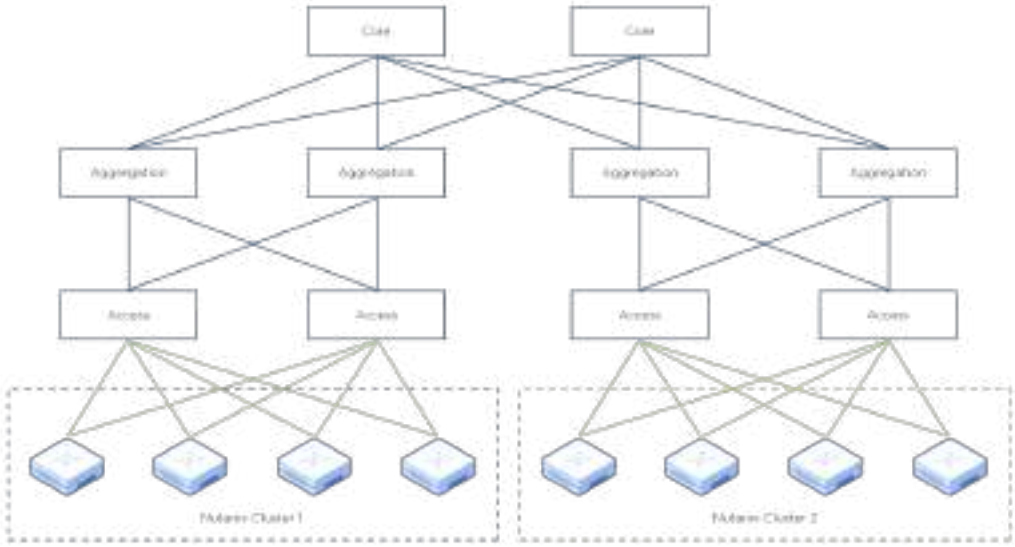


Figure 40: Clusters Connecting to Different Aggregation Layers

Host Networking

AHV Networking

AHV leverages Open vSwitch (OVS) for all VM networking. The virtual switch is referred to as a bridge and uses a br prefix in the name. Read the AHV Networking section on the Nutanix Support Portal for in depth guidance on any settings not covered here.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1071

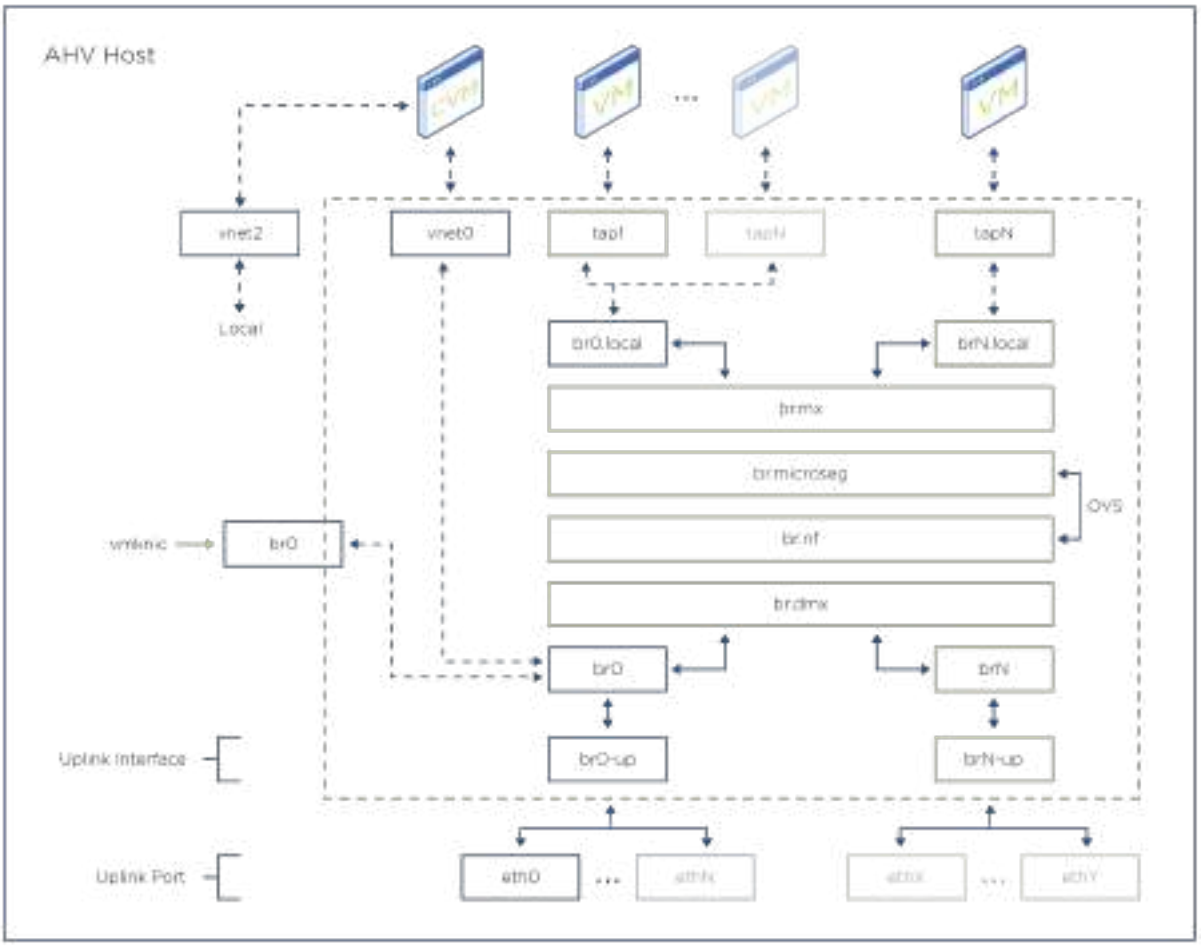


Figure 41: AHV Networking

Bridge

The default bridge, br0, behaves like a layer 2 learning switch that maintains a MAC address table. Additional uplink interfaces for separate physical networks are added as brN, where N is the new bridge number. To ensure that all VM traffic goes through the same set of firewall rules and the same set of network functions, a bridge chain is created with all microsegmentation and network function rules being placed in br. microseg and br.nf respectively.

Traffic from VMs enters the bridge at brN.local. Next, traffic is multiplexed onto the bridge chain, goes through the firewall and network function ruleset, and

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1072

is then demultiplexed on the correct brN for physical network forwarding. The reverse path is followed for traffic flowing from the physical network to VMs.

All traffic between VMs must flow through the entire bridge chain, since brN is the only bridge that performs switching. All other bridges simply apply rules or pass traffic up and down the bridge chain.

Recommendation

- Use only the default bridge, br0, with the two fastest network adapters in the host.
- Converge the management, storage, and workload traffic on this single pair of uplink adapters.
- Additional brN bridges should only be added when connection to a separate physical network is required. For example, if the top-of-rack has two pairs of switches, one pair for storage and management, and another pair for workload traffic, it makes sense to create another bridge, br1 and place the workloads on this bridge.
- Other valid use cases include separate physical networks for iSCSI Volumes workloads, backplane intracluster replication, or workloads like virtual firewalls that require access to a physically separate network. In these cases, the additional bridge is used to connect to the separate top-of-rack network. If there is only a single top-of-rack physical network, then a single bridge with VLAN separation is sufficient.

AHV also includes a Linux bridge called virbr0. The virbr0 Linux bridge carries management traffic between the CVM and AHV host. All other storage, host, and workload network traffic flows through the br0 OVS bridge, or additional brN bridges if configured.

> Note: Do not modify the configuration of any bridges inside the AHV host unless following an official Nutanix guide.

Bond

Bonded ports aggregate the physical interfaces on the AHV host. By default, a bond named br0-up is created in bridge br0. After the node imaging process, all interfaces are placed within a single bond, which is a requirement for the foundation imaging process. A bridge can have only a single bond.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1073

Bonds allow for several load-balancing modes, including active-backup, balance-slb and balance-tcp. Link Aggregation Control Protocol (LACP) can also be activated for a bond for link aggregation. The “bond_mode” setting is not specified during installation and therefore defaults to active-backup, which is the default configuration.

Recommendation

Keep the following recommendations in mind for all bond scenarios to prevent undesired behavior and maintain NIC compatibility.

- Ensure that each bond has at least two uplinks for redundancy.
- Do not mix NIC models from different vendors in the same bond.
- Do not mix NICs of different speeds in the same bond.

Uplink Load Balancing

The following bond modes are available:

- active-backup: Default configuration which transmits all traffic over a single active adapter. If the active adapter becomes unavailable, another adapter in the bond will become active. Limits host throughput to the bandwidth of a single network adapter. No additional switch configuration required.
- balance-slb: Distributes VM NICs across adapters in the bond and periodically rebalances for even uplink utilization. Limits VM per-nic throughput to a single network adapter, but allows utilization of multiple host physical interfaces for multiple VM NICs. NOTE: Not recommended due to negative interaction with default IGMP snooping and pruning network settings for multicast.
- balance-tcp with LACP: Distributes VM NIC TCP or UDP session across adapters in the bond. Limits per-nic throughput to the maximum bond bandwidth (number of physical uplink adapters * speed). Requires physical switch link aggregation. Used when LACP negotiation is required by the datacenter team or throughput requirements exceed a single NIC.

Recommendation

- To keep network configuration simple, use the standard 1,500 byte MTU in the hosts, CVMs, and workload VMs. Nutanix does not recommend jumbo

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1074

frames unless specifically required by high-performance Nutanix Volumes iSCSI workloads or specific workload requirements.

- When switching from 1,500-byte frames to 9,000-byte frames, performance improvements are generally not significant unless the workload uses the maximum network bandwidth for read traffic.

For more information on when to use jumbo frames, see the Nutanix Volumes Guide and AHV Networking guides.

Table 47: Connecting NICs to TOR Switches

NET-010	CONNECT AT LEAST ONE 10 GBE OR FASTER NIC TO EACH TOR SWITCH
Justification	Maintains high availability in the event of the loss of one switch.
Implication	Requires at least two TOR switches, which will impact cost and rack space. Increases total bandwidth to each host to 20 Gbps.

Table 48: Using Bridges with Uplinks

NET-011	USE A SINGLE BR0 BRIDGE WITH AT LEAST TWO OF THE FASTEST UPLINKS OF THE SAME SPEED UNLESS MULTIPLE PHYSICAL NETWORKS ARE REQUIRED.
Justification	Simplifies the design, requiring fewer physical switches and switch ports, while relying on high bandwidth of 10Gbps and faster adapters.
Implication	All traffic is sent over a single virtual switch to a single pair of TOR switches.

Table 49: Using NICs of the same vendor within a bond

NET-012	USE NICs OF THE SAME VENDOR WITHIN A BOND
Justification	Ensures NIC compatibility within the bond and prevents undesired failover behavior.
Implication	NIC vendor choice must be considered when initially purchasing or adding NICs.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1075

Table 50: Using VLANs to separate logical networks

NET-013	USE VLANS TO SEPARATE LOGICAL NETWORKS
Justification	Physical hosts have a limited number of network ports and each port adds complexity. Traffic separation can be logically accomplished without numerous physical ports.
Implication	Enables multiple networks to be used at once without additional hardware, saving on costs, and simplifying the design.

Table 51: Load Balancing

NET-014	USE ACTIVE-BACKUP UPLINK LOAD BALANCING
Justification	Simplifies the design and does not need any additional configuration.
Implication	All traffic is transmitted over one adapter, limiting bandwidth to at least 10 Gbps.

Table 52: Using Standard 1500 Byte MTU

NET-015	USE STANDARD 1,500 BYTE MTU AND DO NOT USE JUMBO FRAMES.
Justification	Simplifies the design and does not need any additional configuration. Reduces risk and complexity from non-standard configuration that only increases performance in certain use cases.
Implication	All network frames are limited to the default 1,500-byte maximum size for interoperability, potentially creating more network overhead for high throughput write workloads.

vSphere Networking

VMware vSphere networking follows many of the same design decisions as AHV networking. The critical design choices for vSphere networking are covered here. See the VMware vSphere Networking Guide for more details.

Nutanix hosts with vSphere ESXi use two virtual switches (vSwitches), named vSwitchNutanix and vSwitch0. vSwitchNutanix is the internal, standard vSwitch used for management and storage traffic between the CVM and the hypervisor.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1076

Recommendations

- Do not modify vSwitchNutanix. vSwitch0 is also a standard vSwitch by default, used for communication between CVMs as well as workload traffic.
- Convert vSwitch0 to the distributed vSwitch following Nutanix documentation . Converting to the distributed vSwitch allows central management of networking for all hosts, instead of host-by-host networking configuration. The distributed vSwitch also adds capability for advanced networking functions such as load-based teaming, LACP, and traffic shaping.
- Connect at least two of the fastest adapters of the same speed into vSwitch0 and use the “Route Based on Physical NIC Load” load balancing method to ensure traffic is balanced between uplink adapters.
- Connect these adapters to two separate top-of-rack switches to ensure redundancy.
- Do not add more vSwitches unless a connection to another physical network is needed to meet security or workload requirements.
- All CVM storage, hypervisor host, and workload traffic should flow through vSwitch0 using VLAN separated between the workload traffic and all other traffic.
- Use the default 1,500 byte frame size on all uplinks unless there is a specific performance or application requirement that would justify 9,000 byte jumbo frames.

Table 53: Use Virtual Distributed Switch (VDS)

NET-016	USE VIRTUAL DISTRIBUTED SWITCH (VDS)

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1077

Justification	Reduces the amount of configuration required in the environment. Makes port group provisioning faster and less error prone. Provides additional features such as LACP and bandwidth shaping. Important: Leave the internal vNetwork Standard Switch used by ESXi host and CVM for internal communication in place, including security settings.
Implication	Ability to configure port groups and other features at the cluster switch level vs. individual nodes. Reliance on vCenter for host and VM network configuration management.

Note: Leave the internal vNetwork Standard Switch used by ESXi host and CVM for internal communication in place, including security settings.

Table 54: Connecting NICs to the TOR Switch

NET-017	CONNECT AT LEAST ONE 10 GBE OR FASTER NIC TO EACH TOP-OF-RACK SWITCH
Justification	Maintains high availability in the event of the loss of one switch.
Implication	Requires at least two ToR switches, which will impact cost and rack space. Increases total bandwidth to each host to 20 Gbps.

Table 55: Using Virtual Switches and Uplinks

NET-018	USE A SINGLE VSWITCH0 WITH AT LEAST TWO OF THE FASTEST UPLINKS OF THE SAME SPEED
Justification	Simplifies the design, requiring fewer physical switches and switch ports, while relying on high bandwidth of 10Gbps and faster adapters.
Implication	All traffic is sent over a single virtual switch to a single pair of top-of-rack switches.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1078

Table 56: Load Balancing

NET-019	USE ROUTE BASED ON PHYSICAL NIC LOAD UPLINK LOAD BALANCING
Justification	Achieves load balancing and use of both adapters with no switch side configuration required.
Implication	Requires the vSphere Distributed Switch to spread VM NICs among uplinks to reduce the most utilized physical network adapter.

Table 57: Using Standard 1500 Byte MTU

NET-020	USE STANDARD 1,500 BYTE MTU AND DO NOT USE JUMBO FRAMES.
Justification	Simplifies the design and does not need any additional configuration. Reduces risk and complexity from non-standard configuration that only increases performance in certain use cases.
Implication	All network frames are limited to the default 1,500-byte maximum size for interoperability, potentially creating more network overhead for high throughput write workloads.

Compute and Storage Design

Nutanix HCI is a converged storage and compute solution which leverages local hardware components (CPU, memory, and storage) and creates a distributed platform for running workloads.

Each node runs an industry-standard hypervisor and the Nutanix CVM. The Nutanix CVM provides the software intelligence for the platform. It is responsible for serving all IO to VMs that run on the platform.

The following logical diagram illustrates the relationship of the components of a Nutanix node:

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1079

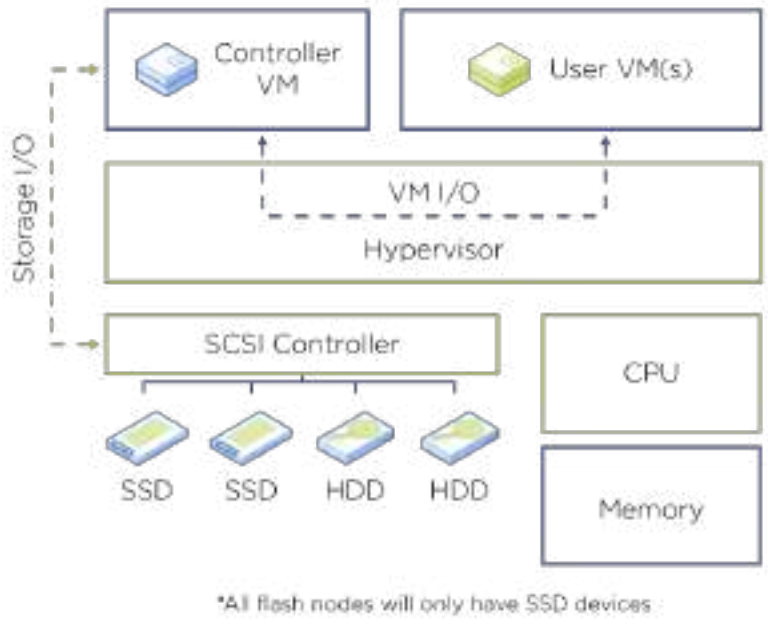


Figure 42: Relationship between the Components of the Nutanix Node

The CVM controls the storage devices directly and creates a logical construct called a storage pool of all disks from all nodes in the cluster. For AHV it uses PCI passthrough and for ESXi it uses VMDirectPathIO.

Compute Design

AHV CPU and Memory Planning

AHV lets you configure vCPUs (similar to sockets) and cores per vCPU (similar to CPU cores) for every VM. Except for the memory used by the CVM and the AHV software, all physical memory can be allocated for use by VMs. AHV guarantees memory allocated to each VM and doesn't overcommit or swap which can impact performance.

The amount of memory required by an AHV host varies based on a number of factors. The host uses from 2GB to 10GB of memory on hosts with 512GB memory.

NUMA and VMs

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1080

Processor sockets have integrated memory controllers. A VM has faster access to memory attached to the physical CPU where it is running versus memory attached to another CPU in the same host. This is called Non-Uniform Memory Access (NUMA). As a result, the best practice is to create VMs that fit within the memory available to the CPU where the VM is running whenever possible.

Table 58: Running Non-NUMA-aware Applications on a VM

CMP-001	IF RUNNING A NON-NUMA-AWARE APPLICATION ON A VM, CONFIGURE THE VM'S MEMORY AND VCPU TO FIT WITHIN A NUMA NODE ON AN AHV HOST.
Justification	This prevents the VM's vCPU and memory access from crossing NUMA boundaries.
Implication	Avoiding crossing NUMA boundaries results in better, more predictable performance.

For example, if a host has 2 CPU sockets with 8 cores each and 256GB memory, the host has 2 NUMA nodes, each with:

- 8 CPU cores
- 128GB memory

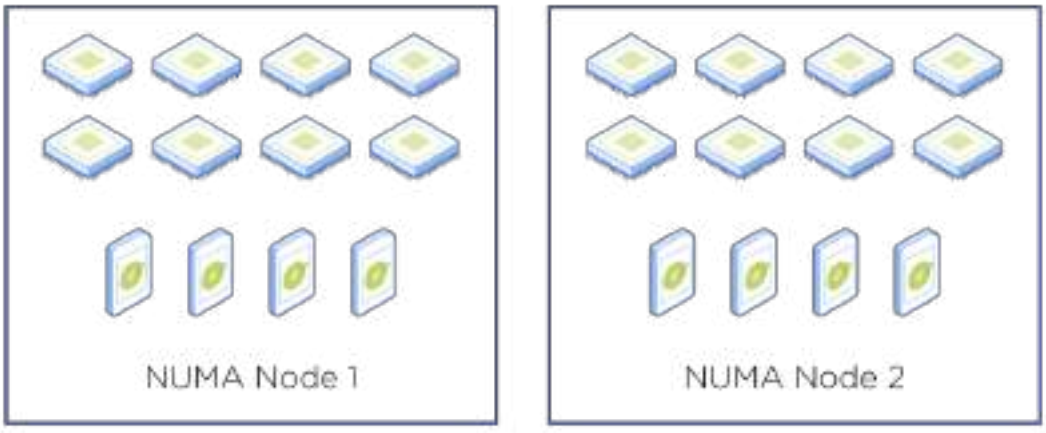


Figure 43: Example Host with 2 NUMA Nodes

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1081

For example, a VM that has 4 vCPUs and 64GB memory, will fit within a single NUMA node on the host and achieve the best performance.

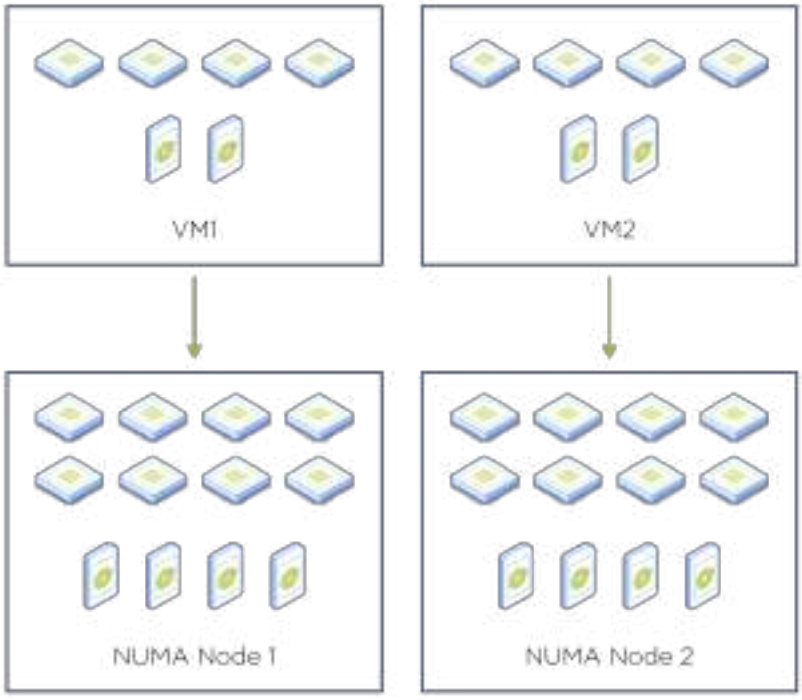


Figure 44: Example of a Single NUMA Node

Virtual Non Uniform Memory Access (vNUMA) and User VMs

The primary purpose of vNUMA is to give large virtual machines or wide VMs (VMs requiring more CPU or memory capacity than is available on a single NUMA node) the best possible performance. vNUMA helps wide VMs create multiple vNUMA nodes.

Nutanix supports vNUMA with both AHV and ESXi. vNUMA requires NUMA aware applications.

Each vNUMA node has virtual CPUs and virtual RAM. Pinning a vNUMA node to a physical NUMA node ensures that virtual CPUs accessing virtual memory see the expected NUMA behavior. Low-latency memory access in virtual hardware (within vNUMA) matches low-latency access in physical hardware (within physical NUMA), and high-latency accesses in virtual hardware (across vNUMA

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1082

boundaries) match high-latency accesses on physical hardware (across physical NUMA boundaries).

In AHV, administrators can configure vNUMA for a VM via the aCLI (Acropolis CLI) or REST API; this configuration is VM-specific and defines the number of vNUMA nodes. Memory and compute are divided in equal parts across each vNUMA node. Refer to AHV admin guide for steps on how to do it.

In ESXi, vNUMA is automatically enabled for a VM with >8 vCPU.

Building on the previous example, if a host with 16 CPU cores and 256GB memory has a VM with 12vCPUs and 192GB memory that is not vNUMA configured, the vCPU and memory assignment will span NUMA boundaries.

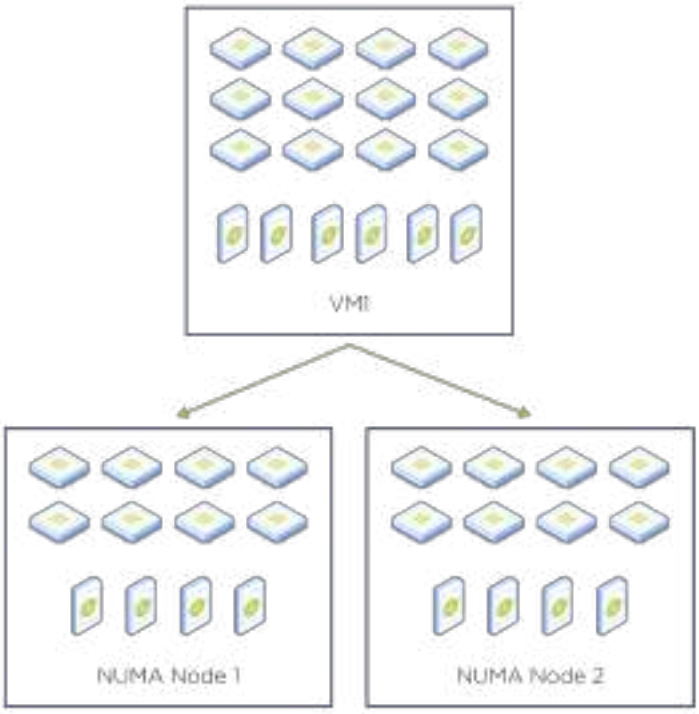


Figure 45: vCPU and Memory Assignment Spanning NUMA Boundaries

To ensure the best performance for wide VMs like this, vNUMA must be configured.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1083

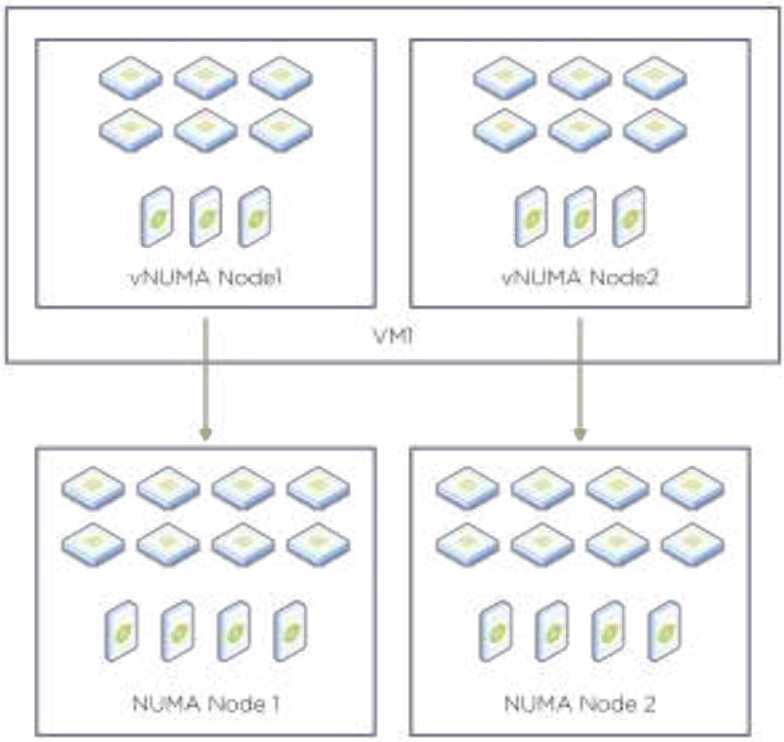


Figure 46: Best Performance vNUMA Configuration for Wide VMs

vNUMA VM configurations require strict fit. With strict fit, for each VM virtual node, memory must fit inside a physical NUMA node. Each physical NUMA node can provide memory for any number of vNUMA nodes. If there is not enough memory within a NUMA node, the VM does not power on. Strict fit is not required for CPU. To determine how many vNUMA nodes to use for a user VM, follow application-specific configuration recommendations provided by Nutanix.

CVM CPU and Memory Considerations

Optimal CVM vCPU values depend on the type of system and how many cores per NUMA node are present in the system. The CVM is pinned to the first physical CPU of the node. The following table gives an overview of minimum vCPU and memory values for the CVM (as of AOS 5.15):

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1084

Table 59: Minimum CPU and Memory Values as of AOS 5.15

Platform Storage or Type	Minimum Memory (GB)	Minimum vCPU
Platforms up to 80TB per node	32	8
Platforms up to 120TB per node	36	12
Platforms up to 120TB per node deploying Nutanix Objects	36	12

For specific recommendations on CVM sizing relating to specific workloads (e.g. Microsoft, Oracle, etc) please refer to Nutanix Solution Briefs and Best Practice Guides for those workloads.

Recommendations

Use Nutanix Foundation to set up a new cluster or node and configure the CVM(s). Nutanix Foundation software automatically identifies the platform and model type. Based on that information, Nutanix Foundation configures the appropriate default values for CVM memory and vCPU.

Storage Design

Nutanix HCI combines highly dense storage and compute into a single platform with a scale-out, shared-nothing architecture and no single points of failure. The AOS Distributed Storage Fabric (DSF) appears to the hypervisor like any centralized storage array, however all of the I/Os are handled locally to provide the highest performance.

Storage planning for this document, requires that you understand some of the high-level concepts for DSF:

Storage Pool

A group of physical storage devices within the cluster. This can include HDDs and both NAND and NVMe SSDs. The storage pool spans multiple Nutanix nodes and expands as the cluster expands. A default storage pool is created when a cluster is created.

Container

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1085

Logical segmentation of the Storage Pool is provided by containers, which contain a group of VMs or files (vDisks). Configuration options and data management services are configured at the container level. When a cluster is created, a default storage container is configured for the cluster.

Note: When VMware ESXi is used, containers correspond to NFS datastores.

Container Guidelines:

A key design question is how many containers to configure in a cluster:

- Nutanix typically recommends minimizing the number of containers created. For most use cases only 1 container is enough.
- Exceptions can be made if two or more applications running on the same cluster require different data reduction and replication factor values. In this case, additional containers can be created for those workloads.

Data reduction, including compression, dedupe, erasure coding and replication factor (RF) values, is configured on a container basis and multiple containers need to be created when different values are desired.

All Nutanix containers are thin provisioned by default. Thin provisioning is a widely accepted technology that has been proven over time by multiple storage vendors, including VMware. As the DSF presents containers to VMware vSphere hosts as NFS datastores by default, all VMs are also thin provisioned by default. vDisks created within AHV VMs are thinly provisioned by default. Nutanix also supports thick provisioned vDisks for VMs in ESXi by using space reservations. Using thick provisioned vDisks might impact data reduction values on containers since Nutanix reserves the thick provisioned space and it cannot be oversubscribed.

Table 60: Creating vDisks in ESXi

STR-01	WHEN CREATING VDISKS IN ESXI, ALWAYS USE THIN-PROVISIONED VDISKS.
Justification	There is no performance difference between thin-provisioned and thick-provisioned disks. Thin provisioning is more space efficient.
Implication	All Nutanix data reduction technologies can be used on the vDisk.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1086

Note: Multi-writer VMDK requires thick provisioned vDisks.

vDisk

All storage management is VM-centric, and I/O is optimized at the vDisk level.

The software solution runs on nodes from a variety of manufacturers. A vDisk is any file over 512KB stored in DSF, including vmdks and VM hard disks. vDisks are logically composed of vBlocks.

Recommendations

Use multiple vDisks for an application versus a single large vDisk.

Using multiple vDisks allows for better overall performance due to the ability to leverage multiple OS threads to do more parallel processing versus a single vDisk configuration. Refer to the appropriate application solution guide for application-specific configuration recommendations for how many vDisks to configure.

Nutanix Volumes

In addition to providing storage through the hypervisor, Nutanix also allows supported operating systems, to access DSF storage capabilities directly using Nutanix Volumes. Nutanix designed Volumes as a scale-out storage solution where every CVM in a cluster can present storage volumes via iSCSI. This solution allows an individual application to access the entire cluster, if needed, to scale out for performance.

Volumes automatically manages high availability to ensure upgrades or failures are non- disruptive to applications. Storage allocation and assignment for Volumes is done with volume groups (VGs). A VG is a collection of one or more disks (vDisks) in a Nutanix storage container. These Volumes disks inherit the properties (replication factor, compression, erasure coding, and so on) of the container they reside in. With Volumes, vdisks in a VG are load balanced across all CVMs in the cluster by default.

In addition to connecting volume groups through iSCSI, AHV also supports direct attachment of VGs to VMs.In this, the vdisks are presented to guest OS over the virtual SCSI controller. The virtual SCSI controller leverages AHV Turbo and iSCSI under the covers to connect to the Nutanix DSF. By default, the vdisks

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1087

in a VG directly attached to a VM are hosted by the local CVM. Load balancing of vdisks on direct attached VGs can be enabled via acli.

Load balancing of vDisks in a VG enables I/O-intensive VMs to use the storage capabilities of multiple CVMs. If load balancing is enabled on a VG, AHV communicates directly with each CVM hosting a vDisk.

Each vDisk is served by a single CVM. Therefore, to use the storage capabilities of multiple CVMs, create more than one vDisk for a file system and use OS-level striped volumes to spread the workload. This improves performance and prevents storage bottlenecks, but can impact your network bandwidth.

Guideline: Core use-cases for Nutanix Volumes:

- Shared Disks
  - Oracle RAC, Microsoft Failover Clustering, etc.
- Where execution contexts are ephemeral, and data is critical
  - Containers, OpenStack, etc.
  - Guest-initiated iSCSI which is required for MS Exchange on vSphere (for Microsoft support).
- Bare-metal consumers
  - Stand alone or clustered physical workload.

Hybrid and All-Flash Nodes

A Nutanix cluster can consist of hybrid nodes, all-flash nodes, or a combination. Irrespective of the node type, each node has an OpLog that serves as a persistent write buffer for bursty, random write traffic. The OpLog is similar to a filesystem journal.

An extent store provides persistent bulk storage for DSF. A hybrid node has a combination of SSDs and HDDs with OpLog stored on the SSDs. All-Flash nodes are composed of SSDs. If there is a combination of SATA and NVMe SSDs, OpLog is stored on the fastest medium.

DSF automatically tiers data across the cluster to different classes of storage devices using intelligent lifecycle management (ILM). For best performance, ILM makes sure the most frequently used data is available in memory or in flash on

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1088

the node local to the VM. The default threshold where the algorithm will move data from the hot tier to the cold tier is 75%. Data for down-migration is chosen based on last access time. In All-Flash node configurations, the Extent Store consists only of SSDs and no tiering occurs.

Recommendations:

For hybrid configurations, Nutanix recommends:

- Sizing the SSD tier so that the active data set of application fits in 75% of usable SSD capacity.
- Nutanix has a collector tool that can be run to determine the approximate active data set size.
- Alternatively, use application-specific tools such as: MAP toolkit for MSSQL; AWR reports and Nutanix scripts for Oracle.
- A general rule is to check how much data has been backed up during a month. Assuming a 70%/30% R/W pattern (if the R/W patterns are unknown), multiply the data you get from backups by 4, which would give an approximate value for hot data. That amount should fit within 75% of the usable cluster capacity.

For All-Flash configurations there is no ILM, so there is no equivalent recommendation.

Table 61: SSD Capacity Considerations When Sizing a Cluster

STR-02	WHEN SIZING A HYBRID CLUSTER, MAKE SURE TO HAVE ENOUGH USABLE SSD CAPACITY TO CONTAIN THE ACTIVE DATA SET OF RUNNING APPLICATIONS.
Justification	Keeping active data on SSD ensures the application achieves the best performance. ILM moves data between tiers. The best-case scenario is active data in the SSD tier all the time.
Implication	More SSD capacity may need to be sized to keep active data on the SSD tier.

Recommendations

For hybrid configurations, Nutanix recommends:

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1089

- Use All-Flash node configurations for business-critical applications for consistent performance. As mentioned before,
- All-Flash configurations can consist of all SATA SSDs or a combination of SATA and NVMe.
- If the application requires very high IOPS with consistent low latency, there is an option to use RDMA with NVMe. RDMA requires RoCEv2 to be configured on the network fabric; Nutanix makes this setup very easy through Prism.

Table 62: Mixing Nodes from Different Vendors in the Same Cluster

STR-03	DO NOT MIX NODE TYPES FROM DIFFERENT VENDORS IN THE SAME CLUSTER.
Justification	Mixing node types from different vendors is unsupported.
Implication	Nodes from different vendors can be setup in separate clusters and all managed centrally from Prism Central.

Table 63: Mixing NVMe and Hybrid SSD/HDD Nodes in the Same Cluster

STR-04	DO NOT MIX NODES THAT CONTAIN NVME SSDS IN THE SAME CLUSTER WITH HYBRID SSD/HDD NODES.
Justification	The performance of NVMe SSD nodes is significantly higher compared to hybrid nodes and mixing them can potentially create performance issues.
Implication	NVMe Nodes can be setup in their own clusters or added to clusters with All SSD nodes and managed centrally from Prism Central.

Node Selection Recommendations

- If your high-level design decision is to use hybrid nodes, you need to decide the number of HDDs and SSDs per node.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1090

- For applications that require high performance like DBs and Tier-1 applications, more drives per node is better.
  - › OpLog will be spread across up to 8 SSDs, so more SSDs results in overall better and more consistent performance. If NVMe devices are present, OpLog is placed on them upto 8 NVMe SSDs.
  - › More SSDs provides more usable space for tiering data.
- For All-Flash nodes, more SSDs provide better performance by making read and write access more parallel, especially for non-optimal workload patterns.
- Use Nutanix Sizer to size usable capacity and obtain node recommendations based on your workload use case.
- Also refer to specific application solution guides and/or best practice guides.

Table 64: HDD to SSD Ratio

STR-05	A MINIMUM 2:1 HDD TO SSD RATIO IS REQUIRED FOR HYBRID CLUSTERS.
Justification	This ensures there is enough bandwidth in the slower storage tier to absorb down migrations triggered by ILM.
Implication	If this rule is not followed, it may result in performance degradation during down migrations.

Note: 4 drive slot and 10 drive slot systems from Dell, Lenovo, and Fujitsu can have 2+2 and 4+6 SSD+HDD configurations respectively.

Table 65: Sizing for Redundancy

STR-06	SIZE FOR N+1 NODE REDUNDANCY FOR STORAGE AND COMPUTE WHEN SIZING. FOR MISSION CRITICAL WORKLOADS THAT NEED HIGHER SLAS, USE N+2 NODE REDUNDANCY.
Justification	Having the storage and compute capacity of an additional node (or two) ensures there is enough storage and compute capacity available for VMs to re-start when a node failure occurs.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1091

Implication	Additional storage and compute capacity is required for N+1 or N+2 redundancy.

Availability Domains and Fault Tolerance

Availability domains are used to determine component and data placement. Nutanix availability domains are:

- Disk Awareness (always).
- Node Awareness (always).
- Block Awareness (optional).Requires a minimum of 3 blocks for FT1 and 5 for FT2, where a block contains either 1,2 or 4 nodes. With Erasure Coding, minimums are 4 blocks for FT1 and 6 blocks for FT2.
- Rack Awareness(optional).Requires a minimum of 3 racks for FT1 and 5 for FT2, and you must define what constitutes a rack and where your blocks are placed. With Erasure Coding, minimums are 4 racks for FT1 and 6 blocks for FT2.

Closely tied to the concepts of awareness and RF is cluster resilience, defined by the redundancy factor or Fault Tolerance (FT). FT is measured for different entities, including:

- Data
- Metadata
- Configuration data
- Free space

FT=1: A cluster can lose any one component and operate normally. FT=2: A cluster can lose any two components and operate normally.

Depending on the defined awareness level and FT value, data and metadata are replicated to appropriate locations within a cluster to maintain availability.

The following table gives an overview of Data awareness and FT levels supported.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1092

Table 66: Data Awareness and Fault Tolerance Levels Supported

DESIRED AWARENESS TYPE	FT LEVEL	MIN. UNITS*	SIMULTANEOUS FAILURE TOLERANCE
Node	1	3 nodes	1 node
Node	2	5 nodes	2 nodes
Block	1	3 blocks	1 block
Block	2	5 blocks	2 blocks
Rack	1	3 racks	1 rack
Rack	2	4 racks	2 rack

*The minimum units increase by 1 if EC-X is enabled.

FT Guidelines

- FT=2 implies RF=3 for data and RF=5 for metadata by default.
  - Use this setting when you need to withstand two simultaneous failures and have cluster and VM data still be available.
- FT=1 implies RF=2 for data and RF=3 for metadata by default.
  - Use this setting when the application is fine with having only 2 copies of data. This will keep the cluster and VM data available after one failure.
- Another option is to set FT=2 for a cluster with specific containers set to RF=2.
  - With this configuration, data is RF=2, but metadata is RF=5.
  - For containers that are RF=2, if there are 2 simultaneous failures there is a possibility that VM data becomes unavailable, but the cluster remains up.
  - This is different than the FT=1, RF=2 case where two simultaneous failures will result in a cluster being down.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1093

Table 67: Fault Tolerance for Workloads/Clusters with Higher SLAs

STR-07	USE FT=2 AND RF=3 FOR WORKLOADS AND CLUSTERS THAT NEED HIGHER SLAS OR FOR CLUSTER SIZES >32.
Justification	Using FT=2 and RF=3 provides additional resilience and capability to survive 2 simultaneous failures.
Implication	Additional storage space is required for FT=2 and RF=3, reducing usable capacity.

Capacity Optimization

Nutanix provides different ways to optimize storage capacity that are intelligent and adaptive to workloads characteristics. All optimizations are performed at the container level, so different containers can use different settings.

Erasure Coding (EC-X)

To provide a balance between availability and the amount of storage required, DSF provides the ability to encode data using erasure codes (EC). Like RAID (levels 4, 5, 6, etc.) where parity is calculated, EC encodes a strip of data blocks across different nodes and calculates parity. In the event of a host and/or disk failure, the parity data is used to calculate any missing data blocks (decoding). In the case of DSF, the data block must be on a different node and belong to a different vDisk. EC is a post-process operation and is done on write cold data (Data that hasn't been overwritten in more than 7 days). The number of data and parity blocks in a strip is chosen by the system based on number of nodes and configured failures to tolerate.

The following table summarizes the expected overhead for EC-X vs standard RF2/RF3 overhead:

Table 68: Expected Overhead for EC-X vs Standard RF2/RF3

	FT1 (RF2 Equivalent)		FT2 (RF3 Equivalent) 3X Storage Overhead
# of nodes	EC strip size	3 nodes	1 node
(data/parity)	EC overhead	EC strip size	2 nodes

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1094

(data/parity)	EC overhead	3 blocks	1 block	
4	2/1	1.5X	N/A	N/A
5	3/1	1.33X	N/A	N/A
6	4/1	1.25X	2/2	2X
7	4/1	1.25X	3/2	1.6X
8+	4/1	1.25X	4/2	1.5X

EC-X Guidelines

EC-X provides the same level of data protection while increasing usable storage capacity.

- Turn on EC-X for non-mission-critical workloads and workloads that have a significant amount of write cold data, since erasure coding works on write cold data and provides more usable storage.
- For more information refer to specific application guides.

Compression

DSF provides both inline and post-process data compression. Irrespective of inline or post-process compression, write data coming into oplog that is >4k and shows good compression, will be written compressed in OpLog.

- Inline: Compresses sequential streams of data or large size I/Os (>64K) when writing to the Extent Store.
- Post-Process: Compresses data after it is drained from OpLog to the Extent Store after compression delay is met during the next curator scan.

Nutanix uses the LZ4 and LZ4HC compression algorithms. LZ4 compression is used to compress normal data, providing a balance between compression ratio and performance. LZ4HC compression is used to compress cold data to improve the compression ratio. Cold data is characterized as:

- Regular data: No access for 3 days.
- Immutable data: No access for 1 day.

Compression Guidelines

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1095

Compression provides on-disk space savings for applications such as databases, and results in a lower number of writes being written to storage. Turn ON inline compression for all containers.

Table 69: Enabling Inline Compression for All Containers

STR-08	ENABLE INLINE COMPRESSION FOR ALL CONTAINERS.
Justification	Since inline compression operates only on sequential data when writing to extent store, enabling it provides immediate space efficiency. Write data coming into oplog is already compressed.
Implication	Slightly higher CPU consumption for compressing/decompressing data.

Deduplication

When enabled, DSF does capacity-tier and performance-tier deduplication. Data is fingerprinted on ingest using a SHA-1 hash that is stored as metadata. When duplicate data is detected based on multiple copies with the same fingerprint, a background process removes the duplicates. When deduplicated data is read, it is placed in a unified cache, and any subsequent requests for data with the same fingerprint are satisfied directly from cache.

Deduplication Guidelines

Deduplication is recommended to be used for full clones, P2V migrations and persistent desktops.

Table 70: Enabling/Disabling Deduplication

STR-09	ENABLE/DISABLE DEDUPLICATION
Justification	Increases effective capacity of caching layer for dedup-able data like VDI clones.
Implication	Slightly higher CPU consumption for running deduplication processes.

Refer to specific application Solution Guides for determining whether to enable deduplication or not.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1096

Virtualization Layer Design

This section describes technical design considerations for design using either Nutanix AHV or VMware ESXi.

Nutanix AHV

Introduction

The Nutanix hypervisor, AHV, is an attractive alternative hypervisor that streamlines operations and lowers overall costs. Built-in to Nutanix Enterprise Cloud and included at no additional cost in the AOS license, AHV delivers virtualization capabilities for the most demanding workloads. It provides an open platform for server virtualization, network virtualization, security, and application mobility. When combined with comprehensive operational insights and virtualization management from Nutanix Prism and Prism Central, AHV provides a complete datacenter solution.

Control Plane

The control plane for managing the Nutanix core infrastructure and AHV are provided by:

- Prism Element (PE)
  - Localized cluster manager responsible for local cluster management and operations. Every Nutanix Cluster includes Prism Element built-in.
  - 1-to-1 cluster manager
- Prism Central
  - Multi-cluster manager responsible for managing multiple Nutanix clusters to provide a single, centralized management interface. Prism Central is an optional software appliance (VM).
  - 1-to-many cluster manager
  - A dedicated PC is required at the source and target sites for any regions or availability zones using DR runbook automation for failing over workloads.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1097

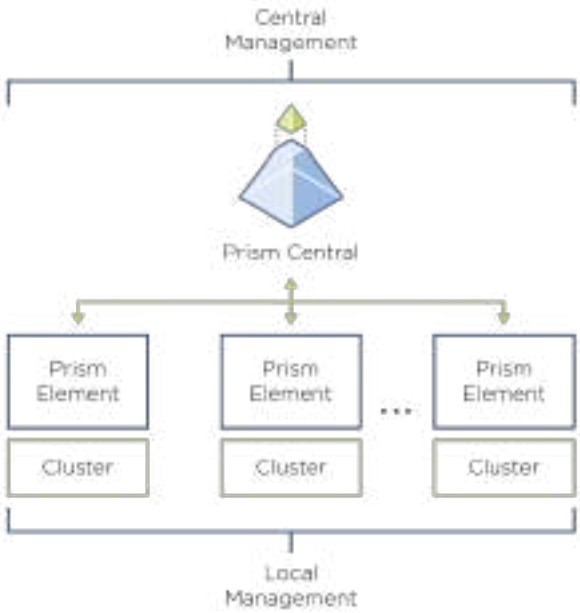


Figure 47: The Nutanix Control Plane

Table 71: Deploying Prism Central for Enhanced Cluster Management

VRT-001	DEPLOY SCALE-OUT PRISM CENTRAL FOR ENHANCED CLUSTER MANAGEMENT.
Justification	Increases the total number of managed objects, increases management plane availability.
Implication	Requires some additional cluster resources to run the necessary VMs.

Table 72: Deploy Prism Central in Each Region or Az Using Runbook Dr Automation.

VRT-002	DEPLOY PRISM CENTRAL IN EACH REGION OR AZ USING RUNBOOK DR AUTOMATION.
Justification	Required for DR runbook automation feature that the source and target sites have separate PC instances controlling them.
Implication	Requires some additional cluster resources to run the necessary VMs.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1098

HA/ADS

Nutanix AHV has built-in VM high availability (VM-HA) and a resource contention avoidance engine called Acropolis Dynamic Scheduling (ADS). ADS is always on and does not require any manual tuning. VM-HA can be enabled and disabled via a simple Prism checkbox. There are two main levels of VM-HA for AHV:

- Best effort. In this HA configuration, no node or memory reservations are required in the cluster. In case of a failure, VMs are moved to other nodes based on the resources/ memory available on each node. This is not a preferred method of HA, since if no resources are available in the cluster after a failure some VMs may not be powered-on. Best effort is the default configuration. Most applicable to non-production environments.
- Guarantee. In this HA configuration, some memory is reserved on each node in the cluster to enable failover of virtual machines from a failed node. The Acropolis service in the cluster calculates the memory to be reserved based on virtual machine memory configuration. All nodes are marked as schedulable with resources available for running VMs. Recommended for production environments. Enable this mode by checking the Enable HA Reservation box in Prism settings.

VM-HA considers memory when calculating available resources throughout the cluster for starting VMs. VM-HA respects Acropolis Distributed Scheduler (ADS) VM-host affinity rules, but it may not honor VM-VM anti-affinity rules, depending on the scenario.

Table 73: Using VM-HA Guarantee

VRT-003	USE VM-HA GUARANTEE
Justification	Ensuring VM high availability is important in production environments. Guarantee should be used in production environments. “Best effort” (default) is optimal in test/ dev environments.
Implication	Reserves enough cluster resources such that an entire host’s worth of VMs can be successfully restarted (RF=2), or two hosts (RF=3). RF=3 must be manually configured, since it is not the default.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1099

For additional information, see: Virtual Machine High Availability.

AHV CPU Generation Compatibility

Similar to VMware's Enhanced vMotion Capability (EVC) which allows VMs to move between different processor generations, AHV will determine the lowest processor generation in the cluster and constrain all QEMU domains to that level. This allows mixing of processor generations within an AHV cluster and ensures the ability to live migrate between hosts.

VMware vSphere

Introduction

VMware vSphere is fully supported by Nutanix with many points of integration. vSphere major and minor releases go through extensive integration and performance testing, ensuring that both products work well together in even the largest enterprises. Rest assured that if you deploy vSphere, the solution is fully supported.

Control Plane

When using vSphere as a part of this document, the control plane is vCenter to manage the vSphere components and Prism Central for managing Nutanix components.

Table 74: Managing ESXi-based Nutanix Clusters

VRT-004	DEPLOY AN HA VCENTER INSTANCE WITH EMBEDDED PSC TO MANAGE ESXI-BASED NUTANIX CLUSTERS.
Justification	Nutanix upgrade automation features, such as 1-click upgrades and LCM, require the advanced control features that vCenter provides. In addition, vCenter Server is required to create and manage the VMware vSphere cluster responsible for DRS and HA.
Implication	Requires additional vCenter licenses and added installation time to fully configure each vCenter instance.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1100

Table 75: Deploy a vCenter in Region or Az Using Runbook Dr Automation

VRT-005	DEPLOY A vCENTER IN EACH REGION OR AZ USING RUNBOOK DR AUTOMATION.
Justification	Required for DR runbook automation feature that the source and target sites have separate PC and local vCenter instances controlling them.
Implication	Requires some additional cluster resources to run the necessary VMs.

EVC

VMware's Enhanced vMotion Capability (EVC) allows VMs to move between different processor generations within a cluster. EVC mode is a manually configured option, unlike the corresponding feature in AHV. EVC should be enabled at cluster installation time to negate the possible requirement to reboot VMs in the future when it is enabled.

Table 76: Enabling EVC Mode

VRT-006	ENABLE EVC MODE AND SET IT TO THE HIGHEST COMPATIBILITY LEVEL THE PROCESSORS IN THE CLUSTER WILL SUPPORT.
Justification	Even if a cluster is homogenous at the outset, it is likely new nodes will be added over time. Enabling EVC mode when a cluster is built helps ensure future node additions are seamless.
Implication	Requires manual configuration to determine the highest compatible EVC mode.

HA/DRS

VMware HA and DRS are core features which should be utilized as a part of this document. Nutanix best practices dictate that a few HA/DRS configuration settings be changed from the default. These changes are outlined in the design decisions below.

Table 77: Enabling HA

VRT-007	ENABLE HA

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1101

Justification	In production environments VM availability is extremely important. Automatically restarting VMs in case of node failure helps ensure workload availability.
Implication	Requires additional cluster resources to ensure VMs on the failed node(s) can be restarted elsewhere in the cluster.

Table 78: Enabling DRS

VRT-008	ENABLE DRS WITH DEFAULT AUTOMATION LEVEL
Justification	Hot spots can develop in a cluster. DRS moves VMs as needed to ensure optimal performance.
Implication	Initiates vMotion for optimal VM performance in case of resource contention. Moving VMs may temporarily impact Nutanix data locality.

Table 79: Disabling VM PDL and APD Component Protection

VRT-009	DISABLE VM PDL AND APD COMPONENT PROTECTION
Justification	These settings are designed for non-Nutanix storage. They should not be enabled in Nutanix clusters because they can cause storage unavailability. APD monitoring is managed via a Nutanix component.
Implication	Permanent device loss (PDL) and all paths down (APD) monitoring is disabled, and vSphere will not monitor for these conditions.

Table 80: Configuring DAS.IGNOREINSUFFICIENTHBDATASTORE

VRT-010	CONFIGURE DAS.IGNOREINSUFFICIENTHBDATASTORE IF ONE NUTANIX CONTAINER IS PRESENTED TO THE ESXI HOSTS
Justification	In many Nutanix clusters a single datastore is used. The warning message is not applicable in Nutanix environments.
Implication	Eliminates false positive warnings when a cluster uses a single datastore.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1102

Table 81: Disabling Automation Level for All CVMs

VRT-011	DISABLE AUTOMATION LEVEL FOR ALL CVMS
Justification	CVMs are stored on local storage and cannot be vMotioned to another host. HA does not need to reserve resources for CVMs since they are bound to a single node and cannot be restarted elsewhere in the cluster.
Implication	DRS will not try and move a CVM to another host. Nor will CVM resources be taken into account for HA calculations.

Table 82: Setting Amount of Reserved Resources in the Cluster

VRT-012	SET HOST FAILURES CLUSTERS TOLERATE TO 1 FOR RF2 AND TO 2 FOR RF3.
Justification	Starting in vSphere 6.5, cluster resource percentage is now tied to "host failures cluster tolerates" and automatically adjusts the percentage based on the number of nodes in the cluster.
Implication	Automatically sets the proper amount of reserved resources in the cluster.

Table 83: Setting Host Isolation Response for VMs

VRT-013	SET HOST ISOLATION RESPONSE TO "POWER OFF AND RESTART VMS"
Justification	In an HCI environment all communications, including storage, are via the ethernet network. If a host becomes isolated on the network, VMs need to be moved to a healthy host to continue to function.
Implication	If a host becomes isolated on the network, the VMs on that host will be powered off and restarted on another node in the cluster.

Table 84: Setting Host Isolation Response for the CVM

VRT-014	SET HOST ISOLATION RESPONSE TO "LEAVE POWERED ON" FOR CVMS

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1103

Justification	If there is a transient network disruption, you do not want the CVMs to be powered off.
Implication	If a host becomes isolated on the network, the CVMs will remain on.

Table 85: Disabling HA/DRS for Each Nutanix CVM

VRT-015	DISABLE HA/DRS FOR EACH NUTANIX CVM
Justification	CVM uses local storage and no attempt to restart on other hosts should be performed.
Implication	vSphere will not try and restart the CVM on another host, which is impossible since the CVM uses local storage.

Table 86: Disabling SIOC

VRT-016	DISABLE SIOC
Justification	If SIOC is enabled, it can have negative side effects. These include storage unavailability, creating unnecessary lock files, and complications with Metro Availability.
Implication	Enhanced storage statistics are not available.

Management Layer Design

Control Plane

This document provides a primary control plane where the majority of daily operational tasks are performed. In this design:

- The primary control plane is Prism Central.
- VMware vCenter is also required if you are using VMware ESXi.

Each of these has a maximum size that limits the total number of VMs, nodes, and clusters that can be managed by an instance.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1104

Prism Central

Prism Central (PC) is a global control plane for Nutanix, which includes managing VMs, replication, monitoring, and value-add products such as:

- Nutanix Calm for application-level orchestration
- Flow Network Security for microsegmentation of east-west traffic
- Prism Pro for advanced task automation and capacity planning

These products are installed from Prism Central and managed centrally for all Prism Element clusters associated to the Prism Central instance.

Prism Central plays an important part in a deployment regardless of the scale. There are two deployment architectures for Prism Central that can be utilized and scaled depending on the size and goals of the design.

Single-VM Prism Central Deployment

The single VM deployment option for Prism Central offers a reduced footprint option for designs that do not require high availability for the control plane beyond that provided by the hypervisor. The single Prism Central VM option can be used with a small or large VM sizing. The size directly correlates to the size of environment it can manage.

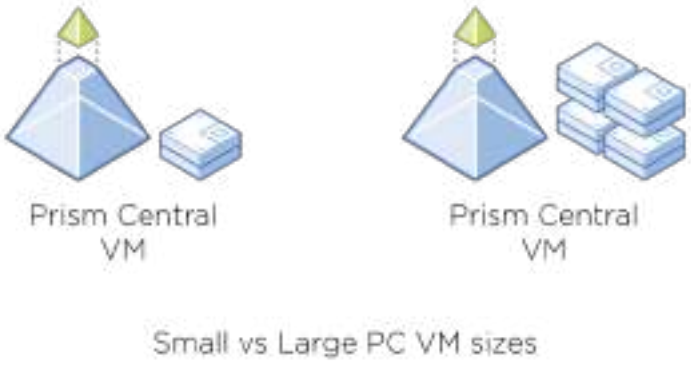


Figure 48: Small vs Large Prism Central VM Sizes

Scale-Out Prism Central Deployment

A scale out PC cluster is comprised of three VMs. All of the members of the cluster are running all of the Nutanix services and products in a distributed architecture.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1105

This distributed architecture allows for the scaled-out Prism Central to manage a larger environment as well as handle more incoming requests from users and the API.

Additionally, it provides a higher level of availability. If one of the VMs is down or performing a maintenance operation, the other members remain available. You have the option of deploying the PC VMs as small- or large-sized VMs.

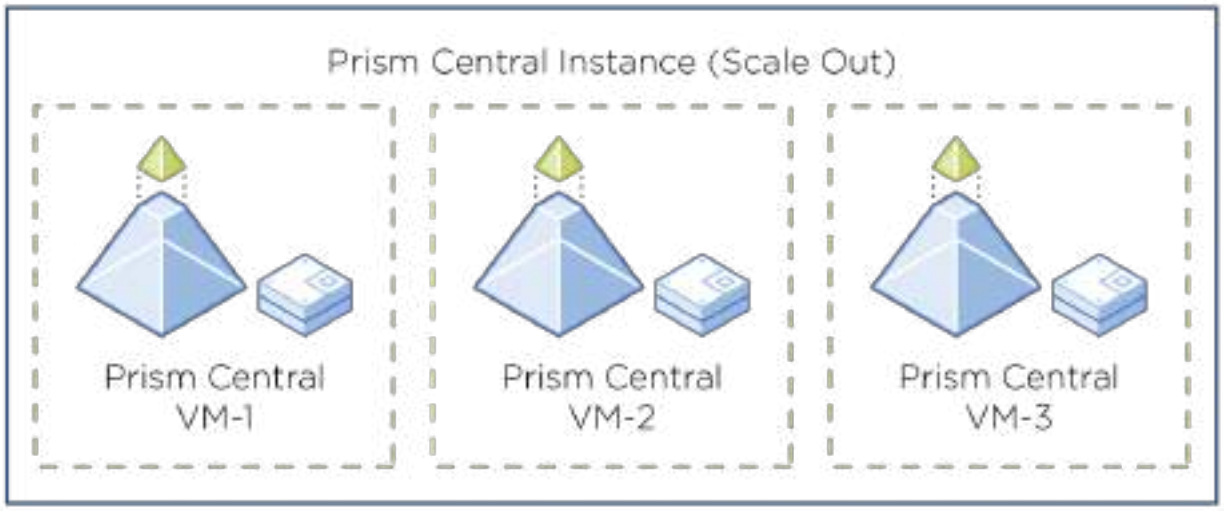


Figure 49: Scale Out Prism Central Deployment

The scale-out Prism Central architecture deploys 3 VMs on the same cluster and is superior in terms of availability and capacity. If scale-out is not the best option from the beginning, it is fairly simple to go from a single PC VM deployment to a scale-out architecture at a later time.

Image Templates

Within any environment operating at scale there is a need to keep approved template images available and in sync between clusters. For AHV clusters, image placement policies should be utilized for this. Image policies are configured to determine the clusters each image can or cannot be utilized in. This makes the initial roll out of new and updated image versions easy.

For ROBO deployments utilizing AHV, image placement policies should be configured to avoid unnecessary data being replicated between locations with limited bandwidth.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1106

Prism Central Recommendations

Table 87: Prism Central Recommendations

Recommendation Area	Description
Prism Central instances	Deploy Prism Central in the following way: • Scale out mode (cluster of 3 VMs). The benefits: • Simplifies capacity planning. • Simplifies platform life cycle management. • Simplifies management for virtual networking. • Reduce management overhead.
Workload Domains	Deploy management workloads such as Prism Central on management clusters.
Access Control	• Integrate with Active Directory. • Leverage AD groups to optimize access management.

VMware vCenter Server

For designs utilizing ESXi as the hypervisor, vCenter is a critical part of the infrastructure for hypervisor cluster management and VM operations. It may be accessed often in environments that are not highly automated. In automated environments, vCenter is needed to perform operations that are sent to it from different orchestration layers.

The vCenter appliance can be deployed in many different sizes. This ultimately determines how large an environment you can support in terms of VMs, hosts, and clusters. Refer to the official VMware documentation for the version you are deploying to determine the proper sizing for your design.

Beyond the size of the environment, the vCenter appliance can be deployed as a single VM or as a vCenter High Availability (vCenter HA) for additional

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1107

availability. The option to deploy vCenter HA does not increase the size of the environment it can manage as a single virtual appliance is active at any time. The size of the environment that can be managed is based on the size of the VMs deployed.

Figure 50: vCenter Appliances

To ensure that the control plane is as highly available as possible, the clustered deployment option is preferred as long as its compatible with other layers of the solution.

vCenter Server Recommendations

Table 88: vCenter Server Recommendations

RECOMMENDATION AREA	DESCRIPTION
vCenter instances	Deploy one vCenter in an HA configuration for all workloads.Configure with Embedded PSC.
Workload domains	Deploy management workloads on management clusters.
Access Control	• Integrate with Active Directory. • Leverage AD groups to optimize access management.

Dependent Infrastructure

There are a variety of other infrastructure services that are necessary for a successful Nutanix deployment, such as NTP, DNS, and AD. You may already

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1108

have these infrastructure services deployed and available for use when you deploy your Nutanix environment. If they do not exist, then you will probably need to deploy them as part of the new environment

NTP

Network Time Protocol (NTP) is used to synchronize computer clock times including network, storage, compute, and software. If clock times drift too far apart, some products may have trouble communicating across layers of the solution. Keeping time in-sync is beneficial when examining logs from different layers of the solution to determine the root cause of an event.

A minimum of three NTP servers should be configured and accessible to all solution layers with the NTP standard recommendation being five to detect a rogue time source. These include AOS, AHV, and Prism Central, plus vCenter and ESXi if using VMware vSphere as the virtualization layer. Use the same NTP servers for all infrastructure components.

Do not use an Active Directory Domain Controller as an NTP source.

If you are in a Dark site with no internet connectivity, consider using a switch or GPS time source.

Table 89: NTP Servers for Infrastructure Components

DEP-001	A MINIMUM OF THREE NTP SERVERS FOR ALL INFRASTRUCTURE COMPONENTS SHOULD BE PROVIDED.
Justification	Unreliable time services can lead to authentication failures, mis-aligned log entries, and other critical errors.
Implication	Provides reliable time services for all system components.

DNS

Domain Name System (DNS) is a directory service that translates domain names of the form domainname.ext to IP addresses. DNS is important to ensure that all layers can resolve names and communicate. A highly available DNS environment should be utilized to support this design. At least two DNS servers

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1109

should be configured and accessible at all layers to ensure components can reliably resolve addresses at all times.

These layers include the following:

- AOS
- AHV
- Prism Central
- VMware ESXi
- VMware vCenter
- Network switches

Table 90: DNS Servers for Infrastructure Layers

DEP-002	A MINIMUM OF TWO DNS SERVERS SHOULD BE CONFIGURED ACCESSIBLE TO ALL INFRASTRUCTURE LAYERS
Justification	DNS is critical for a number of services and infrastructure failures will occur if DNS is unavailable.
Implication	The organization needs to deploy at least two DNS servers and point all services to them.

Active Directory

Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. AD often serves as the authoritative directory for all applications and infrastructure within an organization. For this design, all of the consoles and element managers will utilize RBAC and use AD as the directory service for user and group accounts. Where possible, AD groups should be utilized to assign privileges for easier operations. User access can then be controlled by adding or removing a user from the appropriate group.

The AD design should be highly available to ensure that directory servers are always available when authentication requests occur.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1110

Logging Infrastructure

Capturing logs at all layers of the infrastructure is very important. For example, if there is a security incident, logs can be critical for forensics. An example of a robust log collector is Splunk, but there are other options. Nutanix recommends that you deploy a robust logging platform that meets your security requirements. All infrastructure logs should be forwarded to the centralized log repository.

Recommendation

It is commonly recommended to store the logs in a different cluster, or location, from where they are being collected. This protects the logs in case of a catastrophic cluster failure, ensuring they can later be used for forensics.

Security Layer Design

Nutanix Enterprise Cloud can be used to build private or multi-tenant solutions, and depending on the use case the security responsibility will vary. The security approach includes multiple components:

- Physical
  - Datacenter access
  - Equipment access (firewalls, load balancers, nodes, network switches, racks, routers)
- Virtual Infrastructure
  - Clusters
  - Nodes
  - Management components
  - Network switches
  - Firewalls
  - Load balancers

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1111

- Threat vectors
  - Active
  - Automated
  - Internal
  - External
- Workloads
  - Applications
  - Containers
  - Virtual Machines

Nutanix Enterprise Cloud infrastructure is designed to deliver a high level of security with less effort. Nutanix publishes custom security baseline documents for compliance, based on United States Department of Defense (DoD) RHEL 7 Security Technical Implementation Guides (STIGs) that cover the entire infrastructure stack and prescribe steps to secure deployment in the field. The STIGs uses machine-readable code to automate compliance against rigorous common standards.

Nutanix has implemented Security Configuration Management Automation (SCMA) which is installed, configured, and enabled during the Nutanix deployment. There are configuration options, however one key differentiator is that Nutanix provides this functionality by default. SCMA checks multiple security entities for both Nutanix storage and AHV. Nutanix automatically reports inconsistencies and reverts them to the baseline.

With SCMA, you can schedule the STIG to run hourly, daily, weekly, or monthly. STIG has the lowest system priority within the virtual storage controller, ensuring that security checks do not interfere with platform performance.

In addition, Nutanix releases Security Advisories which describe potential security threats and their associated risks plus any identified mitigation(s) or patches.

For more information about security, see Building Secure Platforms And Services With Nutanix Enterprise Cloud.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1112

Authentication

Maintain as few user and group management systems as possible. A centrally managed authentication point is preferred to many separately managed systems. Based on that general recommendation you should at a minimum take advantage of the external LDAP support provided by Nutanix components.

Prism Central also provides both LDAP and Security Assertion Markup Language (SAML) and makes it possible for users to authenticate through a qualified Identify Provider (IdP). If none of the options are available Nutanix also provides local user management capabilities.

Table 91: Active Directory Authentication

SEC-001	USE ACTIVE DIRECTORY AUTHENTICATION. THIS APPLIES FOR USER AND SERVICE ACCOUNTS.
Justification	User activity logged for auditing purposes and account security is configured and maintained from a single centralized solution.
Implication	Requires a highly available active directory infrastructure and additional initial configuration.

Table 92: Using SSL/TLS Connection to Active Directory

SEC-002	USE SSL/TLS CONNECTION TO ACTIVE DIRECTORY.
Justification	Increases security by eliminating cleartext exchanges on the network.
Implication	Might require additional configuration.

Certificates

All components facing consumers should be protected with certificate authority (CA) signed certificates. Internal or external signed certificates depend on consumer classifi- cation and what kind of service the specific component provides.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1113

Table 93: Using a Certificate Authority

SEC-003	USE CERTIFICATE AUTHORITY (CA) THAT ARE CONSIDERED "TRUSTED CA" BY YOUR ORGANIZATION FOR THE COMPONENTS WHERE CERTIFICATES CAN BE REPLACED. THIS CAN BE EITHER INTERNAL OR EXTERNAL SIGNED CERTIFICATES.
Justification	Certificates are required as part of Transport Layer Security (TLS) protocol and are negotiated during session establishment to establish secure session. They provide an extra layer of security and prevent man-in-the-middle attacks.
Implication	Implementation effort and potentially an extra cost if certificates need to be purchased.

Cluster Lockdown

Nutanix cluster lockdown lets you enforce SSH access to the CVMs and hosts using key pairs instead of passwords.

Table 94: Nutanix Cluster Lockdown

SEC-004	DO NOT USE NUTANIX CLUSTER LOCKDOWN.
Justification	Nutanix recommends that access, including SSH, directly to CVM and hypervisor should be restricted to as few entities as possible:Operators. Keep service account passwords secure.Remote workstations. Use e.g. jump hosts.Networks. Use network segmentation via firewall rules or IPtables rules.
Implication	Users can access the CVM with username and password.

If only password-less communication is required, then enable Nutanix cluster lockdown.

VMware Cluster Lockdown

Cluster lockdown can be enabled at the VMware layer as well. Enabling either normal or strict cluster lockdown mode can fail the Nutanix cluster functionality. Make the necessary ESXi configurations to guarantee Nutanix functionality if vSphere cluster lockdown mode is required.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1114

Table 95: vSphere Cluster Lockdown

SEC-005	DO NOT USE VSPHERE CLUSTER LOCKDOWN.
Justification	No requirements exist in this design that justify vSphere cluster lockdown mode.
Implication	Users can access vSphere cluster with username and password.

Hardening

There are certain hardening configurations you can apply for the AHV host and the CVM if required:

- AHV and CVM
  - AIDE. Advanced Intrusion Detection Environment.
  - Core. Enable stack traces for cluster issues.
  - High Strength Passwords. Enforce complex password policy (Min length 15, different by at least 8 characters).
  - Enable Banner. Get specific login message via SSH.
- CVM only
  - Enforce SNMPv3 only.

Table 96: CVM and Hypervisor AIDE

SEC-006	ENABLE CVM AND HYPERVISOR AIDE
Justification	With AIDE enabled, the environment will perform checksum verification of all static binaries and libraries for improved security.
Implication	Additional, very limited, CVM and hypervisor resources will be required.

Table 97: Configuring SCMA

SEC-007	CONFIGURE SCMA TO RUN HOURLY
Justification	To more quickly capture unacceptable configuration drift. Default is to take actions daily.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1115

Implication	SCMA is lightweight and adds very limited additional load to CVM and hypervisor. Security benefits outweigh the added resources.

Table 98: Unused ESXi Services and Unused Firewall Ports

SEC-008	STOP UNUSED ESXI SERVICES AND CLOSE UNUSED FIREWALL PORTS. Important: Make sure not to stop a service or close a firewall port required by Nutanix, such as SSH and NFS
Justification	To limit the attack surface.
Implication	Additional configuration required.

We recommend that you follow the Hardening Controller VM guide. If you are using AHV, follow the Hardening AHV guide.

For updated Hardening Guides, search portal.nutanix.com for the most recent guide that relates to your version of AOS and AHV.

Internet-facing Services

Security for Internet-facing services is out of the scope of this design, but highly important and mentioned here for awareness.

Internet-facing services are at constant risk of being attacked. Two common types of attacks are denial of service (DoS) and distributed denial of service (DDoS). To help mitigate the potential impact of a DoS or a DDoS attack a design can take advantage of:

- Multiple internet connections (active/backup).
- ISP provided DoS and DDoS filtering.

There are additional ways to implement protection against these types of attacks.

Logging

Logging is critical from an auditing and traceability perspective so making sure the virtual infrastructure, AOS, Prism Central, AHV, ESXi, any additional software

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1116

in the environment send their log files to a highly available log infrastructure is critical.

Recommendation

A minimum one of the individual targets making up the highly available logging infrastructure should run outside of the virtual infrastructure itself so that if the virtual infrastructure is compromised, forensic investigations will need to access logs that might not be available on the cluster itself.

A single centralized activity logging solution for auditing purposes and account security should be configured and maintained.

Table 99: Logging

SEC-009	SEND LOG FILES TO A HIGHLY AVAILABLE SYSLOG INFRASTRUCTURE.
Justification	Logs are helpful in report creation, during troubleshooting, and for investigating potential security breaches.
Implication	Requires initial configuration and a highly available logging infrastructure.

Table 100: Including All Nutanix Modules in Logging

SEC-010	INCLUDE ALL NUTANIX MODULES IN LOGGING.
Justification	Ensures data from all modules are included and search- able via a logging system. Refer to Nutanix Syslog documentation for additional information. Modules can be excluded if needed.
Implication	Data will be generated per module meaning the more modules included, the more log data is generated.

Table 101: Error Log Level for Nutanix Components

SEC-011	USE ERROR LOG LEVEL FOR THE NUTANIX COMPONENTS.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1117

Justification	Ensures data from all modules are included and searchable via a logging system. Refer to Nutanix Syslog documentation for additional information. Modules can be excluded if needed.
Implication	Will not send all logging information to syslog infrastructure. The following levels will be included:ErrorCriticalAlertEmergency

Table 102: ESXi Logging Level, Rotation, and File Size

SEC-012	USE DEFAULT ESXI LOGGING LEVEL, LOG ROTATION, AND LOG FILE SIZES.
Justification	No reason to change size and rotation unless a huge amount of logs are expected.
Implication	In rare situations, logs might rotate very fast.

Table 103: Protocols for Log Transport

SEC-013	IF EXTRA SECURITY AND RELIABILITY ARE REQUIRED, THEN USE TCP FOR LOG TRANSPORT. OTHERWISE, USE THE DEFAULT SYSLOG PROTOCOL, UDP.
Justification	Provides a reliable logging setup and ensures the logs are being received by the logging infrastructure.
Implication	Requires a sender and receiver to establish communication which generates minimal additional network traffic. May require configuration of logging infrastructure to accept TCP communication.

Table 104: Using Port 514 for Logging

SEC-014	USE PORT 514 FOR LOGGING.
Justification	Defined port in syslog RFC. No reason has been identified to change the port.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1118

Implication	Traffic on well-known ports can be easy to locate.

Network Segmentation

To protect Nutanix CVM and hypervisor traffic, place them together in their own dedicated VLAN, separate from other VM traffic. This applies to all hosts in a cluster.

Nutanix recommends configuring the CVM and hypervisor host VLAN as a native, or untagged, VLAN on the connected switch ports. This native VLAN configuration allows for easy node addition and cluster expansion. By default, new Nutanix nodes send and receive untagged traffic. If you use a tagged VLAN for the CVM and hypervisor hosts instead, you must configure that VLAN while provisioning the new node, before adding that node to the Nutanix cluster.

Do not segment Nutanix storage and replication traffic, or iSCSI Volumes traffic, on separate interfaces (VLAN or physical) unless additional segmentation is required by mandatory security policy or the use of separate physical networks. The added complexity of configuring and maintaining separate networks with additional interfaces cannot be justified unless absolutely required.

Table 105: VLAN for Traffic Separation

SEC-015	USE VLAN FOR TRAFFIC SEPARATION OF MANAGEMENT AND USER WORKLOADS.
Justification	VLAN is a well-known standard for traffic separation when there are no requirements specifying physical separation.
Implication	This provides clear separation between: Management and end user traffic, Different management traffic types, and Different end user traffic types.

Table 106: Place CVM and Hypervisor on Same VLAN and Subnet

SEC-016	PLACE CVM AND HYPERVISOR ON THE SAME VLAN AND SUBNET.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1119

Justification	Required for Nutanix functionality. Both hypervisor and CVM should be classified as core or management service traffic delivering the same service and can therefore be placed on the same VLAN.
Implication	Different components placed on the same network segment. Alternate configurations are not supported.

Table 107: Place Out-of-band Management on a Separate VLAN or Physical Network

SEC-017	PLACE OUT-OF-BAND MANAGEMENT ON A SEPARATE VLAN OR PHYSICAL NETWORK.
Justification	Out-of-band management is not required for core Nutanix functionality. To provide additional security, the management interface should not be on the same network segment as the CVM and hypervisor.
Implication	Network or VLAN management.

Role-based Access Control (RBAC)

Nutanix has built-in RBAC in both Prism Central and Prism Element, with the option to create custom roles in Prism Central. RBAC is used to limit access and control for various individuals and groups of administrative users. Use a least-privilege and separation-of- duties approach when assigning permissions to make sure each group or individual user has just enough permissions to perform their duties. Use pre-defined roles or create new roles as needed.

Configure RBAC at the Prism Central level since it provides the overlying management construct. Via Prism Central, consumers and administrators will be directed to underlying components, such as Prism Element, when needed. This ensures your least-privilege configuration stays in place, avoiding common mistakes that occur when RBAC is configured at multiple different levels.

The following table shows Prism Central default roles:

Table 108: Default Prism Central Roles

Role	Purpose

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1120

Super Admin	Highest-level admin with full infrastructure and tenant access. Manages a Nutanix deployment and can set up, configure, and make use of every feature in the platform.
Self-Service Admin	Cloud admin for a Nutanix tenant. Manages virtual infrastructure, oversees self-service, and can delegate end-user management.
Project Admin	Team lead to whom cloud administration is delegated in the context of a project. Manages end-users within a project and has full access to their entities.
Prism Viewer	View-only admin. Has access to all infrastructure and platform features but cannot make any changes.
Prism Admin	Day-to-day admin of a Nutanix deployment. Manages the infrastructure and platform but cannot entitle other users to be admins.
Operator	Lifecycle manager for team applications. Works on existing application deployments, exercises blueprint actions.
Developer	Application developer within a team. Authors blueprints, tests deployments, and publishes applications for other project members.
Consumer	Owner of team applications at runtime. Launches blueprints and controls their lifecycle and actions.

When creating custom roles in Prism Central there are multiple entities available, each with their own set of permission definitions:

- App
- VM
- Blueprint
- Marketplace Item
- Report
- Cluster
- Subnet
- Image

The following table describes Prism Element default roles:

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1121

Table 109: Prism Element Default Roles

Role	Purpose
User Admin	Able to view information, perform any administrative task, and create or modify user accounts.
Cluster Admin	Able to view information and perform any administrative task. Cannot create or modify user accounts.
Viewer	Able to view information only. No permission to perform any administrative tasks. Useful for auditing purposes.

In addition, there are pre-defined roles in VMware vCenter Server, with the option to create custom roles.

Table 110: Use Least-Privilege Approach when Determining Access

SEC-018	USE A LEAST-PRIVILEGE ACCESS APPROACH WHEN DECIDING WHO HAS ACCESS. ALIGN RBAC STRUCTURE AND USAGE OF DEFAULT PLUS CUSTOM ROLES ACCORDING TO COMPANY REQUIREMENTS.
Justification	This approach helps protect the environment from having users performing actions they are not authorized to perform.
Implication	Access requirements need to be defined, created, and implemented for each access group.

Table 111: Align RBAC to Company Structure

SEC-019	ALIGN RBAC STRUCTURE AND USAGE OF DEFAULT PLUS CUSTOM ROLES ACCORDING TO THE COMPANY REQUIREMENTS DEFINED VIA SEC-018.
Justification	There are numerous ways of applying RBAC. This design document can't cover all possibilities.
Implication	If no company structure exists, fall back on description in SEC-018 and create a structure that meets your needs.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1122

Data-at-Rest Encryption

Data-at-Rest Encryption (DaRE) is a security measure to prevent data from being stolen. DaRE offers protection against data exposure in the event of:

- Activities that require a full data copy that will be used outside the platform.
- Failed drives leaving the datacenter.
- Drive or node theft.

Keeping management traffic, including storage traffic, on a separate network is often an adequate data security practice. Nutanix supports four different options for Data at Rest Encryption (DaRE):

- Self-Encrypting Drives (SEDs) with an External Key Manager (EKM).
- Software-based encryption with an EKM.
- Software-based encryption and SED with an EKM (aka Dual Encryption).
- Software-based encryption with the Nutanix Native Key Manager (KMS).

With all software-based encryption options, encryption is performed in the software layer and data is encrypted over the wire, between CVMs. All or part of the user VM data can be encrypted.

- AHV encrypts the entire Nutanix cluster.
- ESXi gives you the option to define encryption on a per-Nutanix-container basis if required.

Self-Encrypting Drives (SEDs) provide FIPS 140-2 Level 2 compliance and can be used without any performance impact. Nutanix Software Based Encryption and Native Key Manager are FIPS 140-2 Level 1 Evaluated.

You can use both software-based encryption and SEDs. This requires an external key management server.

> Note: All methods of DaRE are FIPS 140-2 compliant however if levels 2, 3, or 4 are required a hardware component is necessary. Software-based encryption with the Nutanix Native Key Manager (KMS) can encrypt storage containers (ESXi or Hyper-V) or the entire Cluster (AHV).

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1123

Table 112: Do Not Use Storage Encryption

SEC-020	DO NOT USE STORAGE ENCRYPTION.
Justification	There are no technical requirements to justify implementing storage encryption in this design.
Implication	Data is never encrypted unless encrypted at the virtual machine level or via the ESXi VM encryption feature.

Key Management Server

A key management server is required when using Nutanix storage encryption.

When using an external key management service, you should have a minimum of two key management servers running. At least one server must not run on the infrastructure it is protecting.

Table 113: Do Not Use a Key Management Server

SEC-021	DO NOT USE A KEY MANAGEMENT SERVER.
Justification	No functionality will be used that requires a key management server.
Implication	N/A

Flow Network Security

During the environment life cycle, it's important to ensure compliance is met and that your security configuration meets required standards. Flow Network Security provides a centralized view of the security posture of your Nutanix environment and provides visibility into the security of your on-prem environment based on known compliance standards.

Flow Network Security can help you to comply with regulatory and business-specific compliance policies such as PCI-DSS, HIPAA, and NIST. (Note: Xi Beam is not available for dark sites.)

You gain deep insights into your on-premises Nutanix deployments based on over 300 audit checks and security best practices according to:

- Audit security checks for access, data, networking, and virtual machines.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1124

- Compliance checks against PCI-DSS v3.2.1 for AHV, AOS, Flow Network Security, and Prism Central.
- For more information on Flow Network Security, see the Flow Network Security Guide.

Automation Layer Design

Nutanix supports intelligent IT operations and advanced automation that enable you to streamline operations, enable IT as a Service, and support the needs of developers and business teams. This section covers automation and orchestration of virtual infrastructure, focusing on provisioning and maintenance which are important aspects of the overall solution. Nutanix tools reduce the time required to perform initial setup plus software and firmware upgrades.

Upgrades

Upgrades can occur across a variety of components. The process to upgrade many of these components is primarily executed using LCM, which is able to understand dependencies without operator intervention.

It's important to understand the impact of upgrading certain software components, as their upgrade may affect the outside world.

- AOSWhen upgrading, each CVM is individually upgraded in a rolling fashion. While a CVM is rebooting, the host it is running on is redirected to a remote CVM to deliver storage IO. This is invisible to the VM. However, it does result in a loss of locality, which can potentially impact IO throughput and latency if the load on the system is high.
- HypervisorWhen upgrading the hypervisor on a node, each VM must be migrated off the host for the update to be performed so that a reboot of the host can occur. For vSphere, this requires vCenter integration to be configured to allow for a host to be put into maintenance mode.AHV live migration and vSphere vMotion are normally non-disruptive, however certain applications that utilize polling-style device drivers or that have near-real-time kernel operations cannot tolerate being migrated during the final cutover step. Hypervisor updates will require downtime for these apps if they don't offer native failover functionality.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1125

Firmware

Firmware can be updated for a variety of devices including:

- Board Management Controller (BMC)
- Motherboard (BIOS)
- Host Bus Adapter (HBA)
- Host Boot Device (SATA DOM)
- SSD or HDD
- NIC

Software

Software updates can be performed for multiple components, including:

- Acropolis Operating System (Core AOS in CVM)
- Hypervisor (vSphere or AHV)
- Nutanix Cluster Check (NCC)
- Life Cycle Manager (LCM)
- Acropolis Operating System (AOS in Prism Central)
- MicroServices Platform (MSP in Prism Central)
- Services Functionality
  - Nutanix Files (Prism Element)
  - Calm/Epsilon (Prism Central)
  - Objects Manager (Prism Central)
  - Karbon (Prism Central)
  - Era (independent)
  - Move (independent)
  - X-Ray (independent)

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1126

Life Cycle Manager (LCM)

Nutanix Lifecycle Manager (LCM) improves the efficiency and reliability of IT infrastructure upgrades in modern datacenters. Nutanix LCM determines any software and firmware dependencies, intelligently prioritizes updates, and automates the entire upgrade process across all clustered hosts, without any impact to applications or data availability. It supports one-click upgrades across multiple qualified hardware manufacturers and configurations, so IT teams have the flexibility to deploy the best hardware for each use case – and still benefit from centralized upgrade capabilities. LCM supports AHV, ESXi and Hyper-V hypervisors, plus hardware support for Nutanix, Hewlett Packard Enterprise, Dell/EMC, Lenovo, Fujitsu, Inspur and Intel. LCM supports environments with internet connectivity as well as dark site deployments.

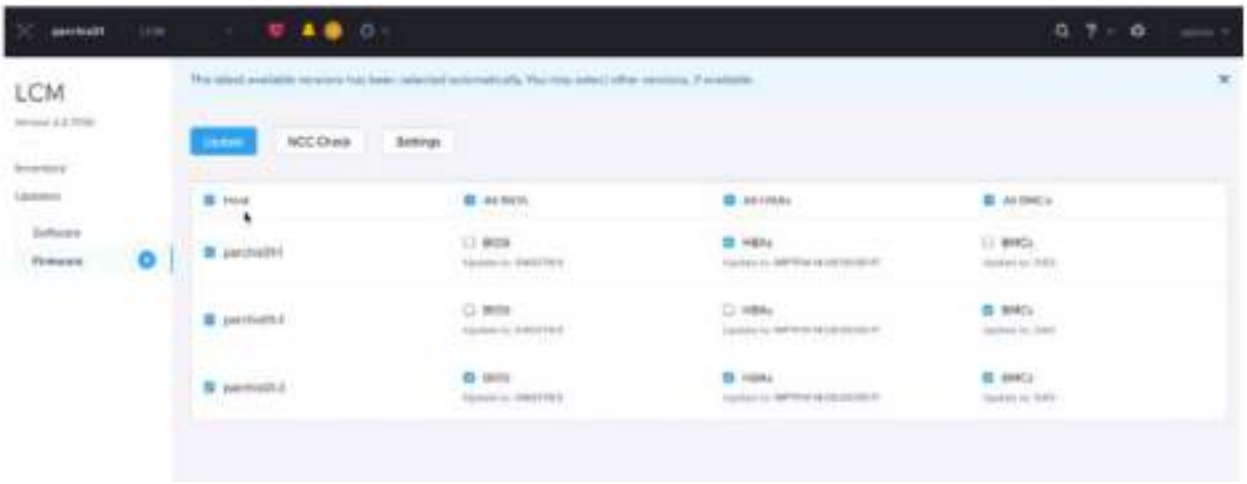


Figure 51: Life Cycle Manager

Foundation

Foundation manages the initial setup and configuration of a cluster. Nutanix nodes may come pre-installed with AHV and the Controller Virtual Machine (CVM) and you can:

- Add the Nodes to an existing Nutanix cluster.
- Create a new Nutanix cluster.
- Re-image the nodes with different AHV and or AOS version or different hypervisor and create a Nutanix cluster.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1127

There are five ways of invoking a Foundation process:

- Connect to a factory deployed Nutanix node's CVM via http://CVM_IP:8000/
- Use portable Foundation, Mac or Windows executable.
- Standalone Foundation VM.
- When adding a node to an existing Nutanix cluster.
- Call Foundation API via third party solution which provides a way to orchestrate the deployment.

Note: The Foundation process may vary for different hardware vendors.

Nutanix provides a Foundation pre-configuration service which is accessible via install. nutanix.com. Via the service, you can define and download the Nutanix cluster configuration to be used during the Foundation process. The downloaded file contains all configuration required to perform the foundation operation and comes in json format. This makes it easy to keep track of configurations, document them, and share with your peers.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1128

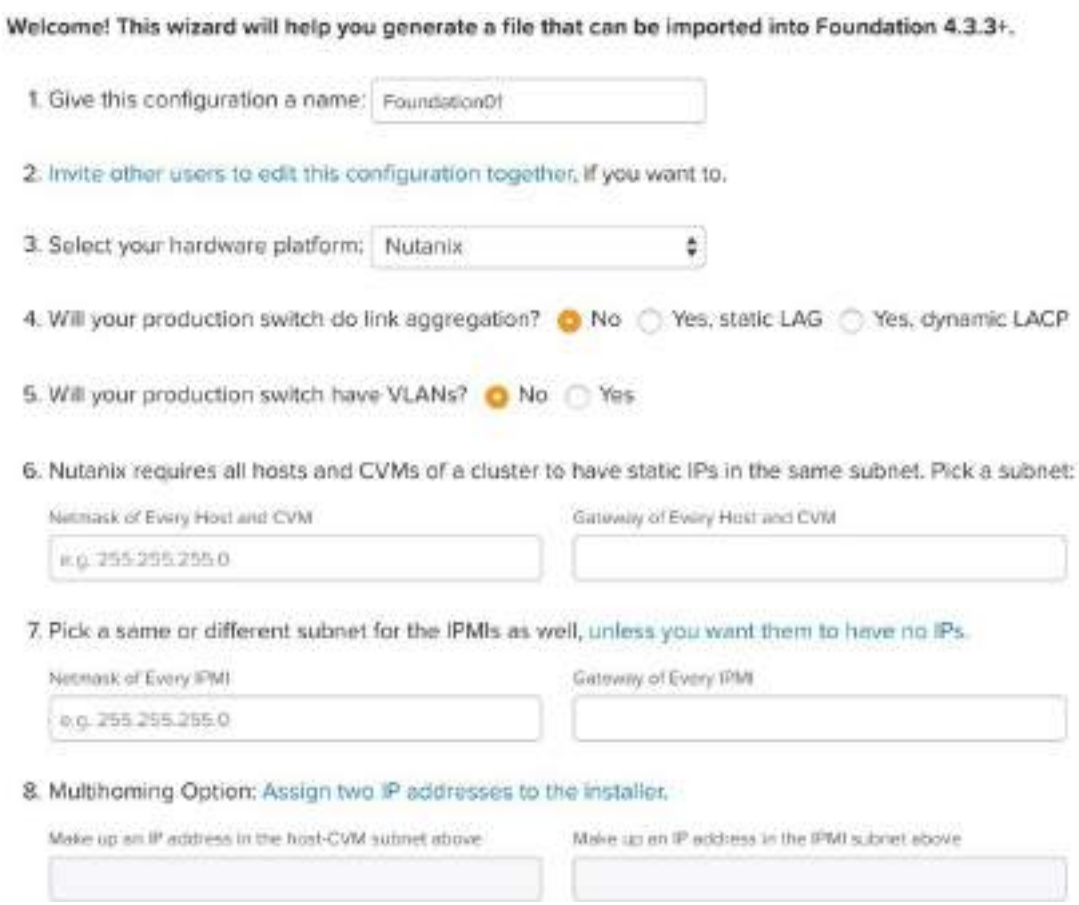


Figure 52: Foundation Pre-Configuration Service

The following table provides an overview of the functions available for the different Foundation software options.

Table 114: Overview of Different Foundation Software Options

	CVM Foundation	Portable Foundation (Windows, Mac)	Standalone Foundation VM
Function	Factory-imaged nodes.	Factory-imaged nodes.	Maintains high availability in the event of the loss of one switch.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1129

Bare-metal nodes	Factory-imaged nodes.		Requires at least two TOR switches, which will impact cost and rack space. Increases total bandwidth to each host to 20 Gbps.
Bare-metal nodes			
Hardware	Any	Nutanix (NX)	
Dell (XC)			
HPE (DX)	Any		
If IPV6 is disabled	Cannot image nodes.	IPMI IPv4	
required on the nodes.	IPMI IPv4 required on the nodes.		
VLAN Support	No	No	Yes
LACP Support	Yes	Yes	Yes
Multi-homing Support	N/A	Yes	Yes

Note: When available, Foundation Central will provide capabilities to perform Foundation operations via Prism Central.

Operations Design

Capacity and Resource Planning

After initial installation and migration of workloads to the platform, long term capacity planning should be enabled to avoid running out of resources. Many of the features discussed are integrated into Prism Pro.

Table 115: Deploying Prism Pro for Enhanced Cluster Management

OPS-001	DEPLOY PRISM PRO FOR ENHANCED CLUSTER MANAGEMENT

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1130

Justification	Analytics, Capacity planning, Custom Dashboards, and Playbooks require the presence of Prism Pro.
Implication	Requires an additional license, which can increase cost.

Cluster capacity

Native runway calculations built into Prism Central will automatically calculate the remaining capacity of the system as soon as the cluster Prism Element is brought under management by Prism Central.

Figure 53: Capacity Runway

These runway calculations should be configured to run as part of periodic reports and reviewed on a regular basis to ensure sufficient capacity exists. This is especially important for organizations that have a significant lag between the date a commitment to purchase additional gear occurs and when its online and available to use.

Expansion planning

When a new workload is identified to be onboarded, planning needs to occur if the new workload size or requirements are outside of established patterns. Prism Central offers a scenario simulation function that shows how the available

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1131

capacity runway would change if this new workload was accommodated. Utilizing this planning functionality helps avoid unplanned capacity constraints.

Figure 54: Expansion Planning

Table 116: Reviewing Monthly Capacity Planning

OPS-002	REVIEW MONTHLY CAPACITY PLANNING
Justification	Analytics, capacity planning, custom dashboards, and playbooks require Prism Pro.
Implication	Requires an additional license, which can impact cost.

Right-Sizing VMs

While general system capacity planning is useful, accurate and efficient system level planning requires accurate sizing for individual workloads. Machine learning in Prism Central provides anomaly detection for VMs when the workload crosses learned thresholds.

In addition, based on a number of thresholds, the system will categorize VMs based on their behavior. These categories include:

- Bully: A VM with potential to degrade the overall cluster performance by impacting the capability of the node they reside on.
- Constrained: A VM that is experiencing very high CPU or RAM utilization and potentially is unable to meet the needs of the application its running and is likely a candidate to increase the resources provided.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1132

- Over-provisioned: A VM that is significantly underutilizing the resources provided to it and is likely a candidate to reduce in size.
- Inactive: A VM that has not powered on recently (dead) or is virtually idle (zombie) that is a candidate for reclamation.

In addition, custom alert policies can be created that match VMs by conditions.

Upgrade Methodology

This section describes the design decisions associated with upgrading the Nutanix infrastructure. Whether to perform upgrades during business hours or outside business hours comes down to a number of possible factors, including:

- Is the environment sized to tolerate failures during upgrades?
- Will performance be adequate during upgrades?
- Past experiences.
- Size of Nutanix cluster.

Table 117: Performing Updates

OPS-003	PERFORM UPDATES AFTER HOURS FOR PERFORMANCE OR MIGRATION SENSITIVE APPLICATIONS
Justification	Reduces load on the system to be handled during rolling CVM reboot from code upgrade.
Implication	Potential staffing impact.

When upgrading, AOS offers the choice of release trains to apply. Each of these is denoted with a major.minor.maintenance.patch numbering scheme, for example: 5.10.7.1 or 5.11.1.1.

A release train is based on the major and minor components. There are two types of release trains:

- Short Term Support (STS) releases which include new features and provide a regular and frequent upgrade path. These releases are maintained for shorter durations.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1133

- Long Term Support (LTS) releases which provide bug fixes for features that have been generally available for a longer period of time. After features have been generally available in an STS for some time, they are included in and LTS, which are maintained for a longer duration.

KB 5505 on the Nutanix Support Portal covers the differences in greater detail.

Table 118: Utilizing the Current LTS Branch

OPS-004	UTILIZE THE CURRENT LTS BRANCH
Justification	Unless a new feature is required for a design, enterprise customers typically prefer a less frequent major version change of software components.
Implication	Lack of access to features present in or requiring new branch.

Updates to an existing train are released on a regular basis and should be applied on a standard cadence.

Table 119: Upgrading to Maintenance and Current Patch Versions

OPS-005	UPDATE TO THE NEXT MAINTENANCE VERSION 4 WEEKS AFTER RELEASE. UPDATE TO THE CURRENT PATCH VERSION 2 WEEKS AFTER RELEASE.
Justification	Unless a new feature is required for a design, enterprise customers typically prefer a less frequent major version change of software components.
Implication	Frequent smaller updates keep the amount of changes per update relatively small, minimizing the amount to troubleshoot in the event something goes wrong.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1134

Testing

Environments which seek to achieve high overall uptime greater than 99.9% should build a pre-production environment to mimic production so that configuration changes can be tested before being pushed into production.

Table 120: Maintaining a Pre-Production Environment

OPS-006	MAINTAIN A PRE-PRODUCTION ENVIRONMENT FOR TESTING ANY CHANGES NEEDED (FIRMWARE, SOFTWARE, HARDWARE) PRIOR TO EXECUTING THE CHANGE IN PRODUCTION.
Justification	Environments typically have stringent uptime due to associated financial penalties or losses that occur from unavailable services. The cost of an outage with a realistic duration often outweighs the pre-production environment cost.
Implication	A pre-production environment will increase the overall cost of the solution.

Monitoring

Nutanix includes a variety of built-in, system-level monitoring functions. The relevant metrics for built-in monitoring are automatically gathered and stored without user intervention required.

Native cluster alerts can be sent from either the individual cluster or Prism Central.

Table 121: Configuring Alerts and Alert Policies

OPS-007	CONFIGURE ALERTS AND ALERT POLICIES IN PRISM CENTRAL, NOT PRISM ELEMENT.
Justification	Creates consistency across multiple clusters and reduces effort when making multiple changes. Also allows for anomaly detection.
Implication	Requires Prism Central to receive alerts.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1135

When alerts are generated, in addition to raising the alert in Prism, the system can generate an outbound message. The two options available for sending alerts are SNMP and SMTP.

Table 122: Utilizing SMTP for Alert Transmission

OPS-008	UTILIZE SMTP FOR ALERT TRANSMISSION
Justification	Creates consistency across multiple clusters and reduces effort to make multiple changes. Also allows for anomaly detection. Offers more options to customize delivery.
Implication	Requires access to SMTP systems.

The following screen shows how to configure Prism to send alerts to a specified email account via SMTP.

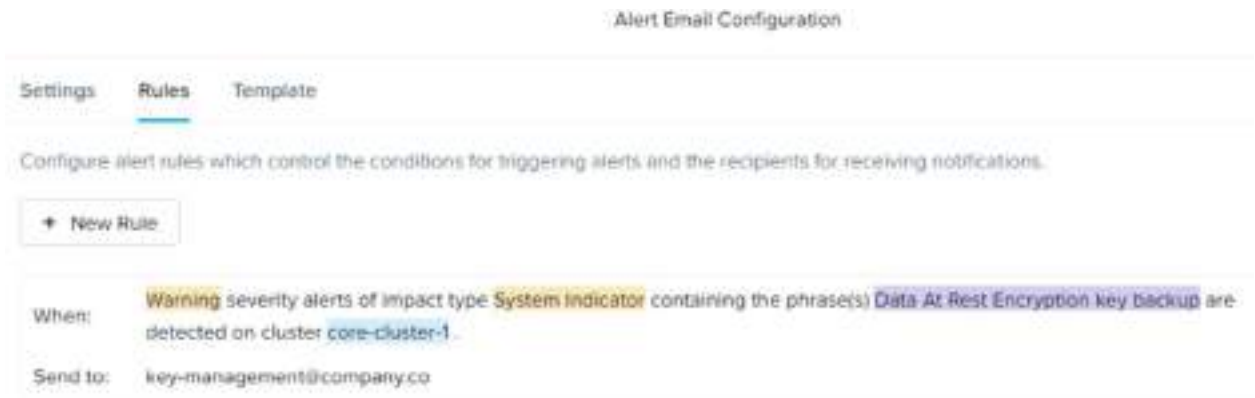


Figure 55: Alert Email Configuration

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1136

5. Multidatacenter Design for Nutanix Core and Business Continuity and Disaster Recovery

Choosing the Right Business Continuity and Disaster Recovery Solution

General Guidance

Choosing the right solution for business continuity and disaster recovery (BCDR) is one of the key decisions every architect must make. A mistake can cause significant pain to the business and millions of dollars of losses.

The two key business requirements when designing BCDR solutions are recovery point objective (RPO) and recovery time objective (RTO). In addition to RPO and RTO, consider work recovery time (WRT) and maximum tolerable downtime (MTD).

- RPO: The maximum acceptable amount of data loss measured in time
- RTO: The maximum tolerable amount of time needed to bring a critical system back online
- WRT: The maximum tolerable amount of time that is needed to verify the system and data integrity
- MTD: The total amount of time that a business process can be disrupted without causing any unacceptable consequences

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1137

Figure 56: General Guidance for Business Continuity

When designing new BCDR solution make sure to understand your business requirements and technical constraints. Nutanix provides a range of protection mechanisms to help with data protection. The general advice when designing BC\DR is:

If an application has native data protection mechanisms (such as Exchange DAG, MS SQL Always On, Oracle RAC) leverage those to provide application data protection. If an application does not provide a data protection mechanism, use Nutanix built-in protection mechanisms.

The flowchart below can help guide your decision making.

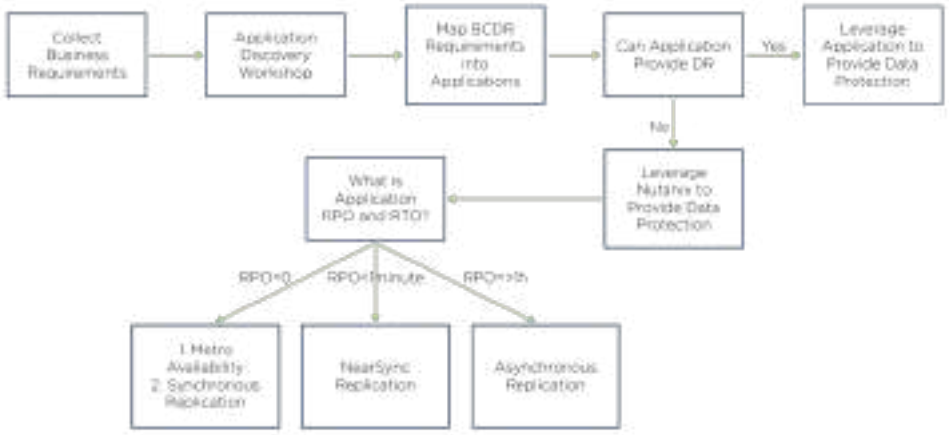


Figure 57: BCDR Workflow

Disaster Recovery Target Considerations

Disaster recovery requires a secondary location that is far enough away from the primary location to ensure that it won't be affected by the disasters you

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1138

need to protect against but close enough that latency and bandwidth don't become a limiting factor. You can use multisite disaster recovery, as described later to protect workloads using a combination of sites at different distances.

Another important consideration is whether disaster recovery uses on-premises locations or an option in the cloud:

- On-premises: Disaster recovery using on-premises target locations gives you complete control over (and responsibility for) your disaster recovery operations. However, it may require significant CapEx and ongoing operating expense to maintain adequate resources to support failover if it becomes necessary.
- Nutanix DRaaS: DRaaS offloads much of the complexity and cost of disaster recovery. Nutanix DRaaS is a simple-to-configure disaster recovery service available to Nutanix customers.
- Nutanix Cloud Clusters: Nutanix Cloud Clusters (NC2) allows you to operate a full Nutanix environment in the public cloud. You can utilize NC2 as a disaster recovery target and take advantage of cloud resources while maintaining full control and complete operational continuity with on-premises Nutanix AOS environments.

Multidatacenter Design

Datacenter Resiliency Patterns

When operating applications across multiple physical locations for the purposes of improved resiliency, there are two common sets of operating patterns.

Active-Active

In an active-active pattern, two (or more) datacenters provide resources to actively support of a service. For this definition, the application is expected to be fully capable of continuing to service requests in the event one of the active AZs goes down. While it is up to the specific application architecture to determine exactly how the components are split up and their fault/partition tolerance, active sites are typically operated with a low latency constraint of 5 ms or less RTT.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1139

In the event of a localized disaster affecting only one availability zone, the application maximum throughput or capability is reduced in proportion to the resources lost in the down AZ.

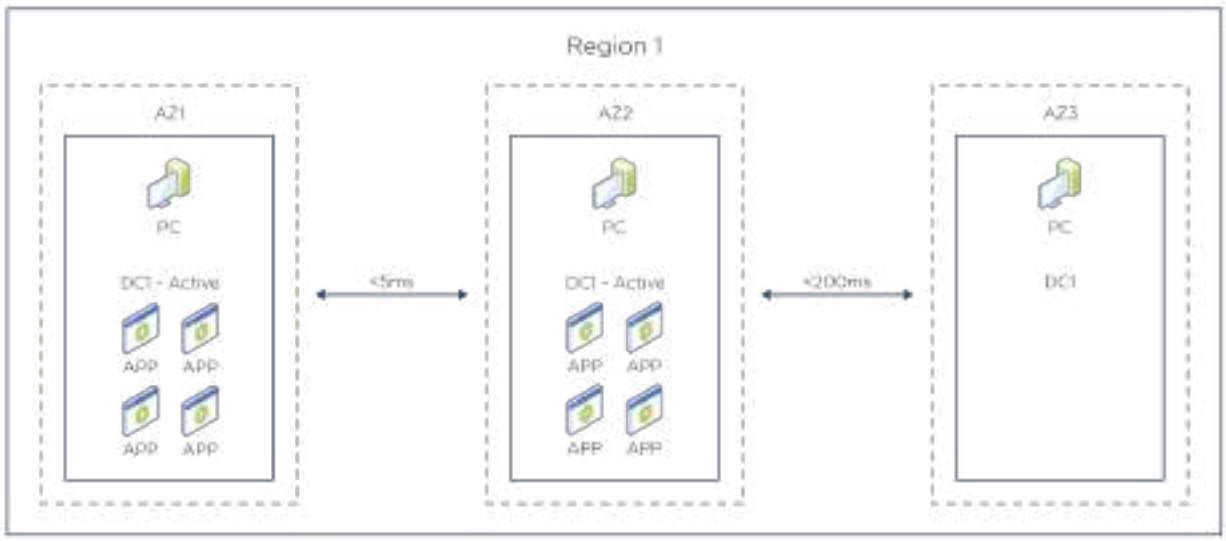


Figure 58: Active-Active

Active-Passive

In an active-passive scenario, only one datacenter has active resources supporting a service. An additional datacenter is available to provide services if the primary datacenter goes down. For some application architectures the passive facility has resources configured and ready (sometimes referred to as warm standby). Under normal conditions those resources are not servicing user requests. These warm standby applications are delineated from true passive systems, where the data is replicated but the compute is not ready and waiting.

A hybrid model is also possible, where a portion of the environment in each datacenter is active and a portion is a standby for another site. For example, business unit 1 (BU1) may run actively out of AZ1 and passively out of AZ2 due to the application design, while BU2 is actively running out of AZ1 and AZ2.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1140

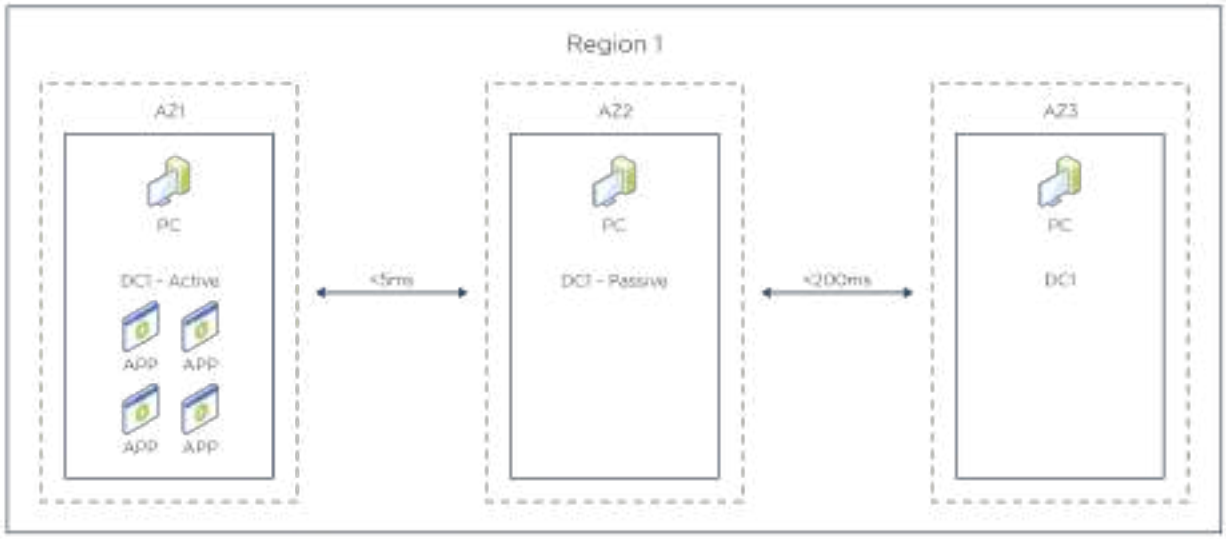


Figure 59: Active-Passive

Multisite Disaster Recovery

In either of the above patterns, application components may be further protected via an N + 1 site providing disaster recovery capacity. Typically, the disaster recovery site is located either geographically far away from the primary system inside of the same region, or in another region entirely, providing better isolation from a widespread disaster (hurricane, large-scale flooding, tier 1 ISP issues), however the physical distances often create greater latency.

Replication Options

Snapshots and Clones

To provide full coverage data protection, Nutanix includes a number of native features, as well as integration with third-party backup vendors.

As a first level of protection (local recovery), an individual cluster can create a snapshot of a vDisk or an entire VM. Nutanix snapshots are redirect-on-write, where the pointers that indicate which physical disk extent maps to a virtual disk are updated only as data changes. This technique creates little to no performance overhead for a running workload when a snapshot exists. Cloned

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1141

entities use the same principle and enjoy the same benefit. Additional data capacity is not used by the snapshot or clone unless changes are made to it.

The minimal overhead makes it low risk to protect as many workloads as necessary with snapshots. Protected VMs can have differing levels of retention and snapshot frequency, allowing for as much flexibility as needed to work around application scheduling requirements.

When choosing a retention schedule, choose the minimum number of snapshots that meet RPO requirements. Each snapshot requires additional metadata space to track the related extents on disk, and excessively deep snapshot chains can increase the background load on the CVM as part of its maintenance processing.

There are two options available for snapshots. Snapshots that invoke a method for quiescence inside the guest VM operating system are termed application-consistent, and those that do not inform the guest VM operating system are termed crash-consistent. AOS can trigger an application-consistent snapshot via Nutanix Guest Tools and/or VMware tools, depending on the hypervisor in use.

Guest limitations may prevent proper quiescence for very large machines (for example Windows VSS cannot handle more than 64 devices/drives concurrently).

Table 123: Utilizing Application-Consistent Snapshots

BCN-001	UTILIZE APPLICATION CONSISTENT SNAPSHOTS WHEN NEEDED BY THE APPLICATION
Justification	VM/application quiescence allows for a “clean” snapshot from the application’s viewpoint.
Implication	Application quiescence can potentially take a significant amount of time, and the throughput of the application may be adversely affected. Consistency groups should have less than 20 members

For ESXi hypervisor triggered clones, AOS supports offloading the clone via VAAI. The VM must meet vSphere’s requirements to trigger offloading (VM

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1142

must be powered off and the clone must reside on the same datastore as the primary VM).

Local snapshots and clones provide an easy restoration point on the local cluster in the event something goes wrong with the VM itself (OS bluescreen after patches, recover to a point before ransomware encryption, etc.). These snapshots can be instantiated in seconds, allowing for a very short RTO until VM boot. Via API integration, 3rd party backup vendors can utilize Prism REST API endpoints to minimize backup load and space required.

Nutanix also provides the ability to replicate data between clusters, where the data point referenced in the snapshot is stored on one or more remote clusters. As part of the snapshot schedule, these remote clusters can have a different retention period than the primary. An example of this would be keeping three daily copies locally on a performance-oriented all flash cluster, and 14 daily copies on a remote hybrid cluster.

There are two different forms of snapshots to support different modes of replication:

- Full snapshots for asynchronous replication (with RPO of 60 minutes or greater).
- Lightweight snapshots (LWS) for NearSync replication (when the RPO is between 15 minutes and 1 minute).

Full snapshots are efficient for keeping system resource usage low when you are creating many snapshots over an extended period of time. LWS reduces metadata management overhead and increases storage performance by decreasing the number of storage I/O operations that long snapshot chains can cause.

Nutanix snapshots are a vital first element of an overall data protection strategy, however they are not a substitute for a full backup methodology. Many organizations subscribe to what's referred to as the 3-2-1 rule, which mandates 3 copies of data, on 2 backup mediums, with at least 1 copy offsite.

Snapshots can be replicated to multiple destination clusters to provide multiple redundant copies if needed. These arrangements are configured as part of the snapshot schedule by specifying each remote site that should receive a copy, and how many to retain at that site. One to many relationships are allowed (Site

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1143

A-> Site B, Site A -> Site B, Site A –> Site N), but cascading relationships (Site A -> Site B -> Site N) are not supported.

Direct Cluster to Cluster Backup and Recovery

When creating the configuration and schedules for snapshots, there are multiple options. Prism Element on each cluster offers a construct called a Protection Domain (PD), which is a grouping of VMs. During a failover event, all the entities in the Protection Domain are activated at the remote site as a group. Each VM must be placed manually in an applicable PD, either via Prism or by an API call.

The RPO (time between successive snapshots) chosen for these entities will determine whether the system uses traditional asynchronous snapshots, or lightweight snapshots.

Recommendations: Protection Domains

- No more than 200 VMs per PD.
- No more than 10 VMs per PD with NearSync.
- Group VMs with similar RPO requirements in the same PD.

Note that size and capacity of a node can limit the RPO achievable for VMs running on it. See AOS Snapshot Frequency for Nutanix Nodes on the Nutanix Support portal for details.

Consistency Groups

Administrators can create a Consistency Group for VMs and volume groups that are part of a Protection Domain where you want to snapshot all members of the group in a crash-consistent manner. All entities in the same Consistency Group will have their snapshot execute at exactly the same time. Entities that are not in a Consistency Group, but part of the same schedule will typically snapshot close together, but not at the exact same moment (potentially a few seconds apart).

Recommendations: Consistency Groups

- Keep Consistency Groups as small as possible. Limit Consistency Groups to fewer than 10 VMs.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1144

- Consistency Groups should only be used for applications with a shared state, such as database replicas.
- A Consistency Groups using application-consistent snapshots can contain only 1 VM.

Table 124: Place Nearsync VMs in their Own Protection Domain

BCN-002	PLACE NEARSYNC VM'S IN THEIR OWN PROTECTION DOMAIN.
Justification	NearSync can only have one schedule so place NearSync VMs in their own PD.
Implication	Multiple PDs will need to be created for different NearSync VMs depending on their schedule requirements.

Snapshot Schedule and Retention Policy

Full Snapshots and Async Replication

Your RPO determines how much data you will lose in the event of a failure. You can create multiple schedules for a Protection Domain using full snapshots at various frequencies with different retention policies.

The snapshot interval should be shorter than the desired RPO to allow for failure and recovery, without manual intervention. This is ideally at least twice as fast as your desired RPO, including data transmission timing. For example:

- RPO objective: data should be no more than 4 hours old
- Snapshot schedule: every 4 hours, starting at 12 AM, with retention on a remote cluster
- Average replication of changes takes approximately 30 minutes.
- The source site experiences an outage at 4:20 AM

In the scenario above because replication of the 4AM snapshot has not completed, the most recent snapshot available is older than 4 hours, violating the RPO goal. A 2-hour (or more frequent) snapshot schedule would avoid this RPO violation.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1145

Table 125: Configure Snapshot Schedules to be More Frequent

BCN-003	CONFIGURE SNAPSHOT SCHEDULES TO BE MORE FREQUENT THAN THE DESIRED RPO
Justification	Cross cluster replication prevents the instant transfer of snapshot contents, increasing the time before snapshot contents are available.
Implication	Desired RPO may be achievable given technology limitations, or the RPO may need to be adjusted to accommodate replication time.

Table 126: Configure Snapshot Schedules to Retain Lowest Number of Snapshots

BCN-004	CONFIGURE SNAPSHOT SCHEDULES TO RETAIN THE LOWEST NUMBER OF SNAPSHOTS WHILE STILL MEETING THE RETENTION POLICY.
Justification	Metadata space management on a cluster is more efficient with a lower number of snapshots.
Implication	Multiple schedules should be created for the same Protection Domain at different levels rather than a simple daily schedule.

LWS and NearSync Replication

Nutanix offers NearSync with a telescopic schedule (time-based retention). When the RPO is set to be #15 minutes and #one minute, you have the option to specify the maximum retention. The system will automatically roll up intermediate recovery points within the retention window specified, based on the table below. Multiple schedules cannot be created with NearSync.

The following table represents the schedule to save recovery points for 1 month:

Table 127: Schedule to Save Recovery Points

TYPE	FREQUENCY	RETENTION
Minute	Every minute	15 minutes
Hourly	Every hour	6 hours
Daily	Every 24 hours	7 days

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1146

Weekly	Every week	4 weeks
Monthly	Every month	1 month

See Nearsync Requirements and Limitations on the Nutanix Support Portal for more information.

Synchronous Data Transfer

For applications that need to meet an RPO goal of zero (simultaneous data updates at multiple sites), Nutanix supports a synchronous replication option. Configuration of synchronous replication also utilizes Protection Domains as described above.

Configuration of synchronous replication requires a container on the source and destination with the same name. The two clusters participating in synchronous replication are required to be within 5ms round trip time (RTT) of each other.

By default, systems protected synchronously will also automatically create a periodic snapshot schedule. These snapshot references are used to reduce the recovery time in the event that the data must be resynchronized, for example after a WAN outage.

Intermixing Protection Levels

Depending on the version of AOS in use, hypervisor, number of sites, and whether you are using Protection Domains or Protection Policies, the supported configuration may differ. For Protection Domains (Prism Element), refer to the following two tables for supported intermixing of protection levels.

Table 128: Protection Domain Two-Site Support Matrix

REPLICATION TYPE	TWO SITES
Asynchronous	AHV, ESX
NearSync	AHV, ESX
Synchronous	ESX

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1147

Table 129: Protection Domain Multisite Support Matrix

REPLICATION COMBINATION	DIFFERENT ENTITIES	SAME ENTITIES
Multiple asynchronous-only combination (1:N)	AHV, ESX	AHV, ESX
Multiple NearSync-only combination (1:2)	AHV, ESX	ESX**
Multiple synchronous-only combination (1:2)	ESX	Not Supported
Asynchronous + NearSync (1:2)*	AHV, ESX	AHV, ESX
Asynchronous + synchronous (1:2)	ESX	ESX
Synchcronous + NearSync (1:2)	ESX	ESX**
Asynchronous + NearSync + synchronous (1:3)*	ESX	ESX**

* STS only, 5.19 and later

** Supported only with vStore-based data protection.

If you are using Prism Central Protection Policies, the following two tables show the two-site and multisite intermixing support matrix.

Table 130: Protection Policy Two-Site Support

REPLICATION TYPE	2 SITES
Asynchronous	AHV, ESX
NearSync	AHV, ESX
Synchronous	AHV*

* STS only, 5.17 and later

Table 131: Protection Policy Multisite Support Matrix

REPLICATION COMBINATION	DIFFERENT/SAME ENTITIES

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1148

Multiple asynchronous-only combination (1:N)*	AHV, ESX
Multiple NearSync-only combination (1:2)	AHV, ESX
Multiple synchronous-only combination (1:2)	Not Supported
Asynchronous + NearSync (1:2) *	AHV, ESX
Asynchronous + synchronous (1:2)	Not Supported
Synchronous + NearSync (1:2)	Not Supported
Asynchronous + NearSync + synchronous (1:3)	Not Supported

* STS only, 5.19 and later

For additional details, see Data Protection and Recovery with Prism Element on the Nutanix Support Portal.

In all cases, a failover action causes all items within the identified PD to be made available at the remote site as a collective unit. Only related entities should be grouped into a PD.

Table 132: Group Applications Together in Unique Protection Domains

BCN-005	GROUP APPLICATIONS TOGETHER IN UNIQUE PROTECTION DOMAINS. KEEP NUMBER OF VM'S PER PROTECTION DOMAIN AS SMALL AS REASONABLY POSSIBLE
Justification	Small groupings of related entities help minimize accidental collateral damage during a partial failover and reduce the need to track complex intermingled scheduling.
Implication	Entire site failover will require activating a larger number of Protection Domains, potentially increasing the time required to bring all entities online.

Nutanix Disaster Recovery

Protection domains are a construct within Prism Element. One limitation is that protection domains don't provide additional controls around VMs associated with a large-scale failover, like start order control or changing the VM IP address due to site change.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1149

Nutanix Disaster Recovery (formerly Leap) supports more advanced constructs relating to replication and failover.

Protection policies offer a way to configure replication grouping using categories. VMs that match a category are automatically protected; in a protection domain you must add them manually.

Nutanix Disaster Recovery also provides recovery plans. Recovery plans can help you control the failover process, allowing you to perform the following operations:

- Specify start order
- Map networks when using DHCP
- Change static IPs for sites that don't have access to stretched L2 networking
- Run scripts to perform in-guest actions as part of failover (if necessary)
- Perform test failovers and validation of the configuration without downtime

Full coverage of Nutanix Disaster Recovery is out of scope for this document. For more information, see the Nutanix Disaster Recovery Guide.

Additional Options

Nutanix offers additional options for ensuring business continuity that are beyond the scope of this design.

- Nutanix DRaaS: Nutanix (or partner) hosted datacenters provide a DRaaS option. Using DRaaS, data replicates to a managed cloud service location in the same way it would replicate to an on-premises disaster recovery location.
- Nutanix Mine: As part of the conceptual 3-2-1 rule, Nutanix supports multiple backup vendors that can integrate via API to offload backup. Mine offers a bundle of backup vendor software and Nutanix platform to provide storage for the retention of backup data, independent of the primary cluster(s) in use.

Disaster Recovery Decision Tree

A good DR solution should involve different levels of service for DR because applications will have different levels of criticality to the business and therefore different requirements for their disaster recovery needs. As a result, this

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1150

document will include multiple architectures specific to meet a variety of scenarios that as a group can be configured to meet the requirements for all application needs. The following flow chart walks through the decision tree for choosing the best Nutanix DR solution to meet your requirements. Each DR solutions is discussed in the sections that follow.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1151

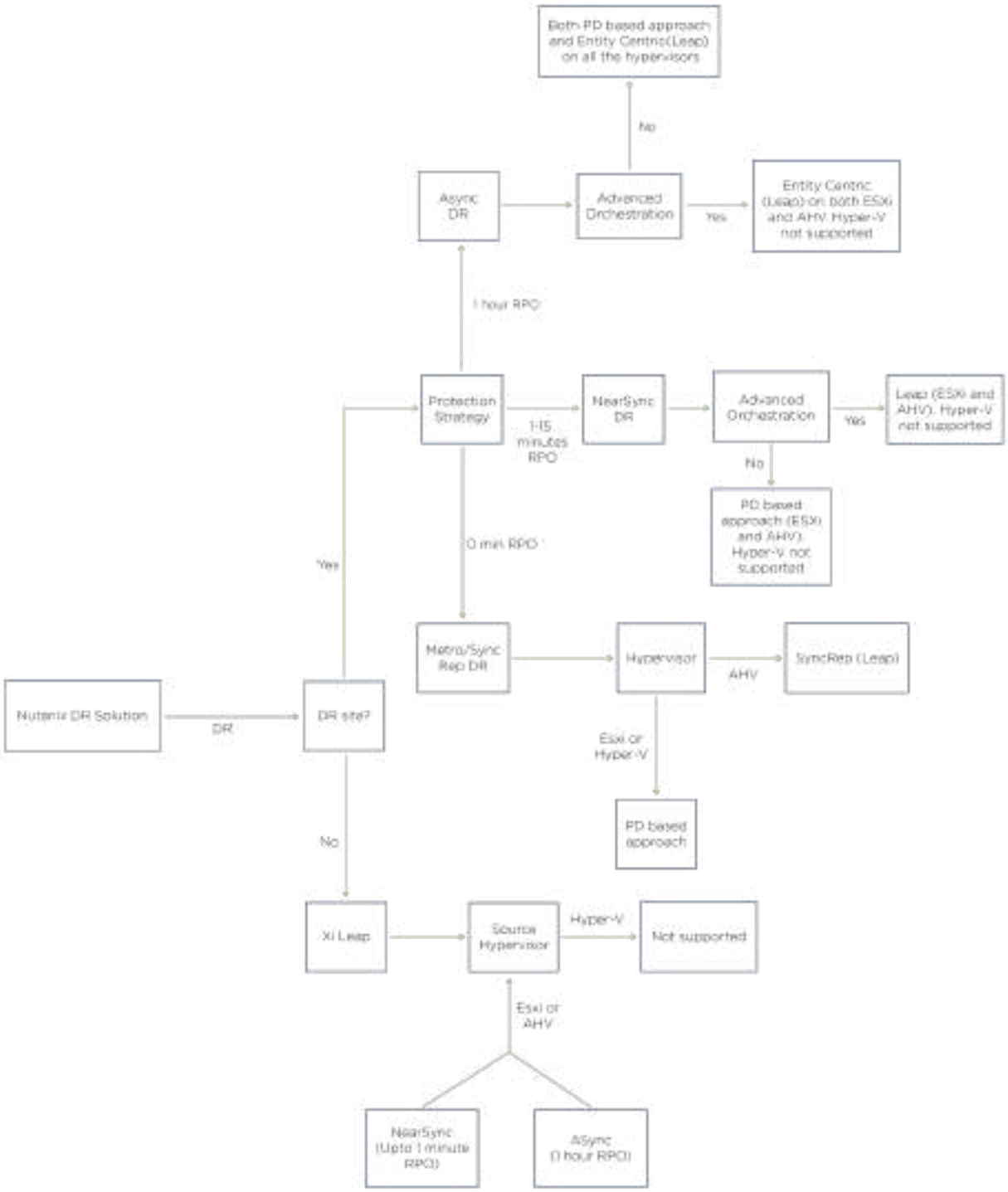


Figure 60: Disaster Recovery Decision Tree

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1152

Nutanix DR solutions

Nutanix Metro Availability

Metro Availability (MA) allows vSphere administrators to leverage hypervisor clustering technology across datacenters. This type of configuration presents two distinct Nutanix cluster to vSphere as a single stretched cluster, and it helps to minimize downtime during unplanned outages. In the event an entire site goes down, vSphere HA automatically starts the virtual machines on the secondary site if a witness has been properly configured.

This configuration is the most complicated choice, requiring stretched layer 2 networking of some form between sites. In addition, while this provides the most rapid failover, the configuration is highly dependent on the network connectivity being resilient and providing a high enough throughput to accommodate application change rates. Systems with frequent intermittent network issues may be better served via a NearSync style connection that is less impacted by network drops.

See the Metro Availability Guide on the Nutanix Support Portal for more information.

Table 133: Application Requires RPO

BCN-006	APPLICATION REQUIRES RPO=0 AND RTO NEAR ZERO
Justification	Business critical applications requires zero data loss and minimal to zero recovery time.
Implication	Nutanix MA requires high bandwidth and low latency (under 5ms). To comply with near 0 RTO, stretched layer 2 networks are required. Nutanix MA is supported only with VMware ESXi, which may bring additional management overhead and increase licensing costs.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1153

Table 134: Application Requires Zero Downtime

BCN-007	APPLICATION REQUIRES ZERO DOWNTIME DR AVOIDANCE SOLUTION
Justification	Business critical application requires zero data loss and zero recovery time during DR avoidance event.
Implication	Nutanix MA requires high bandwidth and low latency (under 5ms). To comply with ZERO downtime during DR avoidance, stretched layer2 networks are required. Nutanix MA is supported only with VMware ESXi, which may bring additional management overhead and increase licensing costs. Nutanix AOS enterprise license is required. With Nutanix Metro Availability you can protect entire datastore. You cannot choose VM to protect.

Synchronous replication

Nutanix synchronous replication is available with Nutanix AHV (using Nutanix Disaster Recovery and AOS 5.17 or later) or VMware vSphere. With synchronous replication workloads are protected with RPO=0. Synchronous replication is used when you cannot provide spanned L2 across datacenters (required by Metro Availability) but still need to provide RPO=0 to applications.

Table 135: Application Requires RPO

BCN-008	APPLICATION REQUIRES RPO=0
Justification	Applications require 0 RPO and minimal RTO.
Implication	Nutanix synchronous replication requires high bandwidth and low latency (under 5ms) datacenter connectivity. Nutanix synchronous replication with AHV is supported only with Nutanix Disaster Recovery. It requires an AOS enterprise license or a Nutanix Disaster Recovery Advanced add-on license.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1154

NearSync replication

NearSync replication enables you to protect your data with an RPO as low as 1 minute. You configure a Protection Policy with NearSync replication by defining the VMs or the Categories of VMs. The policy creates a Recovery Point of the VMs in minutes (1–15 minutes) and replicates it to the recovery site.

Table 136: Provide RPO Between 1 and 15 Min

BCN-009	PROVIDE RPO BETWEEN 1 MIN AND 15 MIN TO AN APPLICATION
Justification	Provide low RPO to storage intensive workloads over limited connectivity.
Implication	A cluster is NearSync capable if the capacity of each SSD in the cluster is at least 1.2 TB. All-flash clusters do not have any specific SSD sizing requirements. NearSync replication with AHV is supported only with Nutanix Disaster Recovery, and it requires an AOS enterprise license or a Nutanix Disaster Recovery Advanced add-on license.

Asynchronous replication

Nutanix asynchronous replication enables you to protect your data with an RPO of 1h or more. You can configure a Protection Policy or Protection Domain with asynchronous replication by defining the VMs or the Categories of VMs. The policy or protection domain scheduler creates a recovery point of the VMs in minutes (60 minutes) and replicates it to the recovery site.

Table 137: Application Requires RPO

BCN-010	APPLICATION REQUIRES RPO=>1H
Justification	Provide RPO=>1h to the application utilizing low bandwidth\high latency datacenter links.
Implication	Nutanix asynchronous replication requires an AOS enterprise license or Nutanix Disaster Recovery Advanced add-on license.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1155

Disaster Recovery Patterns

One-to-One

For smaller environments with only a pair of locations, protect applications between two availability zones. Availability zones can be the same region or across regions. The same workload or application can be protected with different RPO thresholds. Choosing availability zones locations (same region or across regions) defines RPO value for protected application\workloads. If application or workload requires RPO=0, choose availability zones in the same region (latency requirement for RPO=0 is 5ms RTT or less).

1. Two AZ within the same region

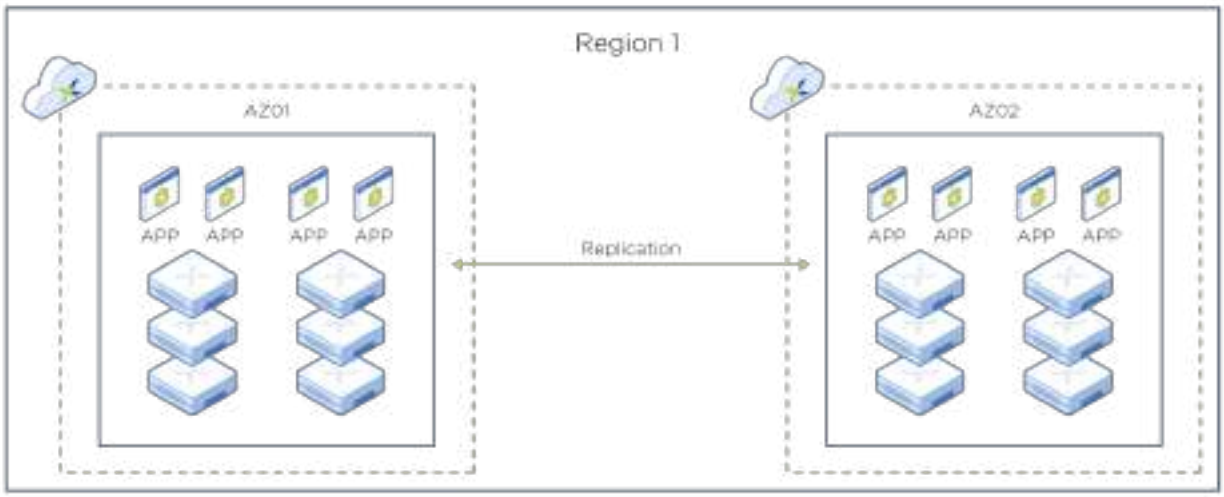


Figure 61: Two AZ within the Same Region

1. Two AZ across multiple regions

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1156

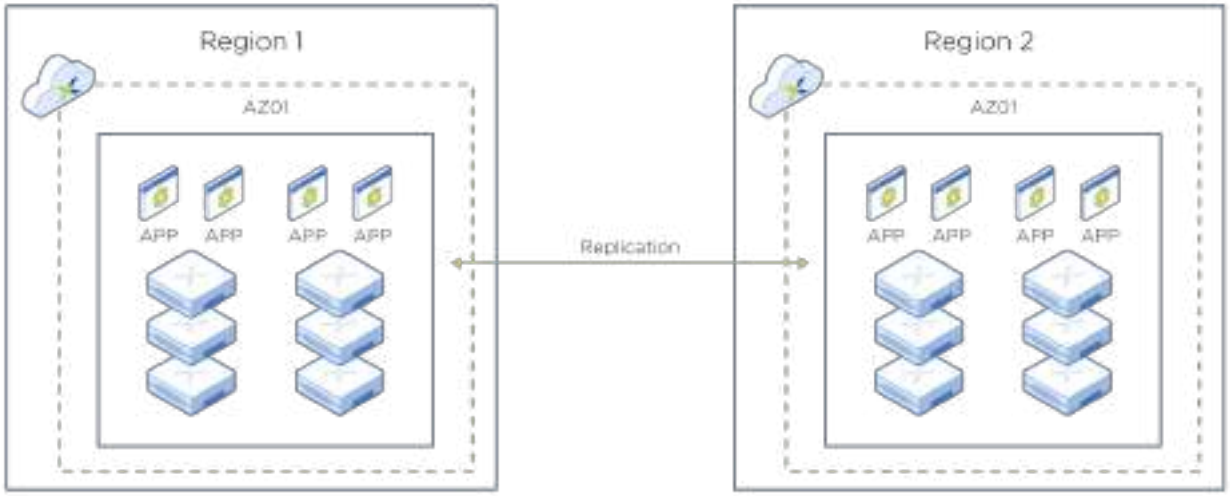


Figure 62: Two AZ across Multiple Regions

1-to-Many

The 1-to-Many DR pattern maps a single source Nutanix cluster to multiple DR target Nutanix clusters. This use case is applicable where an application requires multiple levels of data protection and at the same time providing high uptime and minimal to zero data loss. Availability zones can be located within the same region or across multiple regions. Choosing the availability zone location (same region or across regions) defines minimum RPO value for protected application \workloads.

If an application or workload requires RPO=0 and protection against natural disasters like hurricanes or earth quakes, choose an availability zone in the same region to provide RPO=0 (latency requirement for RPO=0 is 5ms RTT or less) and second availability zone in different region (to provide application resiliency against wide spread natural disasters like hurricanes, floods or earth quakes).

1. Multiple AZ within a single region

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1157

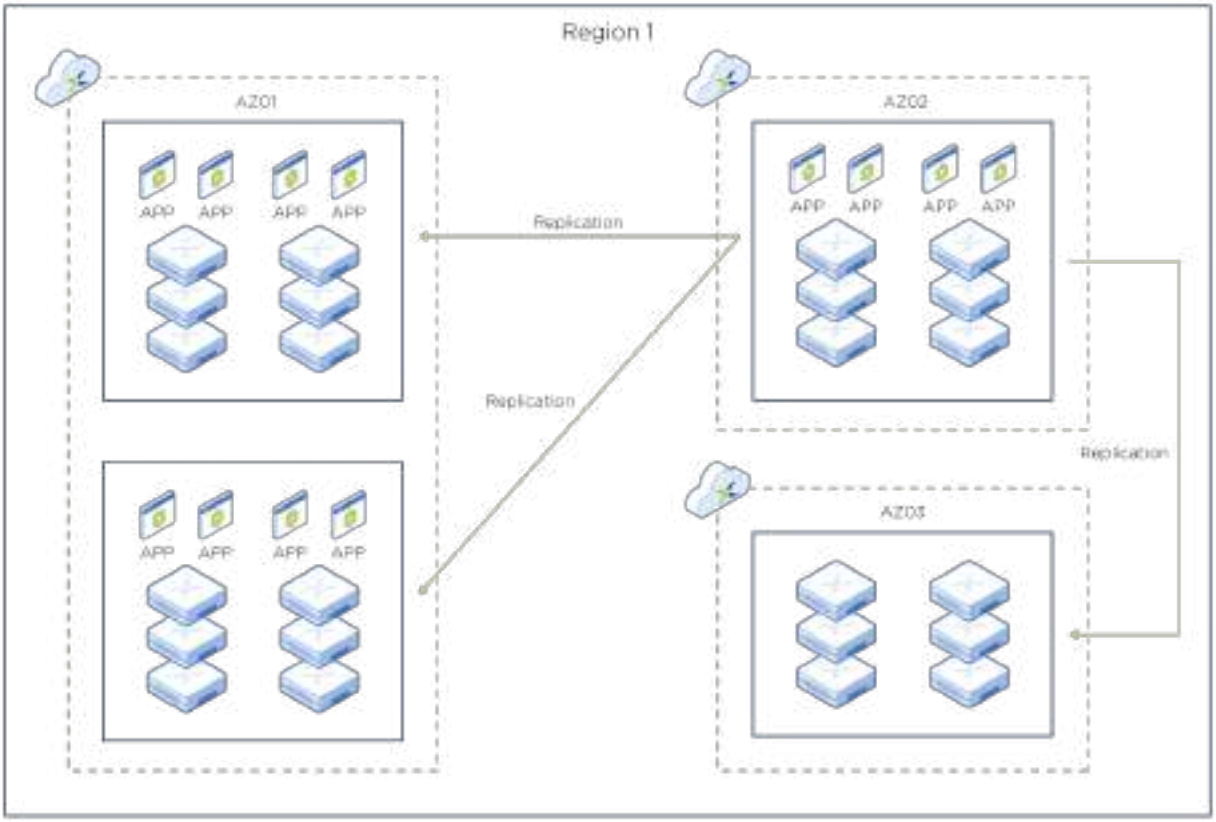


Figure 63: Multiple AZ within a Single Region

1. Multiple AZ across multiple regions

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1158

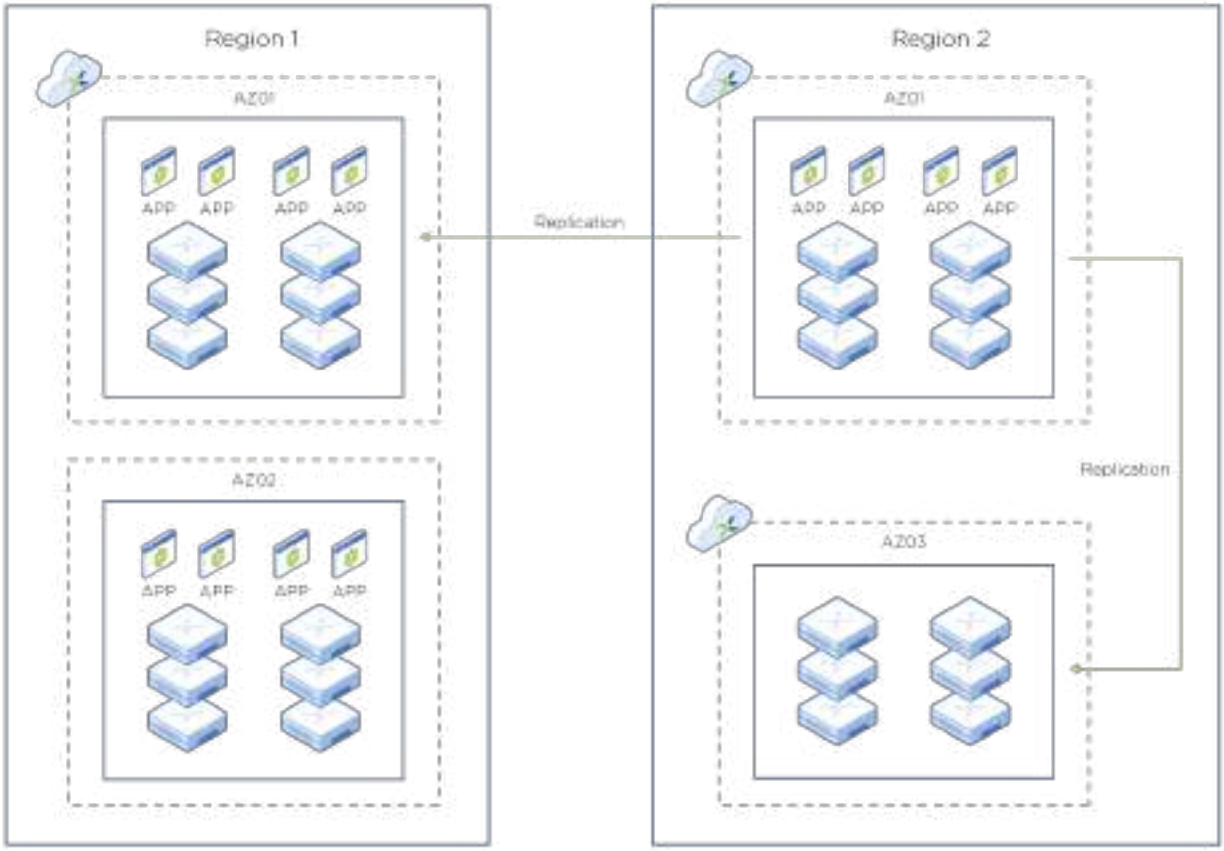


Figure 64: Multiple AZ across Multiple Regions

Many-to-1

The Many-to-1 DR pattern maps multiple source Nutanix clusters to single DR target Nutanix cluster. The best use case for the many-to-1 DR pattern is to protect multiple ROBO locations to a single Nutanix target in a DR hub, which is usually located in a regional or GEO datacenter. Each ROBO location is a separate availability zone which replicates data to the DR hub (which is located in separate availability zone) but the same region.

1. Multiple AZ within a single region

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1159

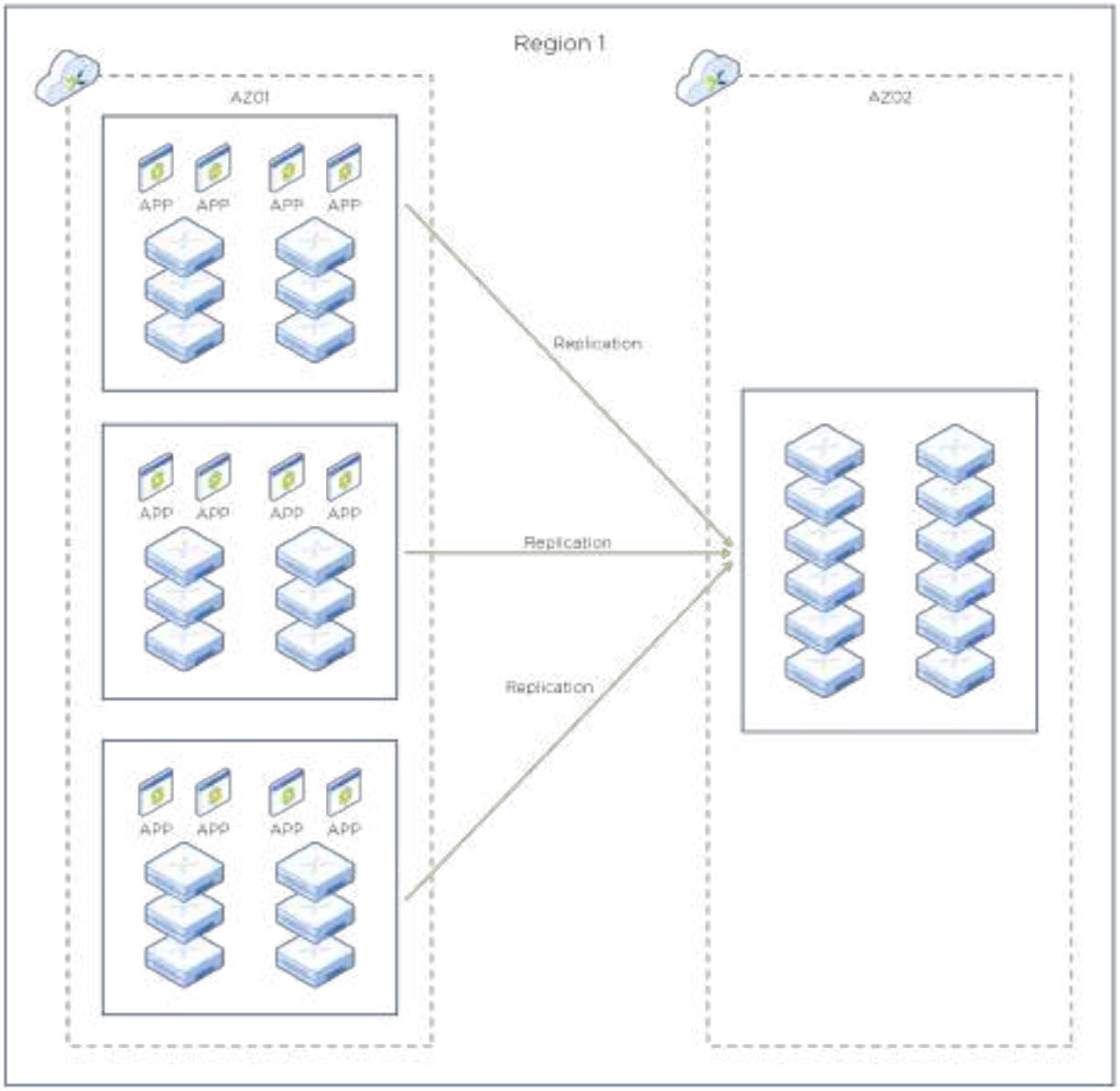


Figure 65: Multiple AZ within a Single Region

1. Multiple AZ across multiple regions

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1160

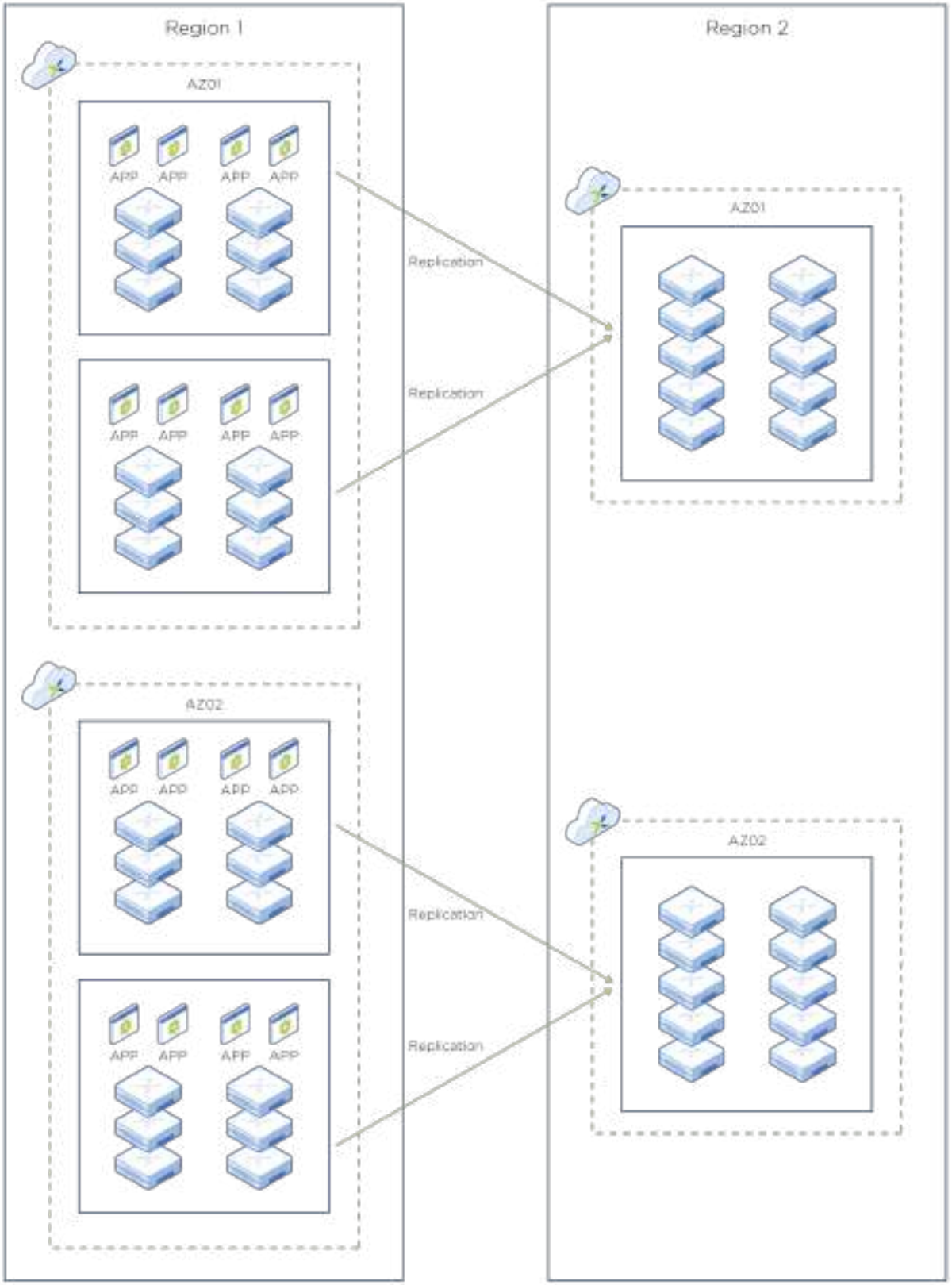


Figure 66: Multiple AZ across Multiple Regions

© 2023 Nutanix, Inc. All rights reserved

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1161

Many-to-Many

Description

The Many-to-Many DR pattern maps multiple source DR clusters with multiple target DR Nutanix clusters.

This pattern is suitable to applications which can run concurrently in more than one location. These applications which are require zero data loss and zero to minimal downtime. Leveraging multiple RPO schedules (synchronous, asynchronous, and nearsync) you can protect each application\workload with the most appropriate method to meet availability requirements.

1. Single region

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1162

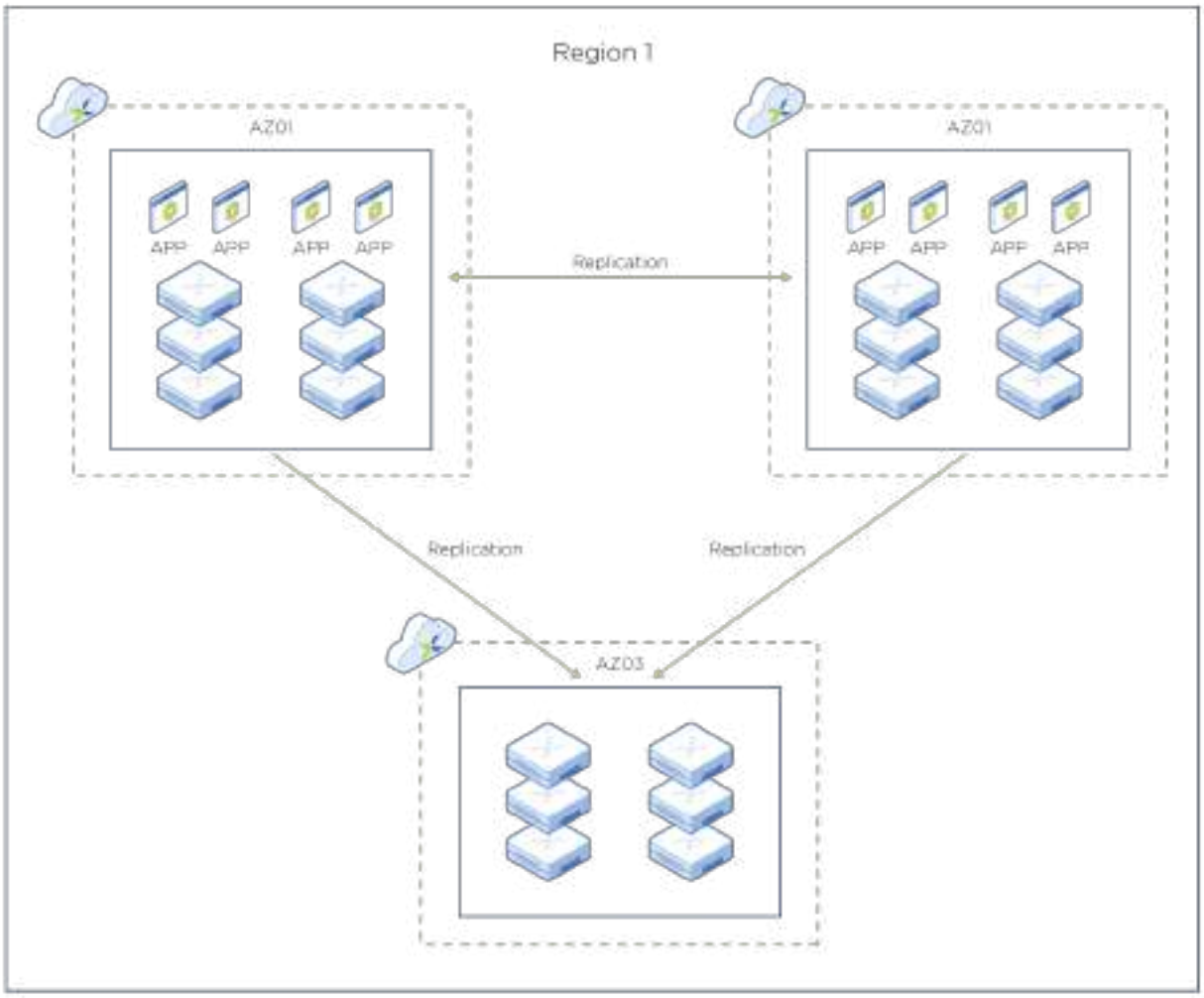


Figure 67: Single Region

1. Multiple regions

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1163

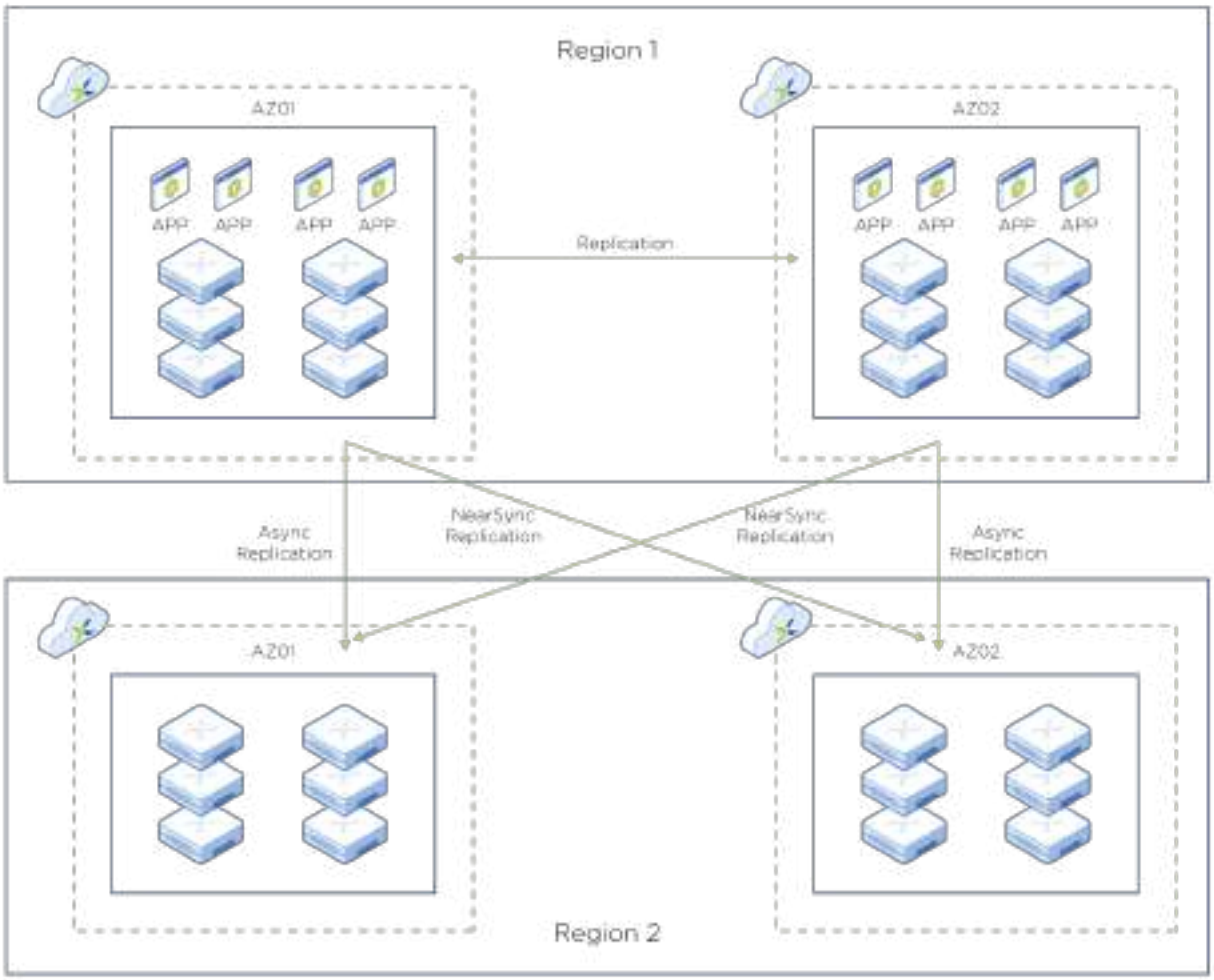


Figure 68: Multiple Regions

ROBO Patterns

For remote and branch offices, there are specific architectural considerations. For sites using three or more nodes in a cluster, the operation of that cluster is similar to a datacenter, while typically constrained by bandwidth, latency, and facilities limitations.

Nutanix supports a limited number of models in either a single-node (no high availability) or two-node (basic high availability) configuration. These configurations are suitable for small-footprint sites running a limited number of

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1164

VMs (from 5 to 10, depending on load). A two-node solution offers the same capacity sizing options as one node, while allowing for failover if one of the nodes goes down. Automatic failover of VMs requires connecting the two-node cluster with a remotely hosted witness VM.

In addition, there are limitations on feature support related to one-node and two-node clusters. Some of the most relevant limitations include the following:

- Lack of expandability (cannot grow to three nodes or larger without running Foundation again)
- Limited VM sizing capacity due to limitations of the supported hardware models
- RPO support of at least 6 hours

For ROBO sites, these options and limitations create a decision point. One-node and two-node solutions are appropriate for systems where a limited feature set and reduced availability still meet necessary requirements. Because these clusters have eight nodes or fewer, you can use 1 Gbps switches. With this more economical server and networking equipment choice, you can achieve a lower price point compared to high-performance datacenter clusters with three or more nodes.

An additional option is per-VM ROBO licensing, where the physical hardware is still composed of three or more hosts. Each VM is explicitly licensed and limited to 32 GB of RAM.

Table 138: Decide on Cluster Licensing Model

DCD-001	DECIDE ON CLUSTER LICENSING MODEL (CBL OR PER VM)
Justification	The two licensing models cannot be mixed on a single cluster.
Implication	Per-VM ROBO licensing model allows for greater hardware capacity and feature set capabilities, while potentially increasing the footprint and hardware cost.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1165

Table 139: Decide on Cluster Type Used

DCD-002	DECIDE ON CLUSTER TYPE USED (IF NOT ROBO PER VM)
Justification	One-node and two-node clusters are restricted to specific models. Clusters with three or more nodes are not restricted.
Implication	Limitations imposed by a one-node or two-node solution cannot be corrected later (in place) by upgrading to three or more nodes.

Fan Architecture

In a fan-in and fan-out architecture, multiple ROBO sites are configured to replicate data back to a centralized location. The main location is normally larger, with enough capacity to meet the storage requirements for all the remote sites' expected replication and retention needs.

When building out a central location, at a minimum it needs enough storage capacity to accommodate the data from each ROBO site that requires protection. An important decision is whether to provide compute capacity to actively sustain the workload in the central site in a disaster recovery scenario, or only to provide capacity to store the data.

Table 140: Decide Whether to Provide Compute for ROBO Failover

DCD-003	DECIDE WHETHER TO PROVIDE COMPUTE FOR ROBO FAILOVER
Justification	A data replication only ROBO DR strategy will be sustainable by a smaller number of data dense storage nodes. An active failover capable ROBO DR strategy will require additional compute capacity to bring the failed services online in the event of a disaster.
Implication	Failover compute capacity must be reserved, potentially increasing solution cost and footprint.

Table 141: Decide on ROBO Failover Compute

DCD-004	DECIDE ON ROBO FAILOVER COMPUTE OVER COMMIT

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1166

Justification	The recovery site will likely only have to provide compute failover capacity for a limited number of concurrent site failures.
Implication	For a centralized location serving many ROBOs, the added cost of failover hardware may be relatively modest and worth the investment.

DR Pairing

For configurations lacking a centralized replication target, an alternative is to create replication partner sites. These sites are typically within a region/availability zone and may have improved network speeds between sites (for example via metro ethernet) versus to a main datacenter. Each of the paired sites should be far enough apart from each other to support recoverability requirements in the event of a disaster.

This configuration can also be used for ROBO in a different country/legal entity than the main datacenter, where data privacy laws make replication back to a larger datacenter impossible.

Control Planes

Control plane design in a multi-site environment is a delicate balance between having a centralized view of everything versus a completely disaggregated view. This design suggests striking a balance, with separate control planes when necessary, to meet availability and product (e.g. VMware SRM or Prism Central) requirements.

vCenter

The guidance for vCenter placement in a multi-datacenter environment is to generally keep the vCenter instance and the clusters its managing within the same availability zone. An exception to this is in ROBO designs where having a vCenter at each remote site is not always desirable since it lacks a single management point for a larger number of sites.

If protecting workloads across availability zones—whether in the same region or across regions—you need to have at least a single vCenter to manage workloads at the source and target sites. This allows for Nutanix DR playbooks or VMware Site Recovery Manager (SRM) to automate the failover of these workloads.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1167

Prism Central

The guidance for Prism Central (PC) placement is to have at least one PC deployment within each availability zone depending on the number of VMs. This allows the PC instance to manage local clusters and resources while utilizing DR runbook automation to connect to PC instances in other regions for protecting workloads. Having separate PC instances at the source and target locations is a requirement for DR runbook automation available within PC. The only time you would deploy more than one PC per availability zone is when you scale past the limits of a single PC.

There are only two situations where you might consider having a PC instance manage clusters in other availability zones:

- ROBO architecture where each site typically has a small cluster and it's desirable to have a single central PC instance to manage them.
- If you have multiple AZs and are not replicating between them, they can be managed by a single PC instance.

Multi-DC Networking

Networking is critical for disaster recovery, since the network forms the backbone carrying all replicated data. Each component in the path from the physical layer of the source cluster, to the physical layer of the destination cluster must be considered. Especially important are the site-to-site links that connect protected sites.

Each Nutanix replication technology has specific requirements to ensure that the connection between sites has sufficient bandwidth, low enough latency, and meets redundancy requirements. Please note that the formulas below do not take into account link latency, and as such, replication over links with high latency can see significantly reduced performance.

The following table summarizes the required networking characteristics for each replication type:

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1168

Table 142: Required Networking Characteristics

REPLICATION TYPE	LATENCY REQUIREMENTS	BANDWIDTH CALCULATION	NOTES
Async DR	NA	Bandwidth needed = (RPO change rate * (1 - compression on wire savings %)) / RPO Max of 800mbps per node	
Near Sync DR	NA	Bandwidth needed = (RPO change rate * (1 - compression on wire savings %)) / RPO Max - Unbounded	
ESXi Metro Availability	Sites: 5msec RTT Witness: 200msec	Metro Container data change rate Max - unbounded	Redundant site links recommended Witness: Separate links
AHV Synchronous Replication	Sites: 5msec RTT	Data change rate Max - unbounded	Redundant site links recommended

In addition to the characteristics of the network transport between protected sites, careful attention must be paid to the VM networking at each site. When a workload moves from one site to another there are many possible options for maintaining workload connectivity to the required customers or endpoints.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1169

Technologies like stretched networking, load balancing, NAT, and more should be considered to provide seamless replication and application connectivity.

Bandwidth Requirements

Replicating data between sites requires that enough bandwidth is available to replicate all of the data changed during the RPO window within the RPO interval. Refer to the Data Protection and Disaster Recovery Guide for a complete explanation of bandwidth calculation.

Calculate this data change rate for both asynchronous and NearSync replication. Here is an example of the bandwidth needed for an RPO of 1 hour with 15GB of data changed during that hour. We assume 30% savings for compression.

Table 143: Bandwidth Needed for an RPO

BANDWIDTH NEEDED = (RPO CHANGE RATE * (1 - COMPRESSION ON WIRE SAVINGS %)) / RPO
Example:
RPO: 1hr (3,600s)
RPO Change Rate: 15GB
Compression Savings: 30%
(15GB * (1 - 0.3)) / 3,600s
(15GB * 0.7) / 3,600s
10.5GB / 3,600s
(10.5GB * 1,000 MB/GB * 8 bits/byte) / 3,600s - converting to Mb/s
84,000 Mb / 3,600s = 23.33 Mb/s
Bandwidth needed = 23.33 Mb/s

The bandwidth needed is easier to calculate when the RPO is zero, since it is equal to the data change rate. Data will be compressed before being sent to another site, so assume compression in this calculation as well.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1170

Table 144: Calculate Required Storage Replication Bandwidth

MULTI-NET-001	CALCULATE REQUIRED STORAGE REPLICATION BANDWIDTH BASED ON RPO.
Justification	Bandwidth must be available to keep up with data change rate and meet the desired RPO.
Implication	Achieving the desired RPO can require significant bandwidth and requires knowledge of the workload's current usage.

In addition to storage replication between sites, bandwidth must be allocated for workload traffic and application level replication traffic. First determine how much workload traffic and application replication traffic will exist. This is largely dependent on the applications in use. Next determine if there are any priority or latency requirements that are unique to the applications. Applications with latency sensitive traffic may require WAN quality of service, or even dedicated WAN links.

Table 145: Calculate Application Specific Bandwidth

MULTI-NET-002	CALCULATE APPLICATION SPECIFIC BANDWIDTH.
Justification	WAN links must also carry application level replication traffic and application traffic.
Implication	Critical application traffic may require more WAN links or WAN quality of service policies.

Latency Requirements

Latency between protected sites will have an impact on the speed of data replication. Latency is a function of physical distance, network cabling plus equipment, and the speed of light.

Asynchronous DR has no minimum network latency requirements as long as the bandwidth requirements can be met. This makes asynchronous replication a great choice for protecting sites a long distance apart such as between regions.

Near-sync DR also has no fixed requirement for minimum latency between sites, but the bandwidth requirement must be met.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1171

Metro Availability has two separate requirements for network latency, one between the protected sites, and another between the protected sites and the optional witness. Between protected sites the latency must be less than 5 milliseconds round trip, or 2.5 milliseconds one way. The sites must therefore be located relatively close to each other, but in separate availability zones. Each protected site must also have a connection to the witness that is within 200 milliseconds or less to allow for reliable message exchange during site failures.

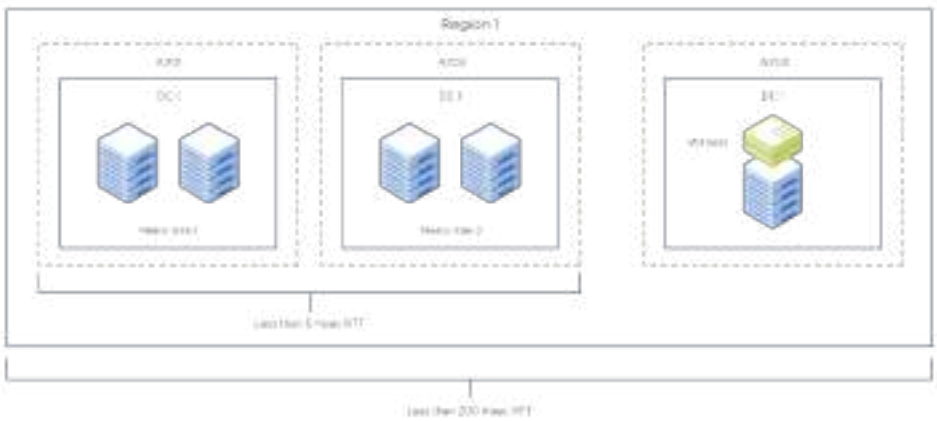


Figure 69: Latency Requirements

Every bit of latency on a link between Metro Availability sites also affects storage write latency for workloads. Keep this latency as low as possible by choosing MA sites that are as close to each other as possible while still providing the necessary physical resilience. In this guide we assume that MA sites exist within the same availability zone, but the witness can be in another AZ, or even in another region.

Table 146: Place Metro and Synchronous Replication Sites within the Same Region

MULTI-NET-003	PLACE METRO AND SYNCHRONOUS REPLICATION SITES WITHIN THE SAME REGION WITHIN 100KM OR LESS THAN 5MSEC RTT
Justification	Latency on metro links is directly added to storage write latency.
Implication	Metro Availability site design must consider physical location carefully.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1172

Table 147: Place Metro Witness within 200msec

MULTI-NET-004	PLACE METRO WITNESS WITHIN 200MSEC
Justification	Sites must receive responses from the witness to determine failure handling.
Implication	Witness can be relatively far from protected sites.

Separating DR Traffic

Nutanix does not recommend isolating DR traffic on separate WAN links because it adds complexity, but if security or business requirements dictate a separated WAN, keep the following in mind.

Consider the scenario where a company has several separate links between protected sites where some are for low latency applications that take high priority. This customer may decide to also purchase an entirely separate physical link between sites that is for higher bandwidth replication traffic that is not latency sensitive and at a lower cost. In essence this is a form of QoS for the application. The customer can ensure that critical application traffic is never stopped by lower priority replication traffic.

It's also possible that the reverse is true for a case like Metro Availability, where certain application and storage replication traffic may take higher priority than other application traffic, and we dedicate an entire WAN link to this storage traffic.

In these cases, the desire is to segment traffic for one purpose over one WAN link between sites, and traffic for another purpose over another link between sites. There are several ways to achieve this goal.

Network Segmentation in the Nutanix CVM

Network Segmentation in the CVM creates another virtual NIC on the CVM and the hypervisor, allowing the separation of user, replication, and DR traffic to different VLANs or physical interfaces. Every CVM and every host needs additional IP addresses in this method, so the configuration for each host becomes slightly more complex.

Network Routing: Manual or Policy Based

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1173

Using network routing, the network devices use criteria like source and destination address, and even TCP ports to determine which link is used for routing traffic. This method requires more advanced network configuration but simplifies the CVM and host configuration.

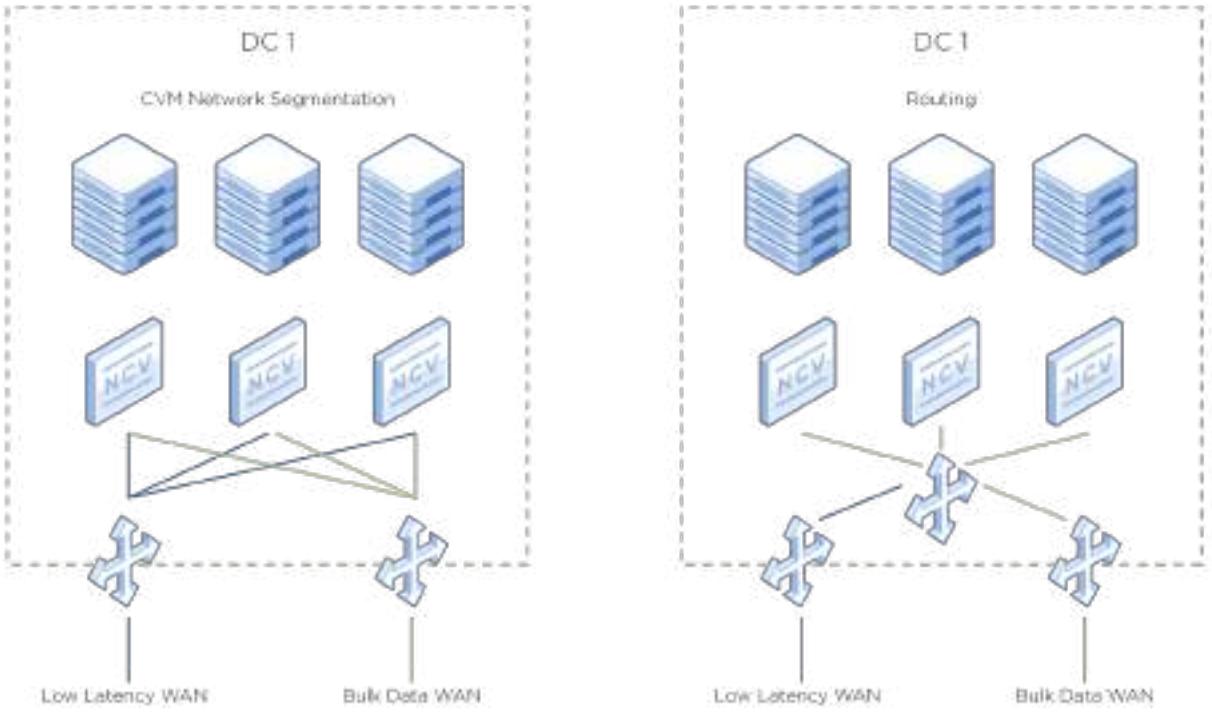


Figure 70: Network Routing

Table 148: Do Not Use Network Segmentation for DR

MULTI-NET-005	DO NOT USE NETWORK SEGMENTATION FOR DR UNLESS REQUIRED. ROUTING SEGMENTATION IS PREFERRED OVER CVM SEGMENTATION
Justification	Network segmentation in the CVM and host adds complexity that must be managed during the system lifecycle.
Implication	Unless specifically required to do otherwise, traffic from applications and DR will share the same network links.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1174

Network Redundancy

Ensure there are redundant paths between protected sites and minimize or eliminate single points of failure. This prevents the failure of a single networking component from stopping replication of storage and application traffic. At each network hop between two protected sites, evaluate whether failure of that component would be gracefully handled, or if would lead to an outage.

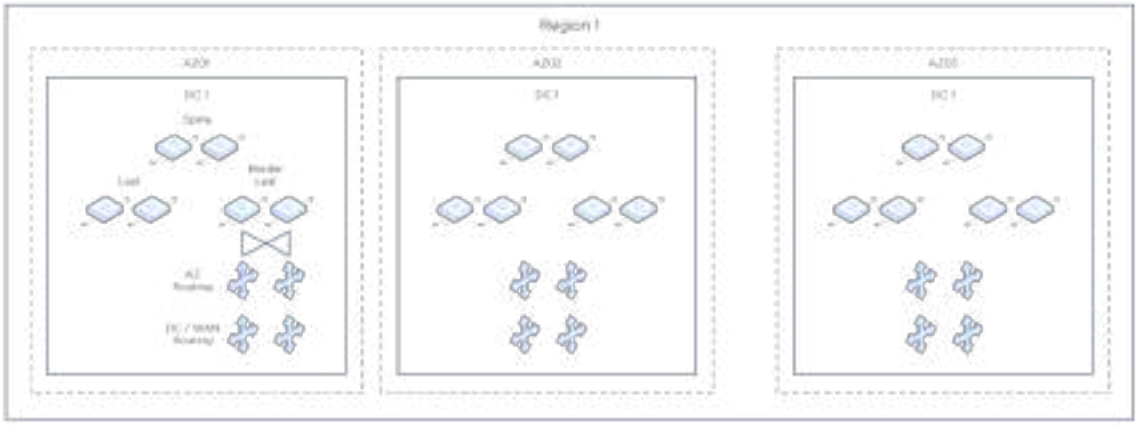


Figure 71: Network Redundancy

For example, in the path between two sites connected over a WAN we have the following components:

- Site 1: Top-of-rack switch (leaf)
- Site 1: Spine switches
- Site 1: Border leaf
- Site 1: DC router
- Site 1: WAN router
- Site 2: WAN router
- Site 2: DC router
- Site 2: Border leaf
- Site 2: Spine switches
- Site 2: Top-of-rack switch (leaf)

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1175

This means we need to ensure redundancy in the following components:

Top-of-rack switch

Ensure that each Nutanix host in every cluster is connected to at least two top-of-rack switches.

Spine switch

Ensure that there are at least two spine switches, and that all leaf switches are connected to all spine switches.

Border leaf

The border leaf is where external services such as routing connect. Ensure that there are at least two border leaf switches, and that they connect to all spines. The border leaf switches should connect to at least two routers, to allow redundant external routing.

DC router

Depending on the size of the deployment, there will be one or more levels of routing between the rack networks and the WAN edge. Each routing tier should provide high availability to allow external routing from the racks to the rest of the DC.

WAN router

The WAN router provides connectivity external to the datacenter. These should be deployed in a redundant fashion, allowing for the failure of any single routing component.

The WAN also presents a special case for WAN Link redundancy. In addition to providing multiple WAN routers, designs should use multiple WAN links, potentially from different network providers.

The WAN provider may be an external entity, or in the case of connection between sites within a campus, they may be entirely within the control of one entity. In these cases where the links are under your control, it is still desirable to use multiple separate physical connections, such as separate fiber links between sites. It's desirable to route these links to the WAN through separate physical paths to protect against ground or aerial utility faults (such as backhoes). It may not always be possible to use different physical paths based on datacenter

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1176

location, design, or infrastructure provider constraints. Where a single point of failure exists, it should be well documented and understood. One example could be a single piece of conduit carrying multiple WAN links inside it between datacenters.

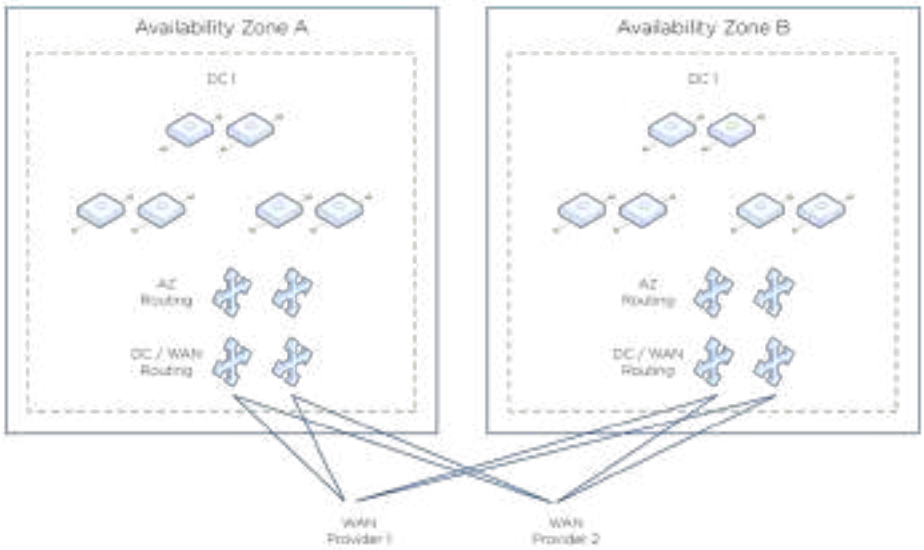


Figure 72: Single Piece of Conduit with Multiple WAN Links

Testing is an important part of the redundancy in any system and networking is no exception. Create and maintain a regular schedule to test the redundancy of each individual component such as routers and switches. Maintenance such as vendor software upgrades and patches as well as regular power maintenance provide great opportunities to verify the resilience during planned single component outages.

Table 149: Ensure Redundancy of Each Network Device

MULTI-NET-006	ENSURE REDUNDANCY OF EACH NETWORK DEVICE. TRACK THE COMPLETE NETWORK PATH BETWEEN PROTECTED SITES
Justification	Failure of a single component must not lead to connectivity failure between protected sites.
Implication	Redundant components must be purchased and configured for high availability and failover.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1177

Table 150: Create and Follow a Redundancy Test Plan

MULTI-NET-007	CREATE AND FOLLOW A REDUNDANCY TEST PLAN. CAPTURE NETWORK COMPONENTS IN PLAN
Justification	High availability configurations are often complex and must be tested to ensure they work as expected.
Implication	Regularly scheduled maintenance must include additional protocols to test network components during this time.

Witness Path Requirements

Using Metro Availability with a witness creates resiliency requirements between the protected sites and the witness site.

First, the witness should be at a separate site from either of the protected sites. This allows the witness to monitor the availability of both sites independently and means that the witness should survive the failure of one of the protected sites. The witness provides no extra benefit if it goes down during a site failure.

In addition, the network path between the protected sites should be a separate path from the path to reach the witness. That means each protected site should have at least two routing paths, one to reach the witness, and another to reach the other protected site.

Finally, the connection between the protected site and the witness site should have no more than 200msec of latency. This helps ensure timely event handling during a failure scenario.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1178

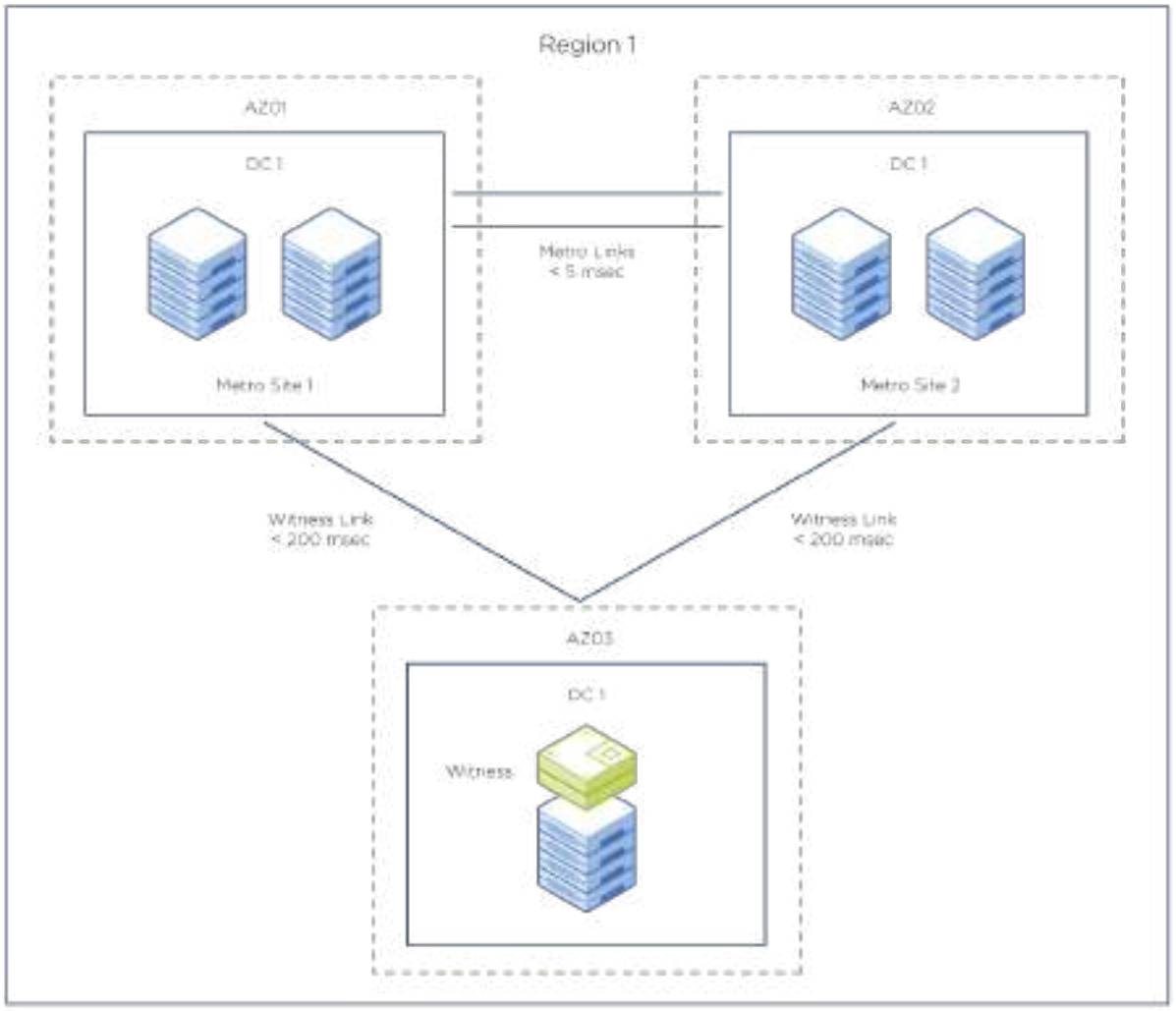


Figure 73: Metro Witness Link Requirements

Table 151: Ensure that the Link Between Protected Sites and a Witness does not Use the Link Between Sites

MULTI-NET-008	ENSURE THAT THE LINK BETWEEN PROTECTED SITES AND A WITNESS DOES NOT USE THE LINK BETWEEN SITES.
Justification	The path to the witness should be a separate, protected link. The witness should be reachable during failures of the link between the protected sites.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1179

Implication	Additional WAN connectivity may be required to maintain a separate external connection to the witness.

Workload Networking

In addition to transporting critical storage traffic, the network also provides access to running applications. During site failures it's important to consider how the application or workload will provide constant access for clients, even when the workload may be running in a secondary location.

IP Address Assignment

There are two approaches for managing workload connectivity during site failures.In the first approach, workloads keep their existing IP addresses and the network provides connectivity in the backup site even when using previous IP addresses. In the second approach, workloads fail over to the second site and receive new IP addresses belonging to the backup site.

The network tools used are outside the scope of this document but consider the following when moving workloads between sites using these tools. The workload and the network capabilities will determine the chosen method.

Case 1: Workloads keep the same IP address

Preserving the IP addresses of workloads during failover is helpful for several reasons. No change is required inside the workloads, which may sometimes not even support IP address changes. This also means any scripts or infrastructure that rely on hardcoded IP addresses will continue to function. The network infrastructure seamlessly handles the transition by migrating the network to the new site, or by maintaining a stretched network at all times. The responsibility of failover reachability is shifted away from the application and to the network.

The following approaches are frequently used to preserve IP addresses:

- Stretched layer 2 networks
- NAT
- Layer 3 route advertisement updates

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1180

Case 2: Workloads receive a new IP address

Provisioning workloads with new IP addresses allows more network flexibility, for instances where moving a network between sites is not feasible. When the workload easily supports IP address changes, or if the network does not support network mobility, changing workload addresses may be the best option. Using a tool to automate these address changes ensures a smooth recovery.

The following tools are often used to provision new addresses at the DR site.

- DHCP / IPAM
- Site Recovery Manager
- Nutanix Runbook Automation
- Manual or scripted steps
- Vendor tools such as Zerto

Table 152: For Each Workload Decide Whether to Maintain or Change

MULTI-NET-009	FOR EACH WORKLOAD, DECIDE WHETHER TO MAINTAIN OR CHANGE IP ADDRESSES DURING FAILOVER.
Justification	
Implication	

Service Advertisement

Service availability is the advertisement of the workload and its availability to external clients at the DR site. There are a number of network and application technologies that can provide service advertisement, and this will be specific to your network and workload. For each application, consider how clients will reach this application at the DR site. This may involve application multi-site awareness, DNS updates, routing updates, load balancers, or some combination of these.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1181

6. Incorporating Optional Nutanix Products and Services

Nutanix offers a number of optional products and services that you may choose to incorporate when implementing private, hybrid, or multicloud solutions on the Nutanix platform. These options can help you quickly satisfy unique organizational requirements.

The subsections that follow introduce the following solutions and provide operational guidelines consistent with earlier sections of this guide:

- Prism Operations: Prism Pro and Prism Ultimate add to the base capabilities of Nutanix Prism to provide monitoring, analytics, and automation capabilities from a single management interface.
- Nutanix Cloud Clusters: Clusters extends the Nutanix stack to the public cloud, creating a single management domain that spans private and public clouds and removes the friction from multicloud operations.
- Flow Network Security: Microsegmentation and other capabilities further enhance the security of your Nutanix operations.
- Files: Files enables a Nutanix cluster to incorporate full-featured file services capabilities, eliminating the need for standalone NAS appliances or file servers.
- Objects: Objects enables a Nutanix cluster to provide S3-compatible, software-defined, scale-out object stores for a variety of use cases, eliminating the need for standalone object storage while supporting applications that rely on object stores with an on-premises alternative.
- Mine: Nutanix Mine is an integrated backup solution, combining the benefits of the Nutanix HCI architecture with the capabilities of proven backup vendors.
- Calm: Calm provides application-level orchestration and lifecycle management, simplifying application management and enabling self-service.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1182

- Karbon: Karbon integrates certified Kubernetes with the Nutanix operating environment, enabling Nutanix clusters to support both VM- and container-based applications while simplifying Kubernetes deployment and management.
- Nutanix Database Service: NDB automates and simplifies database administration, provisioning, and lifecycle management, facilitating database as a service (DBaaS).

Each subsection includes key design objectives, architecture overview, and detailed technical design considerations.

Prism Operations

Key Design Objectives

Table 153: Prism Ops Design Objectives

DESIGN OBJECTIVES	DESCRIPTION	NEW / UPDATE / REASONING
Enable proactive operations management	Prism Pro and Prism Ultimate licenses provide: - Operational automation in response to common triggers - Monitoring for non-Nutanix VMware environments - Application discovery and application-level monitoring	New

Architecture Overview

The operations tier in Nutanix Prism (provided by Prism Pro and Ultimate) focus on the entire IT Ops triangle—monitoring, analytics, and automation. Prism offers a single pane of glass that combines monitoring and automation to isolate pain points and ease the deployment of operational automation. This

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1183

allows you to harness the full power of HCI. The solution aims to remove silos between different monitoring and automation tools and avoid the noise created by dynamic virtual infrastructure environments.

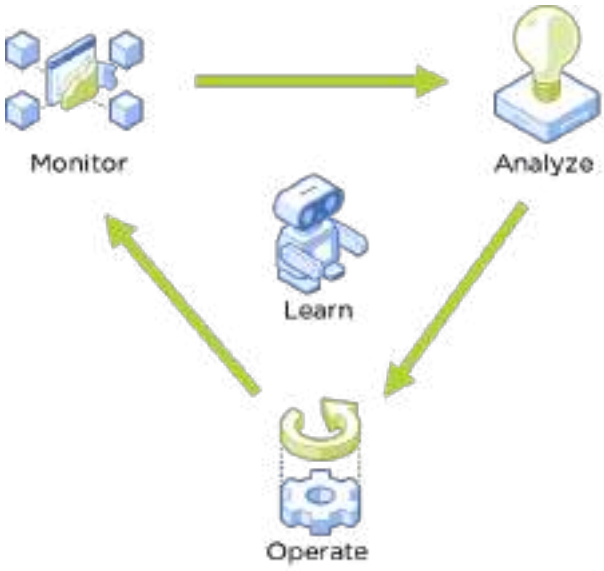


Figure 74: IT Ops Triangle

The goal is to provide broad observability and actionable signals powered by machine learning and automation for a seamless operations experience.

Prism Operations (Prism Ops) is powered by X-FIT, a distributed time series analysis and forecasting system that uses an ensemble of models. X-FIT is an enabler for building a management fabric; it can autonomously optimize datacenter performance and intelligently manage application resource demands using operational data.

Virtualization

- Prism Pro and Ultimate are hypervisor agnostic, working with both AHV and ESXi.
- With the release of Prism Central 2020.9, it is possible to monitor non-AOS vCenter VMs with Prism Pro. Similar capabilities available for an AOS environment, such as runway forecasting and playbook execution, are extended to VMware when it is monitored with Prism.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1184

Management

All Prism Operations features are accessed through Prism Central, which removes the need for separate management tools, providing one tool for monitoring, operational analysis, and automation. With Prism Ultimate, this visibility and functionality has been extended to the application layer.

Automation

- X-Play is a simple-to-use automation engine geared toward the average IT admin managing Nutanix and non-Nutanix infrastructure (as of PC 2020.9). It is based on various triggers, including actionable alerts generated by machine learning insights. As X-Play runs through a Playbook, it initiates a sequence of actions that can be tracked through a corresponding Play.
- Six triggers are currently available: alert-based, manual, time-based, alerts matching multiple criteria, event-based, and webhook triggers. There are 27 out-of-box actions provided that can be customized according to your needs and integrated with third-party tools. Playbooks can also be imported and exported across different Prism Central instances.

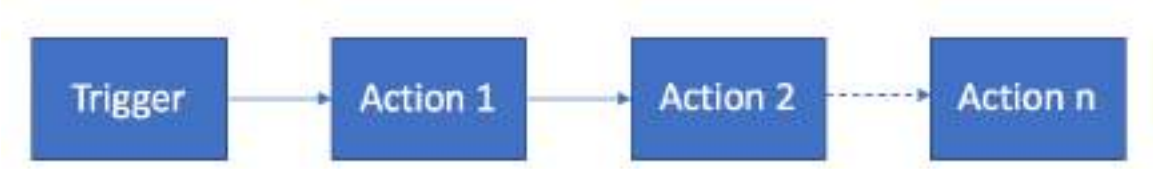


Figure 75: With Prism X-Play, a single trigger can precipitate multiple actions

Prism Licenses

Prism has three licensing tiers:

- Starter: Included free with AOS and deployed automatically with Prism Central. Features include:
  - Monitoring and troubleshooting
  - RBAC
  - LCM upgrades
  - Comprehensive search

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1185

- Pro: Separate add-on license. Enabled via Prism Central. Features include:
  - Customizable dashboards and reporting
  - Capacity forecast and runway planning
  - VM inefficiency detection and right-sizing
  - Anomaly detection and advanced troubleshooting
  - Monitoring non-AOS infrastructure
  - Smart operations automation
- Ultimate. Separate add-on license. Enabled via Prism Central. Features include:
  - Application discovery
  - Application monitoring – SQL Server content pack
  - Cost-metering, budgeting, and chargeback for resources

Prism Ultimate

Administrators may have zero visibility into the applications running inside VMs deployed on Nutanix infrastructure. Troubleshooting application issues becomes onerous without this application data and often requires separate software for application monitoring.

Prism Ultimate collects application metrics using third-party/Nutanix collectors (agentless), providing a single pane of glass to view both application and infrastructure data. With collected performance metrics, Prism Central can now provide a holistic view of IT operations that allows admins to easily monitor and diagnose problems caused by app performance issues without finger pointing.

High-Level Design Considerations

Currently, Prism's operations features are tied to a single instance of Prism Central. This means all nodes registered to a Prism Central instance must be licensed for Prism Pro & Ultimate in order for those nodes to be license compliant.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1186

- To enable Prism Ultimate features, you must increase Prism Central resources to 14 vCPUs and 30 GiB memory on a small Prism Central instance or 18 vCPUs and 48 GiB memory on a large Prism Central instance.
- Prism Ultimate is available beginning with release PC 2020.8. Non-AOS VM monitoring is available beginning with PC 2020.9.

Operational Automation

Table 154: Leverage X-Play Playbooks

OPS-001	LEVERAGE X-PLAY FOR POWERFUL LOW-CODE/NO-CODE OPERATIONAL AUTOMATION
Justification	Playbooks require the presence of Prism Pro.
Implication	Requires an additional license that can increase cost.

The webhook trigger gives a third-party tool the ability to execute actions within Prism Central. Conditional execution based on a string that is read and parsed allows for if-this-then-that (IFTTT) workflows, giving complete control to the admin for building powerful automations. For example, you can create a service ticket in your preferred tool (ServiceNow, etc.) based on alerts or events and trigger further actions in Prism Central based on approval or denial.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1187

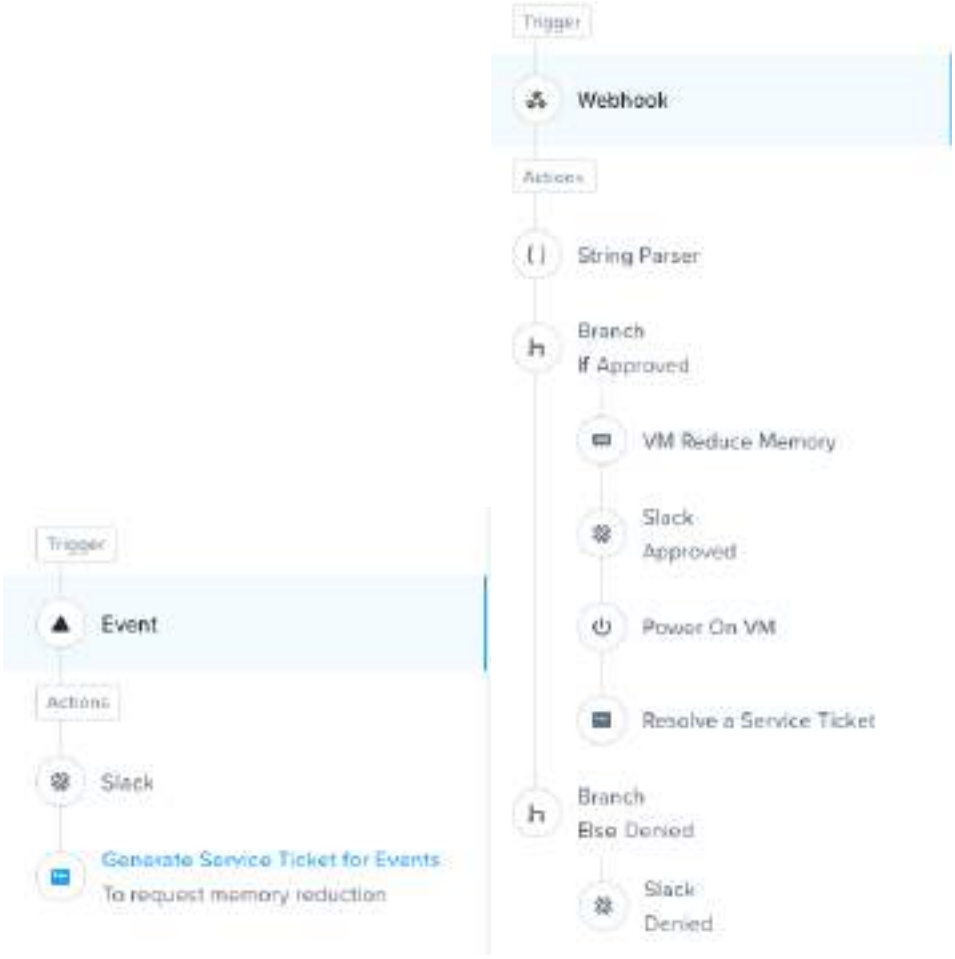


Figure 76: Example Workflows Based on Various Triggers

Non-AOS VM Monitoring

Table 155: Monitor Non-AOS VMs

OPS-002	MONITOR NON-AOS VMs
Justification	VMware virtualized environments not running under AOS can be monitored with Prism Pro.
Implication	Requires an additional license that may increase cost.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1188

A containerized Nutanix collector is deployed on the Prism Central VM and gathers data for each configured VMware cluster, using the X-Stream interface to store the data. X-FIT generates the same intelligence as for a Nutanix cluster, and X-Play can be used to connect to automation.

Figure 77: Monitoring non-AOS VMs with Prism Ultimate

Application Discovery

Table 156: Discover Applications with Prism Ultimate

OPS-003	DISCOVER APPLICATIONS RUNNING ON YOUR INFRASTRUCTURE.
Justification	You can discover and export applications running on your Nutanix cluster with Prism Ultimate.
Implication	Requires an additional license that may increase cost.

Prism Ultimate's agentless discovery allows you to identify application-to-VM dependencies using an API for CMDB integration. (A cloud connection is required.) Internet Protocol Flow Information Export (IPFIX) data is collected from VMs and sent to the Nutanix cloud which analyzes and syncs the findings back to Prism.

App Monitoring

Table 157: Monitor Microsoft SQL Server

OPS-004	MONITOR SQL SERVER

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1189

Justification	Prism Ultimate can provide greater insights into SQL Server operation, enabling you to understand how infrastructure impacts applications and to isolate problems between the two layers.
Implication	Requires an additional license that may increase cost.

Prism Ultimate provides visibility into databases, queries, and SQL-specific metrics plus behavior learning and anomaly detection. The containerized Nutanix collector is deployed on the Prism Central VM and gathers data for each configured SQL instance, using the X-Stream interface. X-FIT then analyzes the data to generate insights and alerts for troubleshooting and automation.

SQL Server is the first app monitoring content pack to be released, providing deeper insights into application performance metrics. It currently supports 100 SQL instances or 94,000 metrics.

Figure 78: Monitoring SQL Server with Prism Ultimate

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1190

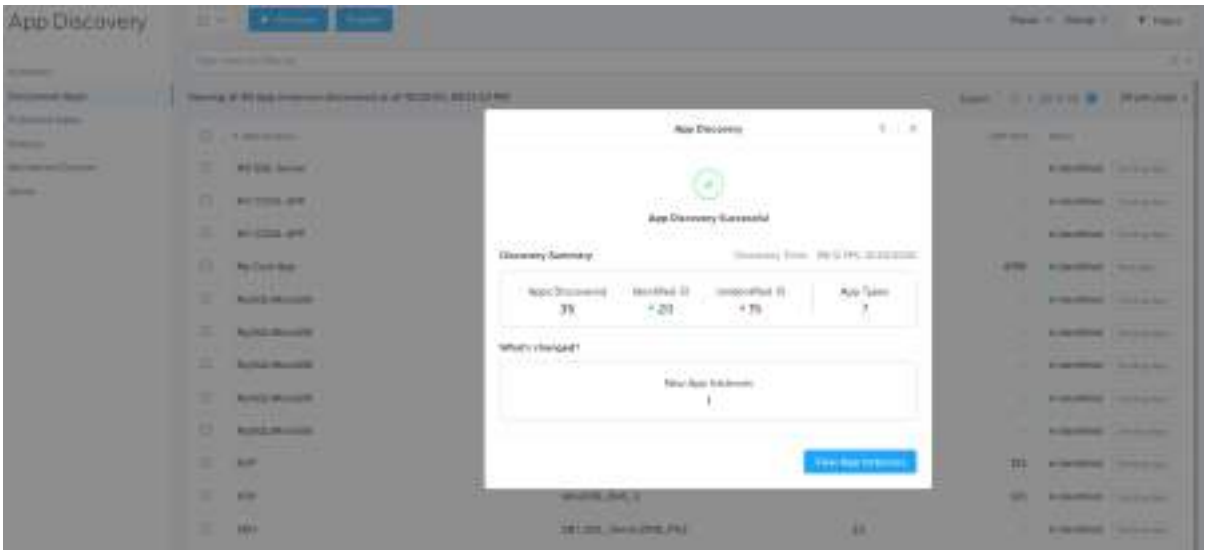


Figure 79: App Discovery

Nutanix Cloud Clusters for Hybrid and Multicloud Operations

Key Design Objectives

Table 158: Nutanix Cloud Clusters Design Objectives

DESIGN OBJECTIVES	DESCRIPTION	NEW / UPDATE / REASONING
Extend Nutanix operations to public cloud	Nutanix Cloud Clusters (NC2) extends the Nutanix operational domain to encompass AWS in addition to on-premises locations	New

Architecture Overview

Nutanix enables customers running Nutanix software on-premises to deploy the same software stack on cloud computing providers such as Amazon Web Services (AWS), resulting in a more uniform hybrid cloud environment. Because NC2 on AWS runs Nutanix AOS and AHV—with the same CLI, UI, and APIs

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1191

—existing IT processes and third-party integrations that work on-premises operate in the cloud without modification.

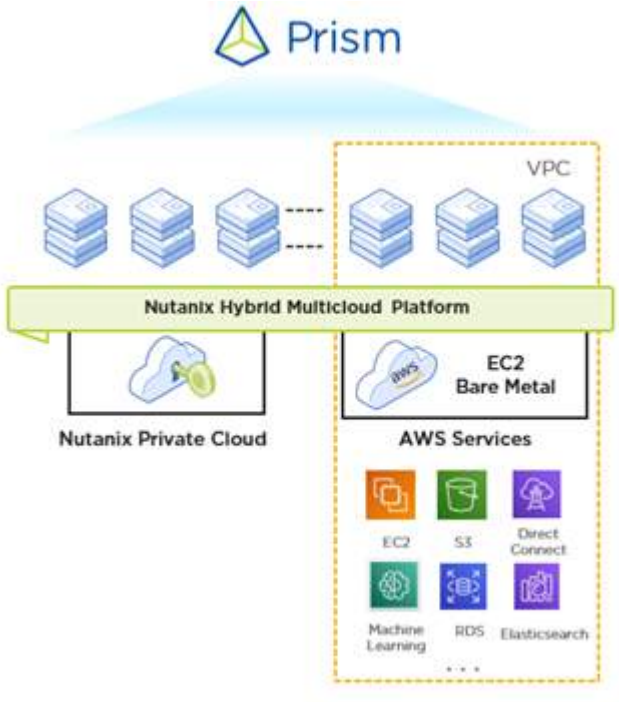


Figure 80: Nutanix Cloud Clusters on AWS

NC2 implements the complete Nutanix hyperconverged infrastructure (HCI) stack using Amazon Elastic Compute Cloud (EC2) bare-metal instances. Each bare-metal instance runs the same Controller VM (CVM) and the Nutanix AHV hypervisor as used on-premises, using the AWS elastic network interface (ENI) to connect to networking. AHV user VMs do not require any additional configuration to access AWS services or other EC2 instances.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1192

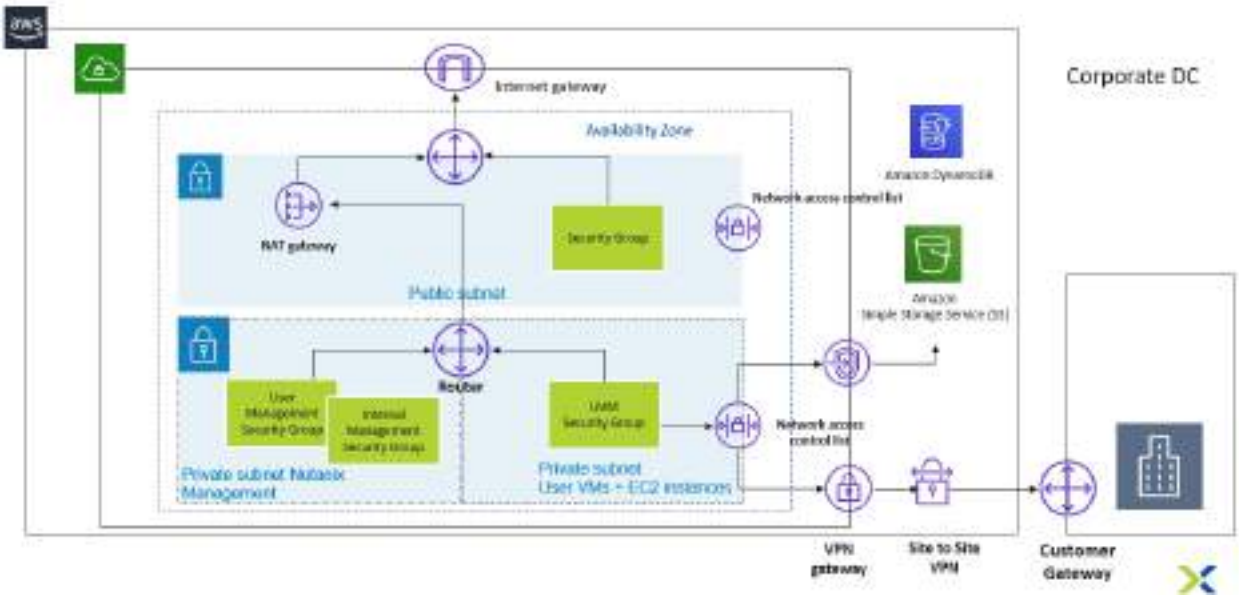


Figure 81: Nutanix Cloud Clusters on AWS Architecture

In most ways, NC2 on AWS is like running Nutanix AOS on any hardware OEM. Almost everything you know about AOS is the same, reducing the need for different systems administrators, tooling, and scripting between private and public cloud. The following description focuses on the differences related to deployment in AWS.

Networking

AHV runs an embedded distributed network controller that efficiently integrates user VM networking with AWS networking. AHV assigns all user VM IPs to the bare-metal host where VMs are running. Instead of creating an overlay network, the AHV embedded network controller simply provides the networking information for VMs running on NC2, even as VMs move between AHV hosts. Because NC2 IP address management is integrated with AWS Virtual Private Cloud (VPC), AWS allocates all user VM IPs from the AWS subnets in your existing VPCs.

NC2 utilizes AWS Elastic Network Interfaces (ENI) to provide IP addresses for virtual machines that get created on EC2 bare-metal nodes using AHV's built-in IPAM. One EC2 bare-metal host can have a maximum of 15 ENIs; NC2 uses the first ENI for host management (CVMs and AHV). The remaining 14 ENIs can be

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1193

used as VM IPs. An ENI on the EC2 instance will only be consumed if there is a VM present on the subnet.

Networking limits and restrictions

The following limits and restrictions apply to NC2 deployments:

- One subnet per ENI.
- An ENI can have up to 50 IP addresses, one of which must be the primary IP.
- The primary IP of an ENI cannot be changed or migrated to another ENI, leaving 49 IP addresses per ENI.
- The private management subnet cannot be used for deploying VMs.
- The user VM subnets cannot be shared between clusters.
- The user VMs should use a separate subnet from other AWS EC2 instances.

Currently, the maximum number of VMs supported is:

14 ENI * 49 IPs = 686 VMs per node

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1194

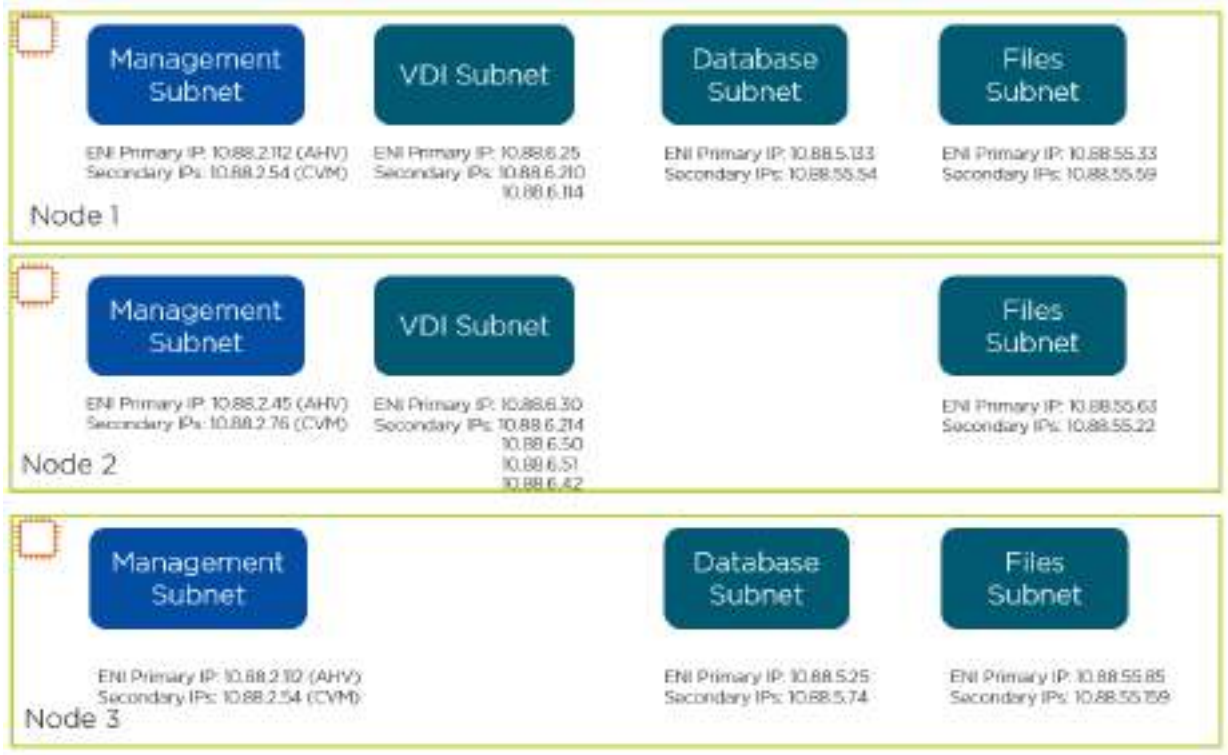


Figure 82: Example IP Address Assignment for an NC2 Deployment

The figure above illustrates that nothing is running on the third node of the cluster on the VDI subnet. We can tell this because no ENI/IPs are being used on that node. Likewise, we only have two database VMs deployed on the cluster on nodes 1 and 3.

IP Mobility

Nutanix does not currently provide a stretched layer-2 network connection to AWS. The Nutanix Disaster Recovery service preserves IP and MAC addresses and can be paired with third-party software to stretch the network. Nutanix Disaster Recovery can automate assigning new IPs to your VMs, and it uses recovery plans that provide network mappings for remote subnets.

Compute

NC2 on AWS currently only supports homogeneous clusters, so you must use the same EC2 bare-metal instance type for all nodes in a cluster. However, you

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1195

can have multiple clusters with different instance types that are optimally suited to the workloads in each cluster.

Hardware Choice

The instance types available will depend on the AWS region you select. NC2 supports four possible EC2 bare-metal instances:

Table 159: Supported EC2 Bare-Metal Instances

INSTANCE	vCPU	MEMORY (GiB)	NETWORK PERFORMANCE	SSD STORAGE (GB)
z1d.metal	48	384	25 Gigabit	2 * 900 NVMe
m5d.metal	96	384	25 Gigabit	4 * 900 NVMe
i3.metal	72	512	25 Gigabit	8 x 1,900 NVMe
i3en.metal	96	768	100 Gigabit	8 x 7,500 NVMe

The i3.metal instance is a great choice for virtual desktop deployments, offering the best price/performance. The i3en.metal instance is good for database workloads and can provide lower TCO when high storage capacity is needed. The z1d.metal and m5d.metal instances are well positioned for general compute and dev/test workloads that are temporary in nature.

Minimum cluster size is 3 nodes, up to a max of 16 nodes. Each instance type consumes a certain amount of vCPU that goes against your configured limits in AWS. You need to ensure that you have sufficient headroom so that you are not prevented from deploying additional nodes in a cluster. If you are deploying a cluster for N+1 availability, your vCPU limits should account for both the additional node and any future growth.

Business Continuity Layer

Protection against site failures

- A Nutanix AWS cluster with three or more nodes is deployed with a Replication Factor (RF) of 2 by default, with nodes explicitly distributed across racks to protect against failure of a single device, node, or rack. You can also configure RF=3 to provide higher levels of redundancy.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1196

- Similar to Nutanix on-premises operation, a single Nutanix cluster on AWS cannot protect against infrastructure failures that affect more than one rack or an entire AWS availability zone. To learn more about Rack Awareness see KB 9723 .

To protect data against large-scale infrastructure failures, Nutanix recommends you regularly back up and/or replicate data to another Nutanix cluster running on premises or in a different AWS Availability Zone (AZ). Consult Data Protection and Recovery with Prism Element for more information. You can also use Nutanix DRaaS. See the Nutanix Cloud Clusters on AWS tech note for more information.

Protection against disruptive actions

- A simple reboot (intentional or not) of an EC2 bare metal instance only temporarily affects a Nutanix cluster running on AWS. The node automatically rejoins the cluster.
- Stopping or terminating an EC2 bare metal instance that is part of a Nutanix cluster on AWS effectively removes that node from the cluster. With the default replication factor 2 configuration, removing a single node does not affect availability. However, stopping more than one EC2 instance can result in data loss.
- Shutting down an AHV host running on AWS from the AHV shell results in the permanent removal of that node from the cluster. The cluster adds a node back when it self-heals. The default replication factor 2 configuration can tolerate unavailability of one node. Shutting down more than one AHV host from the AHV shell can result in data loss.

Security

Securing traffic to and from your AWS cluster can be accomplished using a combination of third-party firewalls, Nutanix built-in security groups, and Flow Network Security.

The NC2 console creates the following security groups when a cluster launches in AWS:

- Internal Management

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1197

- User Management
- UVM

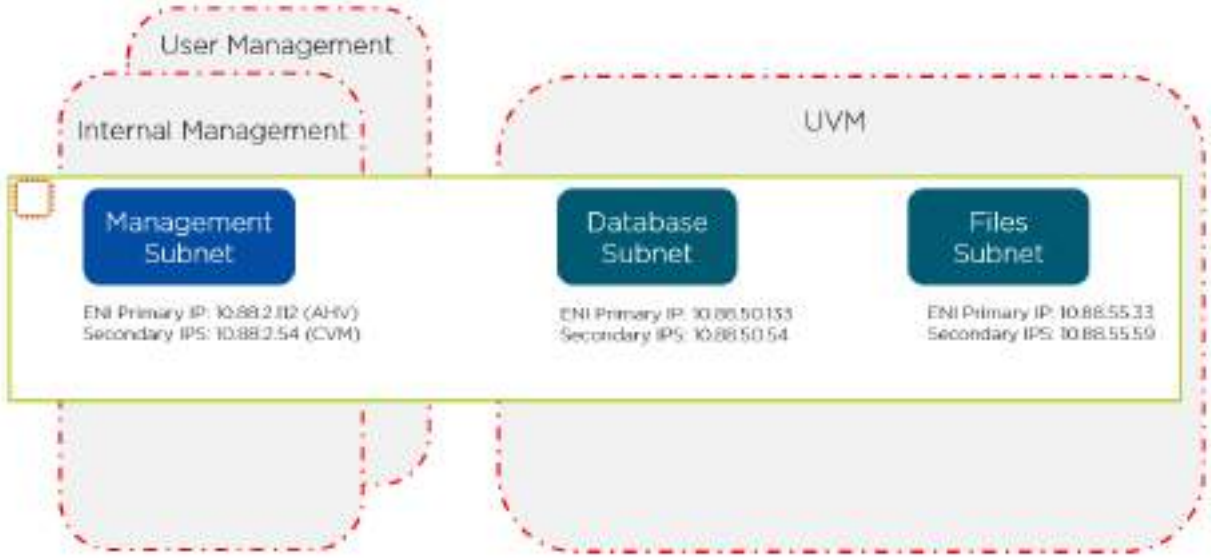


Figure 83: Security Groups Used by NC2

These security groups have the recommended default rules. Nutanix recommends that you do not modify internal management.

All management network ENIs created have the following security groups attached, even after the cluster is running:

- internal_management: Allows all communication between AHV and CVM within a cluster
- user_management: Allows specific ports for UVM to CVM communication

ENIs created for user VM subnets have the following security group attached:

- UVM: Allows communication between user VMs

You can find detailed information on allowed port groups in the NC2 on AWS Deployment and User Guide . Flow Network Security works both in the cloud and on-premises and can be used to segment operations and to block east-west traffic.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1198

High-Level Design Considerations

Networking

Internet Access

Portal Access: Determine how you will enable outbound access from your NC2 cluster to the Cluster Portal. You can route all Internet traffic through your corporate firewall or set up an Internet Gateway in AWS. If your company is blocking outbound traffic, you also need a firewall that can block domain traffic versus subnet ranges since some of the Cluster Portal services are dynamic.

On-Premises Connectivity: There are three native ways to connect to on-premises operations from AWS:

- VPC VPN: Works well for connecting to a single site.
- Transit Gateway: Preferred when you plan to connect multiple sites to your NC2 cluster.
- Direct Connect: Typically, more expensive but provides a very stable connection at your desired speed.

Table 160: Separate Subnets

AWS-01	CREATE SEPARATE SUBNETS FOR USER VMS
Justification	AWS clusters cannot deploy user VMs on the same subnet as the CVMs and AHV hosts. New subnets are also needed if you are using Nutanix Disaster Recovery to fail VMs over to AWS. You should also use different subnets for native AWS EC2 instances.
Implication	Unless using third-party software to create a stretched layer 2 network, you must change your VMs' IP addresses when they move to AWS.

Business Continuity

Determine your availability needs. If you are running dev/test, you probably don't need to replicate data to another region or to an on-premises datacenter.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1199

If you are running production workloads, you need to replicate a copy of your data on-prem, to another AWS region, or use an AHV backup product.

Table 161: Create Availability Zones

AWS-02	USE AWS DIRECT CONNECT OR CREATE A 2ND AWS CLUSTER IN A DIFFERENT AVAILABILITY ZONE.
Justification	To achieve an RPO of zero, you will need to ensure you meet the latency requirements for synchronous replication. If your latency is over 5ms round trip from your primary datacenter, you will have to create a secondary AWS cluster in a different AZ.
Implication	A disaster that affects an entire geography or a system wide event might affect more than one AZ in a given region.

Table 162: Use Replication

AWS-03	PROTECT YOUR AWS CLUSTER BY REPLICATING BACK TO ON-PREM.
Justification	You need to protect yourself from an outage in AWS. You can back up your AWS cluster using AHV-based backup software, but the region where you place the backups has to be able to be restored in a timely fashion. Also, the region you restore service to has to be close enough to meet any on-prem SLAs you might have.
Justification	You need to protect yourself from an outage in AWS. You can back up your AWS cluster using AHV-based backup software, but the region where you place the backups has to be able to be restored in a timely fashion. Also, the region you restore service to has to be close enough to meet any on-prem SLAs you might have.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1200

Table 163: Don't Overlap Subnets

AWS-04	PLAN YOUR AWS VIRTUAL PRIVATE CLOUD NOT TO OVERLAP WITH YOUR ON-PREM SUBNETS.
Justification	Nutanix Clusters does not provide stretched layer 2 networking natively. If you want to failover or migrate your on-prem applications and also keep a subnet active on-prem, you will need a subnet that does not overlap. If your goal is only to achieve a complete failover into AWS, you can create the same subnet in AWS, since your on-premises environment won't be active after a failover occurs.
Implication	Failing over an entire subnet without re-IPing requires you to shut down those subnets on-prem if you intend to keep the connection alive.

Security

AWS Accounts: Determine if your level of risk is acceptable with the privileges delegated to the Cluster Portal. While the Cluster Portal is built with the utmost attention to security, some customers may still want a greater level of separation. To achieve this, customers can use a separate AWS account with VPC pairing to their current AWS account.

Table 164: Allow Outbound Internet Access

AWS-05	ALLOW OUTBOUND INTERNET ACCESS THROUGH AN EXISTING CONNECTION TO THE INTERNET TO ALLOW THE CLUSTER PORTAL TO MANAGE YOUR CLUSTER.
Justification	You should limit the number of attack vectors into your environment. In a hybrid cloud environment, you most likely already have an existing outbound connection. If you only have a public cloud environment, you will have to setup NAT and an Internet gateway.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1201

Implication	You will have to pay for egress networking costs to your on-prem environment(s).

VPC Limits

Table 165: Plan VPC Limits for Growth and Availability

AWS-06	You will have to pay for egress networking costs to your on-prem environment(s).
Justification	Your vCPU limits are set at the regional level and cover many instance types. You should ensure that you have enough headroom for expansion and to accommodate a node failure. If your cluster is using RF=3, then you must ensure that you have enough spare vCPU capacity to accommodate the vCPU needs for two failed nodes.
Implication	Increasing limits affects a variety of EC2 services. You should monitor for any suspicious activity since the limit will be higher.

Nutanix Flow for Microsegmentation

Key Design Objectives

Table 166: Flow Design Objectives

DESIGN OBJECTIVES	DESCRIPTION	NEW / UPDATE / REASONING
Implement microsegmentation for greater security	Provide stateful firewalls to segment applications running in VMs on Nutanix clusters	New

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1202

Architecture Overview

Flow provides microsegmentation functionality using a distributed stateful firewall that enables granular network monitoring and enforcement between VMs running on the AHV platform as well as external entities they communicate with. Flow provides security rules, which enforce what kind of traffic is allowed between VMs. Flow configuration is done via Prism Central (PC) by defining security rules based on categories. Doing the configuration from PC allows centralized management and distributed enforcement, where the enforcement is done on multiple Nutanix clusters and multiple Nutanix AHV nodes. Flow configures OpenFlow rules in each AHV host in order to implement the security rules.

Nutanix Flow uses categories and security rules that are configurable based on defined categories.

Categories

Categories are used to define groups of entities. The category schema consists of keys and values:

- Example Key: Department
- Example Value: Engineering

A {Key, Value} pair together forms a unique tuple in the PC management domain and this tuple is used to tag VMs.

For example, a VM providing production database services may have the following categories assigned to it:

- Key: Value
- AppTier: Database
- AppType: MySQL
- Environment: Production

These categories can then be utilized by Flow to determine what security rules to apply.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1203

Security Rules

Security rules specify the Flow policies which determine how VMs can talk with each other. These rules govern firewalls for applications and many other use cases, including isolating environments or quarantining VMs that are suspected to be infected. Based on the most common use cases, Flow provides four types of policies as shown in Table 164.

Table 167: Flow Policy Types

POLICY TYPE	USE CASE	EXAMPLE DEPLOYMENT
Quarantine	Quarantine Apps/VMs	Fault isolation and control
Isolation	Environment separation	Geographical isolations
App-Type	Application segmentation	App policy or inter-tier
AD-Type	AD/VDI segmentation	ID firewalls

Quarantine Policy

A Quarantine policy denies all traffic to/from specified VM(s)/categories.

Example: VMs A, B, and C are infected with a virus; isolate them to stop the virus from further infecting the network

Figure 84: Effects of a Quarantine Policy

Isolation Policy

An Isolation policy denies traffic between two categories, while allowing traffic within a category.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1204

Example: Separate tenant A from tenant B. Each environment is isolated and runs in parallel without affecting normal network communication.

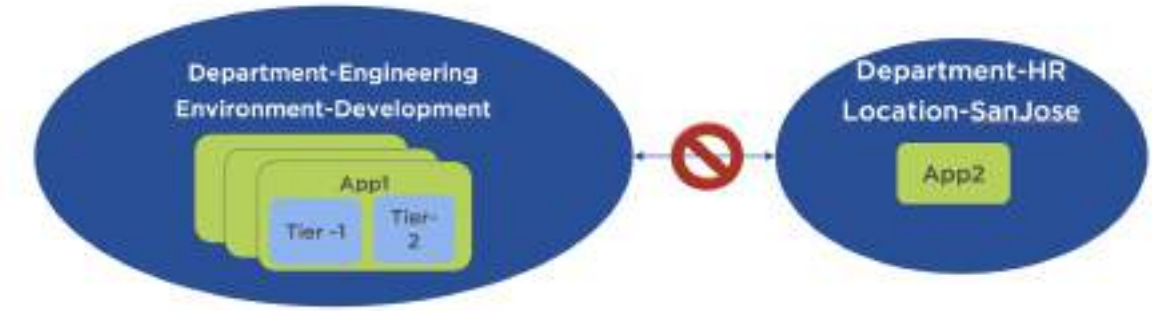


Figure 85: Effects of an Isolation Policy

App-Type Policy

An App-Type policy is used for configuring firewalls for applications running inside VMs. This rule allows you to define what transport (TCP/UDP), Port, and source/destination is allowed/denied.

- [Allow|Deny] Transport: Port(s) [To|From]

Example: Allow transport on TCP port 8080 from Category:Tier:Web to Category:Tier:App

The policy schema consists of Inbounds, Target Group, and Outbounds. Inbounds identify who can talk with the Target Group. Outbounds identify who the Target Group can talk with. Target Group identifies the VMs or applications that are being protected.

Figure 86: Illustration of an App-Type Policy

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1205

AD-Type Policy

An AD-Type policy is used for configuring firewalls for AD/LDAP users. This rule allows you to define what transport (TCP/UDP), Port, and source/destination is allowed/denied.

- [Allow|Deny] Transport: Port(s) [To|From]

Example: Allow subnets (example: clients) to talk with AD groups and allow AD groups to access payroll data

The policy schema consists of Inbounds, AD Groups, and Outbounds. Inbounds identify who can talk with the AD Groups. Outbounds identify who the AD Groups can talk with. AD Groups identify the users (based on VMs that the users have logged into) that are being protected.

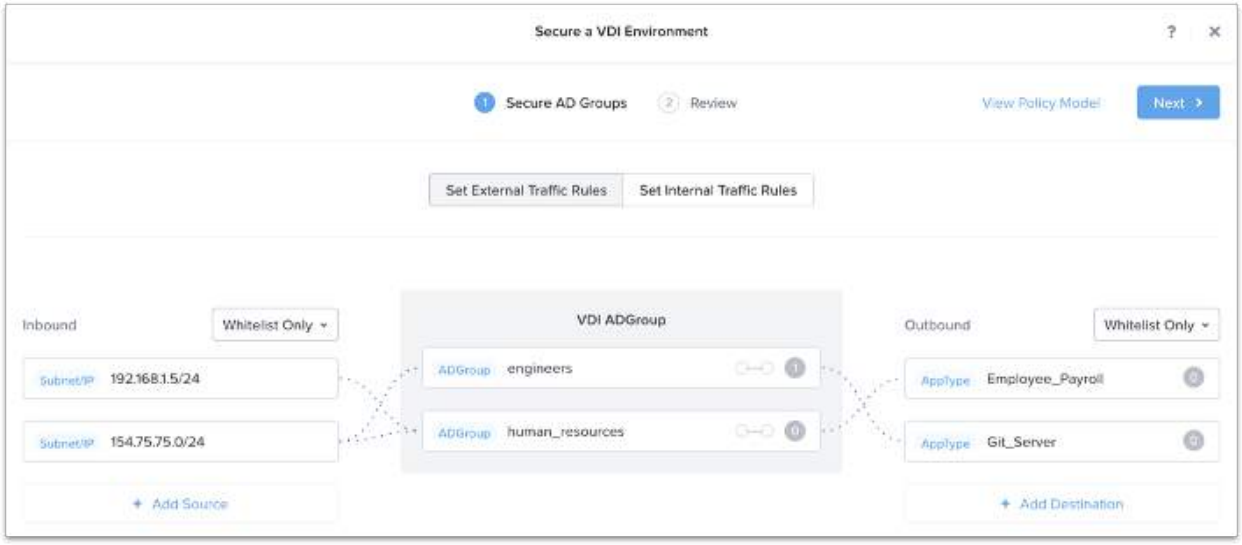


Figure 87: Using an AD-Type Policy to Secure a VDI Environment

The following figure shows an example of using Flow microsegmentation to control traffic for an application:

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1206

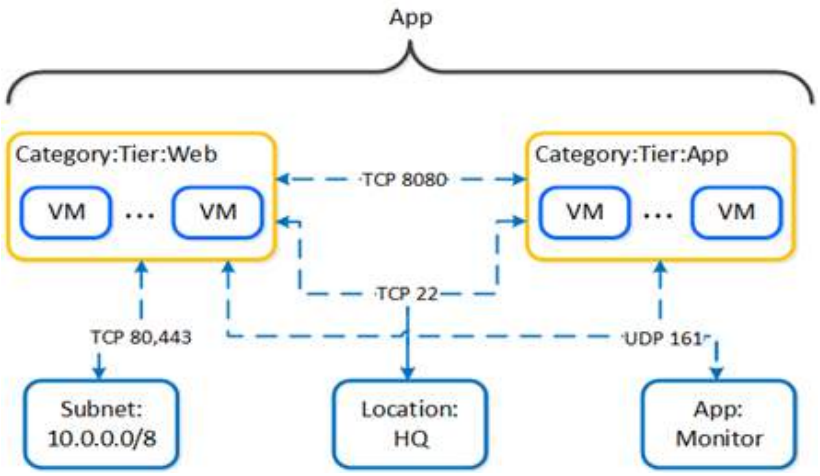


Figure 88: Using an AD-Type Policy to Secure a VDI Environment

Security Rule Actions

A security rule has an action field which determines what action is taken when a rule is matched. With AHV and Flow microsegmentation, there are two types of actions:

- Apply: Enforce the policy by permitting defined flows and blocking all others.
- Monitor: Allow all flows but highlight any packets that violate the policy on the policy visualization page.

Other Flow Features

While microsegmentation—including policy management, policy distribution, policy enforcement, and monitoring— is a core feature of Flow, the product offers many other capabilities such as:

- ID firewalls for VDI security
- Flow policy export/import
- Policy hit logs
- IPV6 enable/disable
- Service groups
- Address groups

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1207

- Audits
- Logging
- NCC alerts
- Service chains for advanced firewalls and integration with third-party devices
- Flow security central for advanced auditing, policy automation, governance
- L2 isolation
- External IPAM support
- Live migration connection tracking
- Nutanix Clusters integration

High-Level Design Considerations

Nutanix recommends the use of microsegmentation to isolate applications that don't interact or talk to each other directly.

Table 168: Use Microsegmentation to Isolate Applications

FLOW-001	USE MICROSEGMENTATION WITH APP-TYPE POLICY TO SEGMENT APPLICATIONS
Justification	Microsegmentation between applications can decrease the attack surface if a datacenter is penetrated and also prevent ransomware and other malware from spreading.
Implication	Nutanix AHV is required to utilize Flow microsegmentation.

If you are running VDI in your environment, using flow to isolate traffic based on AD groups is also extremely useful.

Table 169: Use AD-Type Policy to Isolate VDI

FLOW-002	USE MICROSEGMENTATION WITH AD-TYPE POLICY FOR VDI DEPLOYMENTS

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1208

Justification	Microsegmentation based on AD groups can isolate VDI environments, prevent users from accessing restricted resources, and help prevent ransomware and other malware from spreading.
Implication	Nutanix AHV is required to utilize microsegmentation.

Nutanix Files for Integrated File Services

Key Design Objectives

Table 170: Nutanix Files Design Objectives

DESIGN OBJECTIVES	DESCRIPTION	NEW / UPDATE / REASONING
Enable file services from Nutanix clusters	Nutanix Files provides flexible file services implementations including: - Mixed or dedicated clusters - Flexible storage options - Multiple, separate file servers per cluster - Simple data protection and DR	New

Architecture Overview

Nutanix Files is a scale-out, software-defined file server that provides Server Message Block (SMB) and Network File System (NFS) file services to clients. Nutanix Files leverages Nutanix HCI for its core storage, networking, virtualization (AHV and ESXi) and compute requirements. Management for Nutanix Files is performed from Prism Element.

Nutanix Files instances are composed of a set of VMs (called FSVMs). For a given file server instance, Files requires at least three FSVMs running on three physical nodes to satisfy a quorum for high availability. You can scale out a given file server at any time, by adding FSVMs, up to the number of physical

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1209

nodes in the HCI cluster or a maximum of 16 FSVMs. You can also scale the CPU and memory of the set of FSVMs at any time.

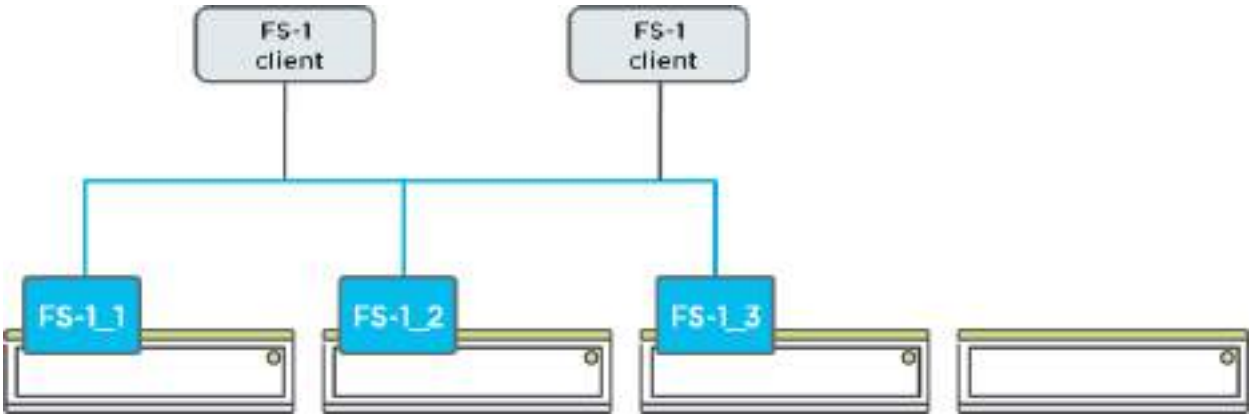


Figure 89: Example of a Nutanix Files Instance

Multiple Files instances can run on the same HCI cluster. Each instance represents an individual namespace. Each instance can scale from three FSVMs up to 16 FSVMs, assuming there are enough resources in the HCI cluster.

You can also deploy single FSVM file servers. Note that single FSVM file servers cannot scale out.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1210

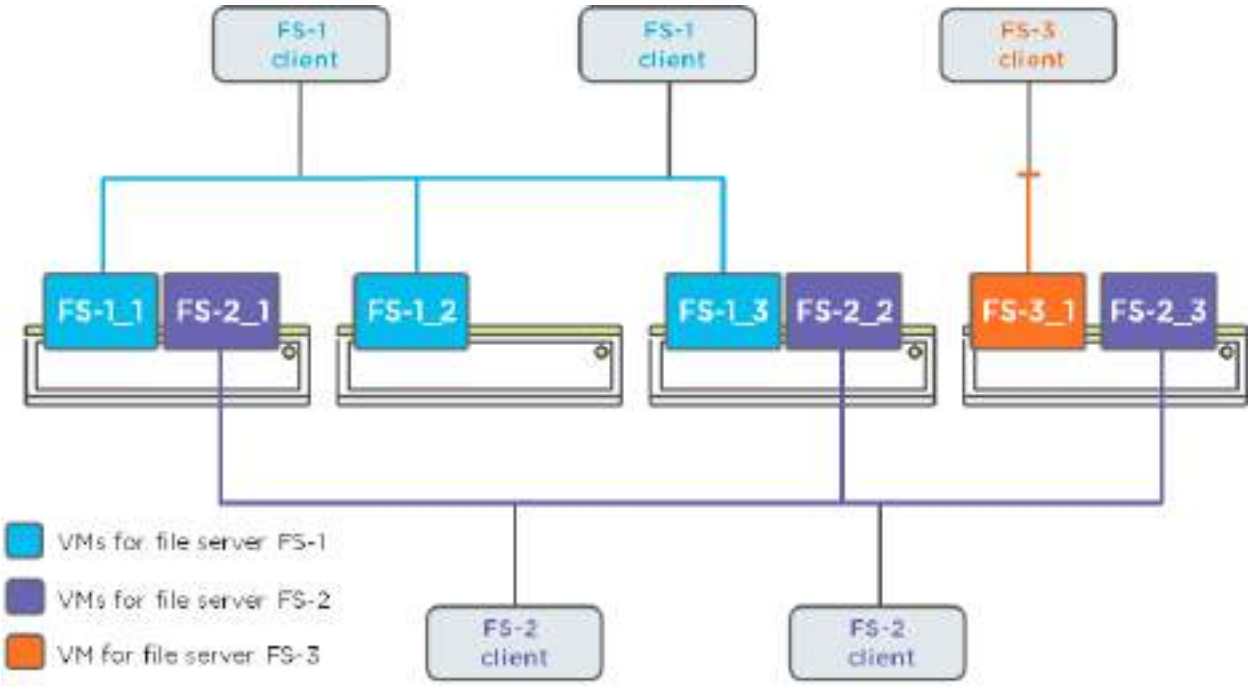


Figure 90: Three Separate Nutanix Files Instances Deployed on a Single Cluster

For file servers with three or more FSVMs, high availability during node failure and Files upgrades is achieved at the file-server level. Resources controlled by a failed or upgrading FSVM are moved temporarily to another FSVM. For single FSVM instances, hypervisor HA provides protection against node failure events.

Each file server has two networks: a client network and a storage network. The client network is used for SMB and NFS traffic and other required services such as active directory, DNS, and NTP. The storage network provides shared storage services for file shares and exports. Nutanix Volumes is used on the backend to provide shared storage, leveraging the iSCSI protocol over the storage network.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1211

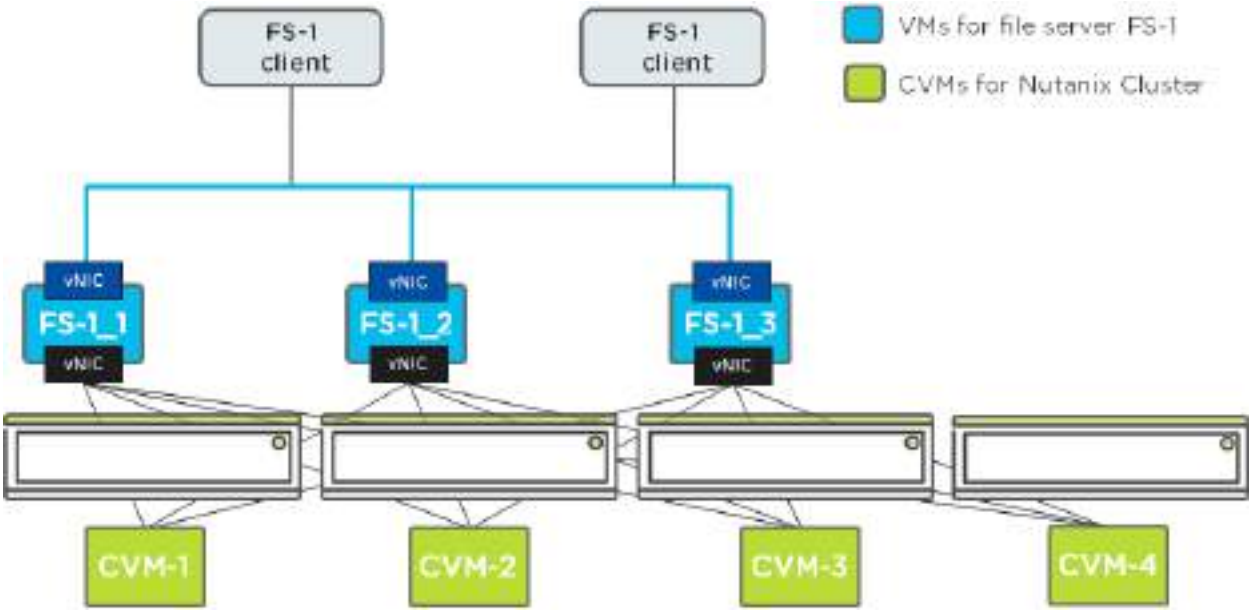


Figure 91: Relationship Between File Server VMs, CVMs, and Cluster Nodes

File shares are load balanced across FSVMs based on share type. Nutanix Files has two types of shares, distributed shares and standard shares.

Distributed shares have distributed ownership across all FSVMs in a Files cluster. Distribution occurs from the top-level directory (TLD) (\\ClusterName \DistributedShare\TLD). Each TLD can belong to a different FSVM and reside in its own volume group. Several volume groups support a distributed share; the total number of volume groups depends on the size of the Files cluster. Each FSVM has five volume groups to support distributed shares. For example, a three-node Files cluster has 15 volume groups to support shares.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1212

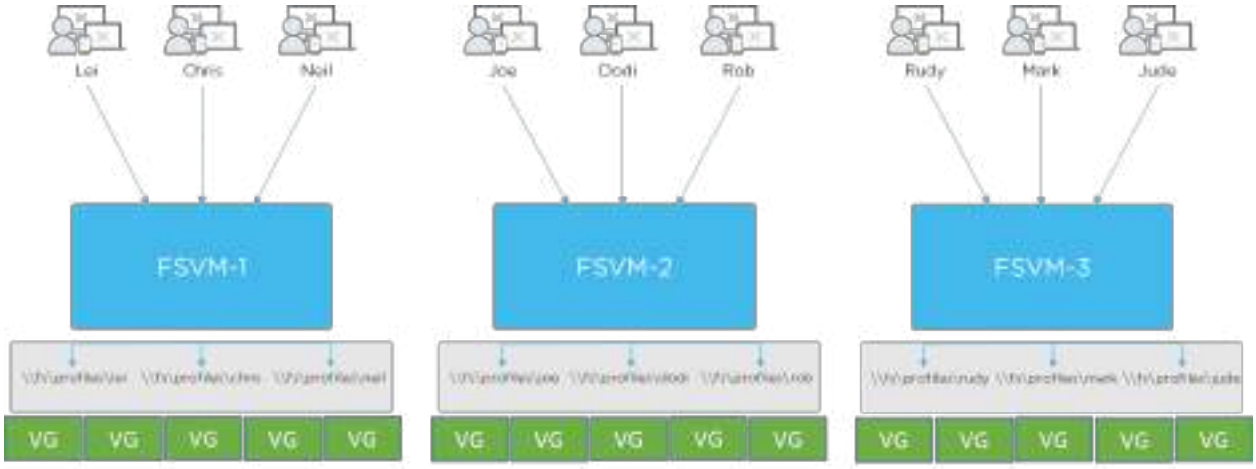


Figure 92: Distributed Shares are Distributed Across Multiple Volume Groups and FSVMs

Standard shares are owned by one file server VM (FSVM) at a time and have a single volume group to store data.

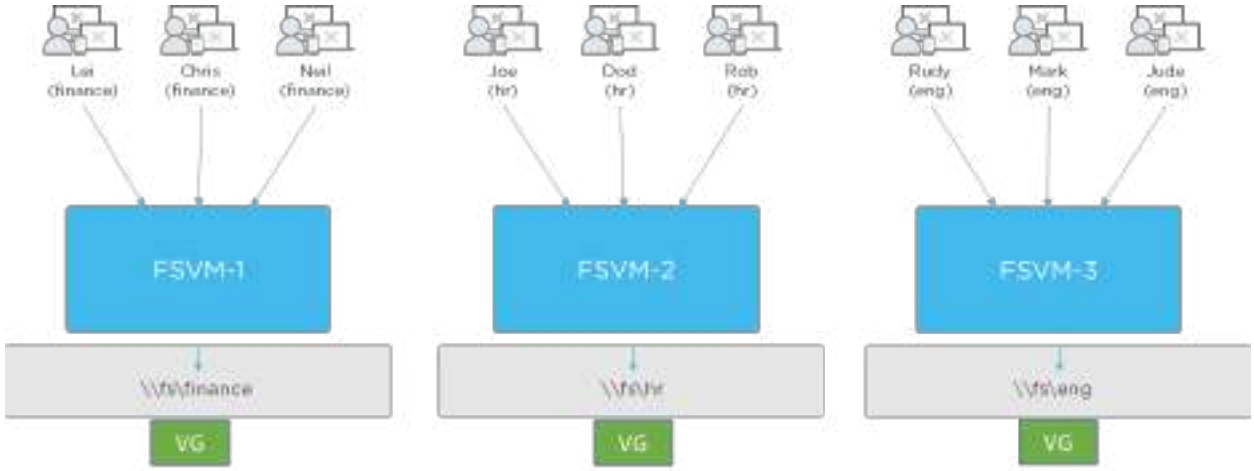


Figure 93: Standard Shares are Assigned to a Single FSVM and a Single Volume Group

For business continuity, Nutanix Files leverages the native data protection of Nutanix HCI. A protection domain is configured for each file server and native Nutanix HCI async and nearsync replication is used to protect configuration and user data.

Nutanix Files can run in a mixed environment along with other workloads, or on a dedicated cluster just for Files. Mixed environments require a Nutanix Files for AOS license, which is an add-on to your AOS license. Dedicated environments

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1213

require a Nutanix Files Dedicated license. In both cases Nutanix Files is licensed based on usable TiB from the perspective of the SMB or NFS protocol, plus any space consumed by snapshots.

High-Level Design Considerations

Mixed or Dedicated Clusters

There is no hard and fast rule regarding whether to deploy Nutanix Files in a dedicated cluster or a mixed cluster with other workloads. Like any other workload, the compute and storage density of your applications, performance requirements, failure domains, management domains, and other considerations need to be weighed.

Table 171: Mixed or Dedicated Environments

FILES-001	USE NUTANIX CLUSTERS DEDICATED TO FILE SERVICES WORKLOADS
Justification	File services tend to need storage dense configurations, with a higher ratio of HDD to SSD. Unstructured data workloads typically have limited data overwrites and large amounts of cold data, which benefit from erasure coding (EC-X).
Implication	Dedicating clusters to specific workloads can potentially lead to inefficient compute and storage utilization.

Hybrid Storage or All Flash clusters?

Every environment is different, but unstructured data has a tendency to have a small amount of active data and a large amount of inactive or cold data and also tends to be storage dense. High storage density with a majority of cold data leads many Nutanix Files deployments to utilize clusters with hybrid storage (a combination of SSD and HDD in each node). Considerations for sizing hybrid clusters is discussed in the Storage Capacity Utilization and Sizing section below. The Nutanix Files Sizing Guide (Nutanix Portal account required) can also help.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1214

Table 172: Choose Hybrid Clusters

FILES-002	USE HYBRID STORAGE NUTANIX CLUSTERS
Justification	Most unstructured data use cases work well with hybrid storage solutions where hot data resides on SSD and cold data resides on HDD. The Nutanix Distributed Storage Fabric will tier data as required between local or remote nodes and SSD or HDD based on the workload.
Implication	End user performance will be negatively impacted if an insufficient SSD tier is sized for the use case.

Number of FSVMs per File Server Instance

Each file server instance consists of some number of FSVMs. It's recommended to deploy at least 3 FSVMs for high availability at the file server level. The amount of compute you assign to each FSVM, and the number of FSVMs beyond the minimum of three, depend on your performance requirements. You need to ensure there is enough compute assigned to FSVMs to support the expected number of concurrent user connections. The release notes (System Limits section) for each version of Files contains a table that provides guidance. For example, the number of supported SMB connections per FSVM in the Nutanix Files 3.8 release is:

- 4 vCPU/12 GB memory = (supports up to) 500
- 4 vCPU/16 GB memory = 1000
- 6 vCPU/24 GB memory = 1500
- 6 vCPU/32 GB memory = 2000
- 8 vCPU/40 GB memory = 2750
- 12 vCPU/48 GB memory = 3250
- 2 vCPU/64 - 96 GB memory = 4000

You also need to ensure that enough storage IOPs and throughput are available for your specific workload. The number of FSVMs also plays a role in performance. Recommendations for sustained read and write performance per FSVM can be found in the Nutanix Files Sizing Guide (Nutanix Portal account

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1215

required) and the Nutanix Files Performance Guide (Nutanix Portal account required).

Once the minimum number of FSVMs and compute resources are determined, it is recommended that you take a balanced approach to the number of FSVMs, allowing you to scale-up or scale-out if needed. Having a 16-node AOS cluster does not mean you need a 16 FSVM file server.

Table 173: Minimum FSVMs

FILES-003	USE A MINIMUM OF 3 FSVMs
Justification	Three FSVMs or more provides improved high availability with less-disruptive maintenance operations versus single FSVM configurations.
Implication	Using a minimum of three FSVMs may lead to excessive resource utilization in environments with multiple file servers. Also, ROBO configurations require a minimum of three physical nodes which could lead to the over allocation of resources.

Table 174: N+1 Configuration

FILES-004	USE AN N+1 CONFIGURATION OF FSVMs TO PHYSICAL NODES
Justification	Having one physical node more than the number of FSVMs reduces performance impact during HA events.
Implication	Maintaining an additional node leads to unused compute resources during normal operations.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1216

Table 175: CPU and Memory Allocation

FILES-005	ALLOCATE MORE THAN THE MINIMUM FSVM CPU AND MEMORY RECOMMENDED FOR YOUR PLANNED WORKLOAD
Justification	The recommended FSVM configuration for SMB environments is the minimum to support the specified number of users. Allocating more than the minimum will help ensure better performance and avoid under sizing.
Implication	Allocating more than the minimum memory and CPU for FSVMs may lead to over-allocated resources. You can always scale-up FSVM resources to improve performance or support more users online when needed.

Number of File Server Instances

Many environments will need to deploy multiple file server instances on the same hardware. Some of the considerations for deploying multiple file servers include:

- Replacing an existing file server environment with multiple namespaces. Each file server instance represents a namespace.
- Different remote replication (RPO) requirements.
- Multiple untrusted Active Directory domains. Nutanix Files supports one registered Active Directory per file server instance. Domain trusts are required for accessing a common file server.
- File server administration between different teams or tenants may require multiple file servers with separate management domains.
- Nutanix Files supports one external VLAN per file server instance. Non-routed VLANs may require their own file server instances.

Once the number of file server instances is determined, you can then determine the total compute requirements per physical node.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1217

Table 176: Minimum Number of File Servers

FILES-006	USE THE MINIMUM NUMBER OF FILE SERVER INSTANCES FOR YOUR NEEDS.
Justification	Using the minimum number of file server instances helps simplify management and reduce wasted resources.
Implication	Single, large file server instances can result in longer maintenance operations, such as scaling-up or upgrades.

File Server Networking

It's recommended that the file server client network be in close relation to the clients accessing the shares for best performance. It's also recommended that you place the file server storage network on the same VLAN as eth0 of the CVM. A flat non-routed storage network for iSCSI traffic will ensure the best performance.

Table 177: File Server Storage Network

FILES-007	PLACE THE FILE SERVER STORAGE NETWORK ON THE SAME VLAN AS THE eth0 INTERFACE OF THE CONTROLLER VMS.
Justification	Using the same network VLAN for the FSVM storage network and the CVM iSCSI network ensures the best performance.
Implication	Files does not currently support the iSCSI network segmentation feature of AOS. For security purposes, some environments may require complete separation of the iSCSI network from any management network.

Table 178: Shortest Route Between Client and Server

FILES-008	PLACE THE FSVM CLIENT NETWORK SO IT USES THE SHORTEST NETWORK ROUTE FOR THE MAJORITY OF FILE SERVER CLIENTS.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1218

Justification	Ensuring the shortest route between client and server will give the best performance for your end users and applications.
Implication	Creating file servers with networks local to your end users can improve performance but may lead to more complex environments, increasing administrative burden.

Standard Shares or Distributed Shares?

Distributed shares are recommended for the majority of use cases. Distributed shares will help to ensure data is hosted by all FSVMs. Data must be spread across multiple top-level directories within a distributed share to ensure load balancing. Standard shares use an individual volume group and can only scale to 280TB (with the Files 3.7 release). Standard shares are also only hosted by one FSVM at a time. Multiple standard shares would be needed to load balance an environment across FSVMs.

Table 179: Utilize Distributed Shares

FILES-009	USE DISTRIBUTED SHARES
Justification	Distributed shares provide automatic load balancing of top-level directories across FSVMs. Distributed shares help to limit the number of shares needed to load balance an environment, simplifying administration.
Implication	Distributed shares do not support files in the root of SMB shares today (Files 3.7 has support for NFS). Using the Nutanix Files MMC to manage top level directories can add some complexity to administration.

Storage Capacity Utilization and Sizing

Nutanix Files leverages the core data services of the Nutanix platform, including fault tolerance and replication factor options. For data reduction, inline LZ4-based compression per file share (performed by Nutanix Files) and erasure coding at the storage container level are recommended.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1219

Deduplication is not recommended. Any storage sizing exercise for Files should take into account the potential for savings based on both compression and erasure coding. File types should also be taken into account. For example, file types like video and image data will not benefit from storage compression. Cold data benefits from erasure coding.

Storage capacity consumed by self-service snapshots and/or data protection snapshots should also be factored into storage sizing. Nutanix Sizer helps to determine potential capacity when considering data reduction, snapshot overheads and change rates for Nutanix Files workloads.

Table 180: Compression

FILES-010	USE FILE SERVER SHARE-LEVEL INLINE COMPRESSION
Justification	Compression provides considerable space savings with minimal performance impact in Files environments.
Implication	Small potential for performance impact.

Table 181: Erasure Coding (EC-X)

FILES-011	USE AOS CONTAINER-LEVEL ERASURE CODING
Justification	Considerable storage space savings will be obtained by ensuring EC-X is enabled in Files environments.
Implication	Files environments with heavy overwrite activity could see a performance impact with EC-X enabled.

Table 182: Deduplication

FILES-012	DO NOT ENABLE AOS CONTAINER-LEVEL DEDUPLICATION
Justification	Testing has shown minimal space savings benefits when using storage container deduplication with Nutanix Files.
Implication	A small amount of additional space utilization may occur.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1220

Table 183: Scheduling Snapshots

FILES-013	USE TELESCOPING SNAPSHOTS SCHEDULES
Justification	Telescoping schedules (x hourly, y daily, z weekly) ensures efficient space utilization while minimizing performance impact.
Implication	Keeping fewer long-term snapshots limits fine-grained recoverability over time.

Disaster Recovery

Nutanix Files supports both async and nearsync replication. Files deployments commonly use storage-dense nodes which historically have had snapshot frequency limitations when using AOS based data protection.

Nutanix Files 3.8 introduces Smart DR. With Files Smart DR the replication engine is no longer managed by the AOS clusters using native Nutanix protection domains. Nutanix Files now directly manages the replication. Because Files manages replication, node density limits specific to AOS snapshots and replication no longer apply. You can now use our most storage-dense nodes, which support up to 350TB of hybrid storage, with the benefits of native remote replication.

If you choose to continue to use AOS based snapshots and replication, follow the node density, SSD, and CVM compute requirements for your expected RPO. Read more in the Data Protection Guide.

Table 184: Disaster Recovery

FILES-014	USE THE MINIMUM NUMBER OF DISASTER RECOVERY SNAPSHOTS NEEDED FOR YOUR BUSINESS RPO REQUIREMENTS.
Justification	Keeping a smaller number of short duration snapshots ensures the most efficient storage utilization.
Implication	Retaining fewer long-term snapshots limits fine-grained recoverability over time.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1221

Table 185: Disaster Recovery

FILES-015	USE FILE ANALYTICS
Justification	File Analytics provides native auditing, anomaly detection, data age categorization, reporting and ransomware protection. These features help you better understand your unstructured data and can protect you from unwanted activity.
Implication	File Analytics consumes additional compute and storage resources on your cluster. The File Analytics release notes provides guidance on sizing your File Analytics VM.

Nutanix Objects for Integrated Object Storage

Key Design Objectives

Table 186: Design Objectives

DESIGN OBJECTIVES	DESCRIPTION	NEW / UPDATE / REASONING

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1222

Enable S3-compatible object store within Nutanix clusters	Nutanix Objects lets you create flexible object stores suitable for a variety of use cases. Features include: - Mixed or dedicated clusters - Flexible storage options - Advanced storage efficiency - Multiple object stores per cluster - Object stores spanning multiple clusters - Versioning - WORM - Object lock - Data protection and DR	New

Architecture Overview

Nutanix Objects is an S3-compatible, software-defined, scale-out object storage solution. Nutanix Objects leverages Nutanix AOS for its core storage, network, virtualization (AHV and ESXi) and compute requirements. Management of Nutanix Objects is performed from Prism Central.

Nutanix Objects is deployed as a set of Kubernetes Pods running on top of the Nutanix Microservices Platform (MSP). MSP is a fully managed Kubernetes deployment, where the entire lifecycle is managed by the Nutanix platform. There are two types of services which are deployed on MSP, Objects Worker Nodes (Workers) and Objects Load Balancers.

Nutanix Objects deployments can start as small as three nodes and scale-out across multiple AOS clusters. This multi-cluster scalability ensures that you can build large-scale Objects deployments with petabytes of data and billions

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1223

of objects. Objects deployments can live on dedicated AOS clusters (Objects Dedicated) or be deployed alongside existing workloads.

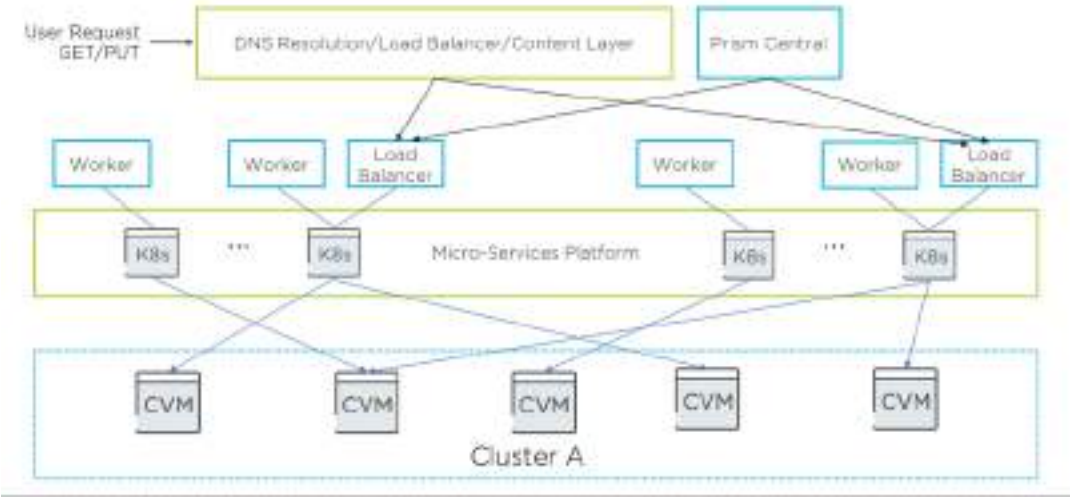


Figure 94: Nutanix Objects Deployments

Multiple Objects instances can run on the same HCI cluster. These instances can represent different namespaces (ex. customer-a.domain.tld, customer-b.domain.tld) or different use-cases (ex. backups.domain.tld, splunk.domain.tld). Each instance can scale from three Workers to 31 Workers in a single cluster.

For Object Stores with three or more Workers, high availability during node failure and Objects upgrades are performed at the object server level. All API requests for objects are redirected to other Workers by the Load Balancers during an HA or Upgrade event. For single-node Objects instances (Dev/Test use cases), hypervisor HA is utilized during HA or Upgrade events.

Each Worker has two networks: An Internal network and an External network. Each Load Balancer (has two networks as well: An Internal network and an External network, used for client access. The Worker utilizes the Internal network interface to communicate to the Load Balancer, while the Load Balancer utilizes its External network interface to communicate with clients utilizing the S3 API protocol.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1224

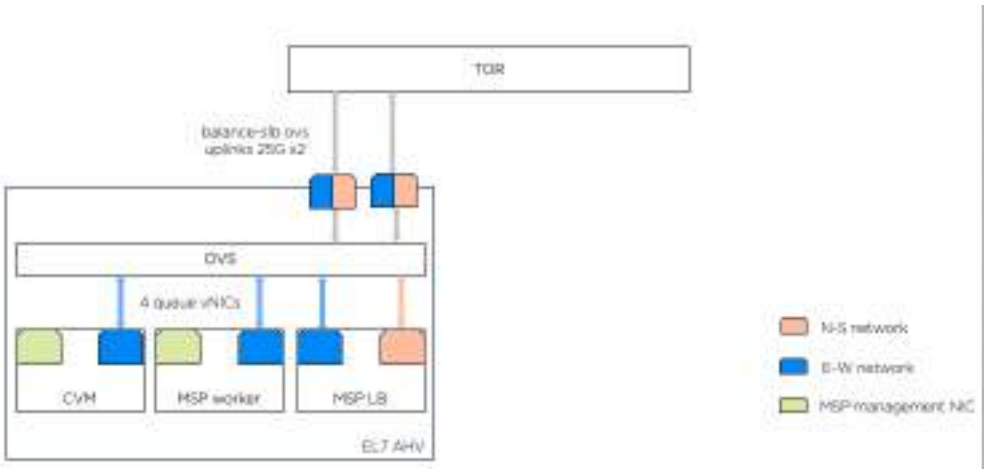


Figure 95: Internal and External Networks

Hints about the physical location of the metadata are stored at the Objects layer, enabling faster reads. This is because the hint can be passed for the lookup at the CVM layer, and we can skip the vBlock lookup. This keeps the latency for time-to-first-byte low.

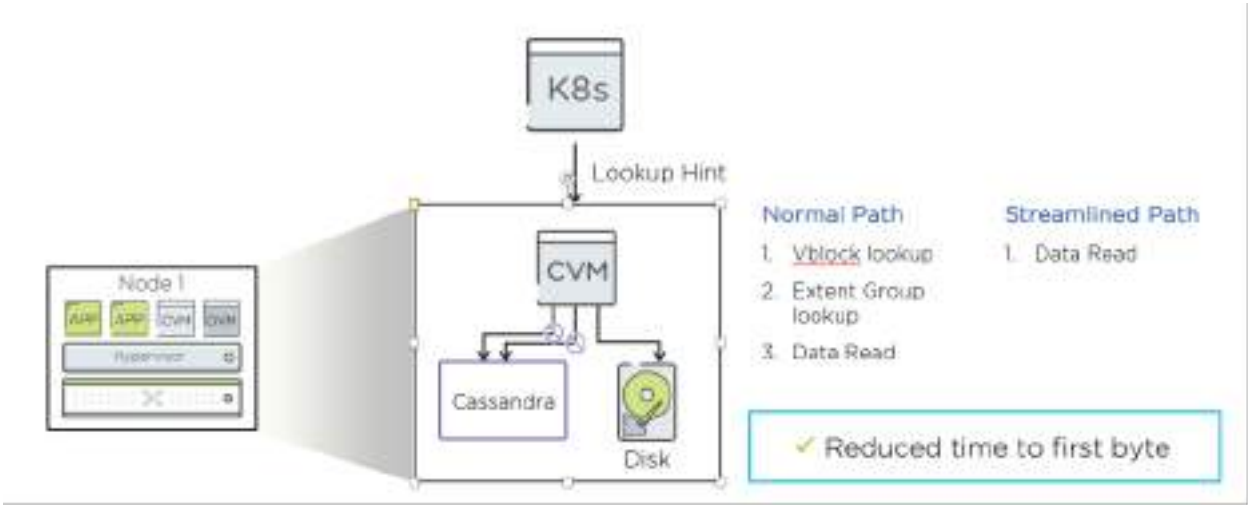


Figure 96: Lookup Hints

For business continuity, Nutanix Objects has replication built in. Streaming replication allows objects to be replicated at the bucket level from one cluster to another. Given that objects are inherently immutable—meaning a particular object cannot be edited—having a replicated copy of the object that may or

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1225

may not be versioned gives an organization a powerful business continuity option. Coupling Versioning and WORM (Write Once, Read Many) allows you to keep and store copies of objects for a set period. WORM ensures that even an administrator or Nutanix support engineer cannot delete your objects, allowing you to meet compliance needs or protect against ransomware.

Nutanix Objects may run in a mixed environment along with other workloads, or in a dedicated environment just for Objects. You can license for mixed environments with the Nutanix Objects for AOS add-on to your AOS license. Licensing for dedicated environments requires the Nutanix Objects Dedicated license. In both cases Nutanix Objects is licensed based on Used TiB from the perspective of the S3 protocol, not the amount of storage used on disk after Compression or Erasure Coding.

High-Level Design Considerations

Objects Networking

Table 187: An Object Store Requires Internal and External Networks

OBJECTS-001	PROVIDE INTERNAL AND EXTERNAL NETWORKS
Justification	The internal network is used for communication between the components of an object store. The external network is used for client communication.
Implication	N/A

The Internal network needs to have IPAM enabled for that network in AHV. See the Network Configuration section of the documentation for more info.

Mixed or Dedicated Environments?

Table 188: Mixed or Dedicated Objects Clusters

OBJECTS-002	MIXED OR DEDICATED OBJECTS CLUSTERS?

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1226

Justification	Mixed Objects clusters, combining Objects and production workloads, are most often used for small deployments or alongside applications that are actively utilizing object-based storage. Dedicated Objects clusters are for large object-based storage deployments, such as backup/archive, big data, or object stores where a high level of performance is desired.
Implication	Mixed clusters will be utilizing resources alongside production workloads, so proper sizing of existing environments must be considered. Dedicated clusters will require their own hardware, which includes the need to size for rack space, power, cooling, networking, and many other physical factors.

Whether to deploy Nutanix Objects in a mixed or dedicated environment is mostly determined by your workload needs. Like any other workload, the compute and storage density of your applications, performance requirements, failure domain, management domain and other considerations need to be weighed.

Hybrid Storage or All Flash Clusters

Table 189: Hybrid or All Flash Clusters

OBJECTS-003	HYBRID OR ALL FLASH AOS CLUSTERS

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1227

Justification	Hybrid clusters that combine HDD and flash storage are used for very large deployments where the cost per TB of raw capacity is the most important concern. Use-cases for Hybrid clusters often include backup, archive, and big data. All Flash clusters are used for smaller deployments or when high levels of performance and the lowest application latency are required.
Implication	Hardware costs are often much higher for All Flash clusters vs Hybrid.

Given that objects are write-cold, the decision between Hybrid vs All Flash infrastructure primarily comes down to workload access patterns and cost. If access patterns are highly random and need very low latency, then consider All Flash. If workloads are highly sequential (e.g., Backup/Archival) hybrid may be best. Utilizing Nutanix's standard sizing methodologies is usually the best way to size infrastructure for Nutanix Objects.

Storage Efficiency

Table 190: Enable Compression

OBJECTS-004	Enable Compression
Justification	Enable compression for all workloads. Erasure Coding is enabled for all Nutanix Objects deployments by default.
Implication	Compression can significantly reduce storage consumption for many data types.

Nutanix Objects utilizes AOS and all its storage efficiency capabilities to ensure that your object store consumes storage as efficiently as possible. After seven days, all objects are erasure-coded because Objects utilizes a "never overwrite" architecture by design.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1228

Number of Worker Nodes Per Object Server Instance

Table 191: Number of Worker Nodes

OBJECTS-005	NUMBER OF WORKER NODES
Justification	The number of worker nodes should first be based on resiliency requirements. For anything other than Dev/Test, multiple workers are recommended. Light, medium, or heavy performance configurations can be chosen based on your application's required requests per second.
Implication	More memory and CPU capacity are needed as the number of worker nodes increase.

Nutanix Objects is a scale-out platform rather than scale-up. As performance needs increase, you simply add more workers.

Recommended Configurations:

- Light Performance (1,000 requests per second) – (3) Workers, 10vCPU/32GB Memory each, (2) Load Balancers, 2vCPU/4GB Memory each
- Medium Performance (10,000 requests per second) – (4) Workers, 10vCPU/32GB Memory each, (3) Load Balancers, 2vCPU/4GB Memory each
- Heavy Performance (20,000 requests per second) – (5) Workers, 10vCPU/32GB Memory each, (4) Load Balancers, 2vCPU/4GB Memory each
- Custom – Scale out worker nodes as performance needs increase. Maximum number of worker nodes is equal to the number of nodes in an AOS cluster. A maximum of (4) Load Balancers can be deployed
- Single Node – (1) node deployments for Dev/Test can be created by choosing a custom deployment and setting the resources to 10vCPU/32GB Memory

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1229

Multiple Object Store instances

Table 192: Multiple Object Stores

OBJECTS-006	MULTIPLE OBJECT STORES
Justification	Multiple object stores can be deployed on a single cluster to support: - Multi-tenancy: Requires authentication across multiple domains. - Different VLANs: In a highly segmented network with routing concerns between VLANs, a customer may choose to deploy multiple object store instances across each network.
Implication	More resources (CPU, Memory) will be required for the additional Worker and Load Balancer nodes. Prism Central and all AOS nodes will need to have trunked access to all VLANs needed for deployment.

Nutanix Objects supports deploying multiple Object Store servers. This allows you to deploy multiple instances based on your requirements. This could be used in a multi-tenant situation, different networks, etc.

Multi-Cluster Object Stores

Table 193: Multi-Cluster Object Stores

OBJECTS-007	MULTI-CLUSTER OBJECT STORES

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1230

Justification	Very large, multi-petabyte object stores can be spread across more than one AOS cluster. This can also allow you to utilize land-locked storage in other clusters to scale out the storage available to Nutanix Objects.
Implication	All clusters utilized for multi-cluster object stores must be within the same datacenter and registered to the same Prism Central instance.

Since Nutanix Objects utilizes Nutanix AOS for storage, it is important that clusters are sized to meet AOS recommendations. For very large multi-petabyte object stores, you may split the object store across multiple AOS clusters.

Objects enables you to utilize storage from other AOS clusters within your datacenter. For large, multi-rack object stores you can utilize Nutanix Objects to deliver a very large namespace spread across multiple clusters and even multiple hypervisors.

Multi-cluster object stores are also useful when you need to utilize "land-locked" storage from other Nutanix clusters, ensuring you utilize your existing capacity efficiently.

Versioning

Table 194: Enabling Versions

OBJECTS-008	ENABLE VERSIONING?
Justification	Versioning is used when an application or organization needs to retain the old versions of changed objects.
Implication	Each version is another copy of the data that lives on disk. Additional capacity is utilized to store the old versions.

Object versioning ensures that previous versions of an object are kept when the object is overwritten with a PUT or POST. Previous versions can be set to be deleted after they reach a certain age.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1231

WORM (Write Once, Read Many)

Table 195: WORM

OBJECTS-009	WORM (WRITE-ONCE, READ-MANY)
Justification	Versioned WORM can be used when an application requires that a DELETE request for an object must occur, but the organization needs to retain the previous version of that object for a specified period. Versioned WORM can be used when an application requires that a DELETE request for an object must occur, but the organization needs to retain the previous version of that object for a specified period. Non-versioned WORM is used when an organization wants to block any DELETE operations on the objects in a particular bucket.
Implication	Versioning utilizes additional storage.Objects effected by a WORM policy cannot be deleted, utilizing cluster storage for the period specified in the policy. Objects effected by a WORM policy cannot be deleted, utilizing cluster storage for the period specified in the policy.

Nutanix Objects supports versioned and non-versioned WORM. WORM ensures that no one can permanently delete any object within a specified window of time (e.g., 3 years). WORM is set at the bucket level.

WORM is very useful for protecting against ransomware, as the object store will deny any object changes or deletions.

Versioned WORM allows DELETE operations to occur, causing the current version of an object to be labeled as a previous version, while retaining no current version. This is useful when the application needs to be able to do

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1232

DELETE operations, but the organization requires that the object be retained for a certain period.

Non-versioned WORM will not allow any DELETE operations to occur on any object in a bucket with WORM enabled.

Object Lock

Table 196: Object Lock

OBJECTS-010	OBJECT LOCK
Justification	Used for applications that require the ability to set WORM policies on individual objects via API (e.g., Veeam).
Implication	Objects clusters must be sized for additional storage requirements for objects marked with WORM policy.

Object Lock is object-level WORM that can be set per object by applications via APIs.

Lifecycle Policies

Table 197: Lifecycle Policies

OBJECTS-011	LIFECYCLE POLICY
Justification	A Lifecycle policy can be set when an application or organization requires the ability to delete objects after they reach a certain age. This is often used in conjunction with a WORM policy to ensure that objects are kept for the amount of time necessary to meet regulations, but no longer than that.
Implication	Objects are automatically deleted once they reach the specified age. Ensure this is the desired behavior or retain replica copies on another cluster using streaming replication.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1233

Lifecycle settings on a bucket allow you define the time when objects are permanently deleted. WORM settings always take precedence over Lifecycle settings, ensuring objects are kept for the required amount of time.

Streaming Replication

Table 198: Streaming Replication

OBJECTS-012	STREAMING REPLICATION
Justification	Backups of objects need to be stored off-site or be made highly available across multiple sites.
Implication	Duplicate hardware required for secondary object store. Prism Central at both sites must be set up as an Availability Zone in order for Streaming Replication to see both sites.

Nutanix Objects has built in, object-based replication. Streaming Replication enables you to replicate objects from one cluster to another with an RPO that can be measured in seconds.

Nutanix Mine for Integrated Backup

Key Design Objectives

Table 199: Nutanix Mine Design Objectives

DESIGN OBJECTIVES	DESCRIPTION	NEW / UPDATE / REASONING
Enable integrated backup	Nutanix Mine integrates backup into the Nutanix ecosystem using Nutanix-controlled infrastructure as a backup target and integrating with proven third-party data protection solutions.	New

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1234

Architecture Overview

Nutanix Mine is an integrated backup solution, combining the performance, scalability, and ease of use of Nutanix HCI with the robust feature set of industry-proven backup vendors. Nutanix Mine automates the provisioning of your secondary storage solution, optimizing performance and ensuring adherence to backup vendor best practices.

Mine can be purchased and configured in a number of predefined sizes and can be scaled-out as needed:

Table 200: Nutanix Mine Configurations

	XSmall	Small	Medium	Scale-out
Rack Size	2U	2U	4U	2U
# of Nodes	4	4	4	2
Raw Capacity	48 TB	96 TB	192 TB	96 TB
Usable Capacity (Extent store in N+1)	15TB	30TB	60TB	+40TB
Effective Capacity (assuming 2:1 comp/ dedup	30-50 TB	60-100 TB	120-200TB	60-100TB
Scale-out unit	XS	Single NX8235-G7	Single NX8235-G7	-

At the time of this writing, Nutanix Mine supports two backup vendors: Veeam and HYCU. For future Mine supported backup vendors, reference the Mine section in the Nutanix Portal Documentation

Veeam

Veeam Backup & Replication (VBR) provides a full suite of backup capabilities for all Nutanix-supported hypervisors as well as physical workloads. In addition to VM workloads, Veeam supports the ability to back up Nutanix Files.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1235

- VBR leverages a distributed architecture in which backup components such as Backup Proxies, Backup Repositories, and management consoles can be deployed in multiple sites as needed, to maximize performance and minimize performance bottlenecks.
- Veeam leverages Microsoft Windows as its underlying operating system for the VBR server as well as Backup Proxies for vSphere and Hyper-V hypervisors. Configuring backup jobs for vSphere, Hyper-V, and physical workloads is performed within the VBR management console.
- For Nutanix AHV, a separate Linux-based Veeam AHV Backup Proxy is deployed on the AHV cluster(s) you wish to back up, and backup job configuration and management is performed via a separate web interface.
- Backup jobs are defined on a per-VM-group basis, with backup schedules, archival implementation, and RTO and RPO targets defined by the user for each group.
- Veeam supports the ability to tier to S3-compatible object storage, which, with its WORM capabilities, can help defend against ransomware attacks.

HYCU

HYCU provides native Nutanix backup support with an emphasis on simplicity and ease of use via web-based administration and configuration. HYCU supports:

- Backup for Nutanix AHV and VMware vSphere workloads with native Nutanix snapshot awareness.
- Use of Nutanix Change File Tracking (CFT) APIs for optimized backup of Nutanix Files.
- Ability to back up physical servers as well as integrated application awareness for Oracle Database, SAP HANA, Microsoft SQL Server, and others.
- The ability to backup directly to an S3-compatible object store as well as the ability to schedule an archival job to replicate backups from the Mine appliance to object storage.

HYCU closely integrates with Nutanix Disaster Recovery Replication technology to allow for a distributed architecture and to accommodate ROBO workloads in

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1236

which native Nutanix snapshots replicated via Nutanix Protection Domains can be leveraged within the HYCU backup solution.

High-Level Design Considerations

Choosing a Backup Vendor

Table 201: Choose a Backup Vendor

BAC-001	CHOOSE A BACKUP VENDOR TO USE WITH NUTANIX MINE
Justification	Choose a backup vendor from the list of qualified vendors for use with Mine.
Implication	Your current backup vendor may not be qualified.

When deciding which Mine Backup solution to use in your deployment, the choice comes down to which solution best meets your business and technical requirements and your budget. Key areas to consider when choosing a backup vendor are:

- Primary workload support (including legacy and current OSes, applications, and File Storage)
- Backup and retention requirements
- Staff skill set and training (architecture, administration, daily operations)
- Scalability of the solution
- Licensing costs and model (including existing licensing agreements)
- Integration with the existing environment
- Migration of existing backup repositories and data
- Management plane technical features and performance
- Simplicity or complexity of the solution
- Features or products that support only one hypervisor or the other
- Satisfaction with existing backup solution(s)

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1237

- ROI/TCO of the full stack

Freedom of choice is a key tenet of Nutanix. After considering these factors, it is likely that one backup platform stands out as the best option for your deployment. No matter which backup software you choose, the solution is backed by world-class Nutanix support as well as the chosen backup vendor's support.

Deploy Mine in Conjunction with Nutanix Objects

Table 202: Utilize Objects for Archival

BAC-002	UTILIZE NUTANIX OBJECTS AS AN ARCHIVAL TIER FOR BACKUPS
Justification	Both Veeam and HYCU support S3-compatible object stores, so you can deploy Nutanix Objects as an archival tier with either option for ransomware protection and operational and cost efficiency. Optionally HYCU can be deployed to backup directly to an S3-compatible object store
Implication	May require additional licensing for Nutanix Objects.

Nutanix Mine can be deployed in a number of configurations depending on backup storage capacity and performance. Because both Veeam and HYCU support offloading backups to an S3-compatible Object Store, Nutanix Objects can be leveraged as an archival tier for backups. Using Nutanix Objects in conjunction with a Nutanix Mine deployment offers the following benefits:

- Ransomware protection: By using WORM-enabled Buckets and Objects' S3-compatible Object Lock API, backups can be protected against ransomware and deliberate or accidental deletion.
- Greater flexibility: With the use of Nutanix Objects, backup administrators can choose to keep backup data on either or both the Mine Cluster and Object Store and leverage the benefits of Objects Replication to distribute backup copies across datacenters or regions.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1238

- Cost-efficiency: For long-term retention requirements, administrators can choose to tier off backups to Objects and free up Mine Secondary storage for more recent or higher priority backups

The following diagram highlights the different architectural patterns in which Nutanix Mine can be deployed across single or multiple datacenters and/or regions.

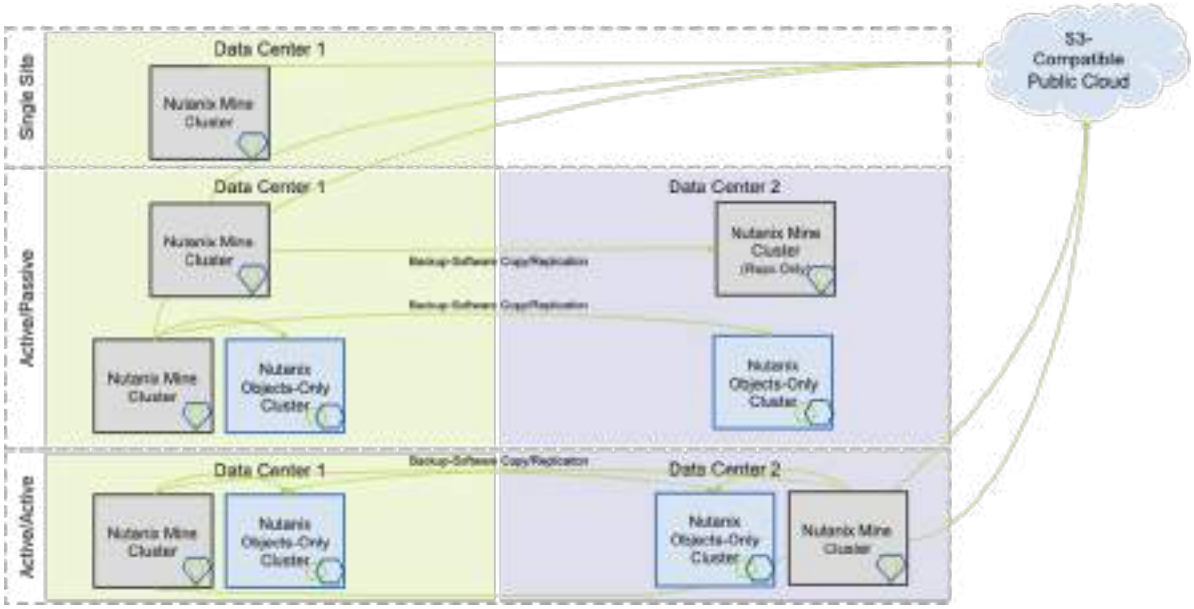


Figure 97: Mine Deployments Across Datacenters or Regions

Calm Application Orchestration

Key Design Objectives

Table 203: Nutanix Calm Design Objectives

DESIGN OBJECTIVES	DESCRIPTION	NEW / UPDATE / REASONING
Private/Public cloud automation and lifecycle management	Virtual Machines, Bare Metal endpoints, Containers	Update

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1239

Architecture Overview

Nutanix Cloud Application Lifecycle Management (Calm) is an enterprise-grade, multi-cloud application and infrastructure lifecycle management framework. Nutanix Calm provides application lifecycle management, monitoring, and remediation to manage heterogeneous infrastructure, including VMs, bare-metal servers, and containers. Nutanix Calm supports multiple platforms and endpoints so that you can have a single self-service and automation framework that can manage your applications and infrastructure. The core automation constructs available in Calm are:

- Blueprints. Blueprints provide automation instructions for single or multiple instance(s) (VMs, containers, or native cloud services) governing application creation and lifecycle management of the instance(s). Blueprints can support instance creation, deletion, and any number of standard or custom day 2 management actions.
- Runbooks. Available with Calm version 3.x and later, runbooks provide the ability to create a set of automation tasks that are endpoint agnostic. Any day-to-day management operation that is performed manually, can be encapsulated in a Calm Runbook and executed against any service in your IT estate (VMs, bare-metal instances, containers, or native cloud services.)

Nutanix Calm includes several additional capabilities for efficient management of Hybrid Cloud automation:

- Self-service via the Calm Marketplace, the ServiceNow plugin for Nutanix Calm, or any self-service platform of your choice via Calm API integration.
- Governance via built in RBAC and project resource management
- Resource quota management (for on-premises endpoints only) via Policy Engine
- An intuitive and user-friendly GUI
- A powerful code-based approach with a Python-based Domain Specific Language (DSL) that Nutanix has released and open-sourced.
- The API-centric design of Calm enables extensibility for integration with many industry automation, configuration management, and self-service solutions such as Ansible, Terraform, Puppet, Chef, SCCM, ServiceNow, Cherwell, BMC

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1240

Remedy, etc. This enables organizations to leverage existing intellectual capital from any of these solutions, allowing for rapid deployment and a short learning/adoption curve.

Hybrid Cloud management enables you to leverage all of the Calm capabilities on non-Nutanix providers (VMWare on Nutanix and non-Nutanix infrastructure) and the major public cloud solutions (AWS, GCP, and Azure). Nutanix Calm is a native service in Prism Central and is automatically enabled in Prism Central for both single Prism Central and scale-out Prism Central deployments.

Design Considerations

Sizing Considerations and Lifecycle Management

When enabling Calm, you must choose between a small or large deployment.

Table 204: Choose a Small or Large Calm Deployment

CALM-001	SMALL OR LARGE CALM DEPLOYMENT
Justification	You can start with a small deployment and easily scale to a large deployment at a later date.
Implication	To make an informed decision, you must first familiarize yourself with the sizing parameters, requirements, and Certified Configurations in the Nutanix Calm Administration and Operations Guide. Your chosen sizing allows you to hot-add necessary resources to Prism Central instance(s) with no disruption to Prism Central services.

It is recommended to upgrade Calm to the latest version as quickly as possible when new releases become available. This allows you to leverage new features and capabilities quickly and ensures you receive the latest available fixes/patches, etc. Calm is deployed through Prism Central and tied to the same user interface. However, the two can be upgraded independently of one another. As with Prism Central, all Calm releases are Long Term Support (LTS); Calm

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1241

does not provide Short Term Support (STS) releases. See the earlier section Operations Design for information on LTS and STS.)

Table 205: Upgrade to Most Recent Calm Version

CALM-002	UPGRADE TO THE MOST RECENT VERSION OF NUTANIX CALM
Justification	The Calm product team delivers fixes, enhancements, and new features on a regular cadence. You will want to leverage these enhancements as quickly as possible. Upgrading Calm is a non-disruptive LCM function that allows Calm to be upgraded separately from Prism Central or other application services running on Prism Central.
Implication	Calm blueprints from a newer version of Calm are usable with older versions of Calm.

Infrastructure-as-Code solutions require the creation of software code and a developer mindset. Robust processes for code creation and release management are imperative. It is recommended to deploy Calm in a minimum of two separate Prism Central physical instances, one for development and one for production. Larger enterprise deployments may consider up to four separate environments if their existing datacenter architecture includes separate environments and processes for Development, Test, QA, and Prod.

With this implementation methodology, you can follow the recommendation Calm-002 and always work with the latest Calm release in the development environment, and then roll the Calm upgrades through your other environments as part of a lifecycle management. This enables development and testing of existing and new blueprints with the latest version, while at the same time supporting existing blueprints and applications via the Production Calm instance. This also allows for maintaining a previous Calm version for backwards compatibility for existing blueprints.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1242

Table 206: Deploy Calm for Development and Production

CALM-003	SEPARATE CALM INSTANCES FOR DEVELOPMENT AND PRODUCTION
Justification	Maintaining a development instance of Prism Central and Calm allows for an independent upgrade of Calm and integration testing against all blueprints and runbooks prior to upgrading in production. This provides an additional advantage in cases where new features become available, and you wish to update blueprints or even new automation blueprints or runbooks leveraging the new features prior to upgrading production.
Implication	This requires a separate instance of Prism Central (this could be a single instance even on a single node cluster) on a separate Nutanix cluster. This also adds an additional instance of Calm to manage from the point of view of RBAC access for developers, etc. This is minimal overhead especially since only automation engineers and developers will be leveraging the Dev instance. If you currently leverage a release management process, it may require updates to include Calm.

Business Continuity and Disaster Recovery

It is recommended that you create a process (automated or manual) to execute Nutanix-provided backup scripts via SSH from Prism Central to protect Calm. These scripts are documented in the Calm support documentation. If a cold Prism Central instance is not immediately available for a restore, then a new Prism central/cluster instance can be provisioned and used as a target for a Calm restore. The only risk with this approach is the impact to RTO due to having to rebuild the Prism Central instance as a new target.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1243

If you have enabled the policy engine for your Calm instance, then there is a separate script to create backups of your policy engine database. The policy engine database backup can be used to restore the policy engine to either an earlier state or to a new policy engine VM.

Table 207: Calm for DR and Backup

CALM-004	DEFINE A PROCESS FOR CALM DR AND BACKUP/ RESTORE
Justification	In the event of data corruption or loss of Prism Central, Nutanix Calm blueprints, runbooks, and configurations need to be backed up. It is recommended that the backup scripts are scheduled to run at a set time each day.
Implication	A separate “cold” Prism Central instance(s) with Calm enabled is required as a restore target for the backup/ restore script. An external scheduler is required to run the scripts via SSH. Customers with Prism Pro can use an X-Play Playbook to call a Calm Runbook to execute the backup script. Keep in mind that Prism Central has security features that limit its ability to remotely execute some SSH commands, and the Calm Runbook will need to SSH to an independent endpoint (VM or container) to run the backup command.

Management and Operations

Calm requires integration with an AD/LDAP source, and Calm can leverage Prism Central’s existing AD/LDAP configuration. Local Prism Central users cannot be used for user and role assignments in Calm. The AD/LDAP integration for Calm is tied to the Project construct. It is a best practice to align your AD/LDAP security groups to projects and roles within Calm in order to achieve the desired self-service consumption model for each project. You can create security groups for Calm projects and roles and then add AD

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1244

users to these groups to simplify access management via standard AD user authentication. (For example, for “ProjectA” all developers are assigned to a group called “ProjectADev” that is associated with the project. Adding new developers to this security group grants them access to the project resources based on their AD/LDAP credentials).

Control of project configuration (creation, group membership, etc.) can also be performed via Calm blueprints and Runbooks via API if you need a more dynamic RBAC project/resource model. This way, self-service features in Calm can be used to automate RBAC policies.

The Prism Central “admin” account can be used to gain/restore access to Calm if something happens to the Active Directory LDAP connection(s).

Table 208: Calm and RBAC Configurations

CALM-005	ALIGN PROJECT STRUCTURE AND RBAC CONFIGURATION
Justification	Design Calm Projects and Security Groups to align with AD/LDAP users and roles that are specific to entitlements for administering, developing, managing, and consuming automation constructs (blueprints, runbooks. etc.)
Implication	AD/LDAP configurations in Prism Central are required in order to leverage Calm RBAC features.

Calm has a native feature to help manage and share code across environments. End-users can select blueprints to provision into any environment in any geography at runtime. This allows blueprints to be created once and delivered to any Calm physical instance without having to manage multiple copies of the same blueprint. Through RBAC, administrators can assign users/groups to projects that control access to who can provision which blueprints in which environments. It is a good design principle to align your physical Calm instances to both your environments (e.g., Dev, Test, QA, Prod) and your deployment geographies (e.g., Americas, Europe, Asia). Here is an example of what this might look like for a global enterprise deployment of Calm.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1245

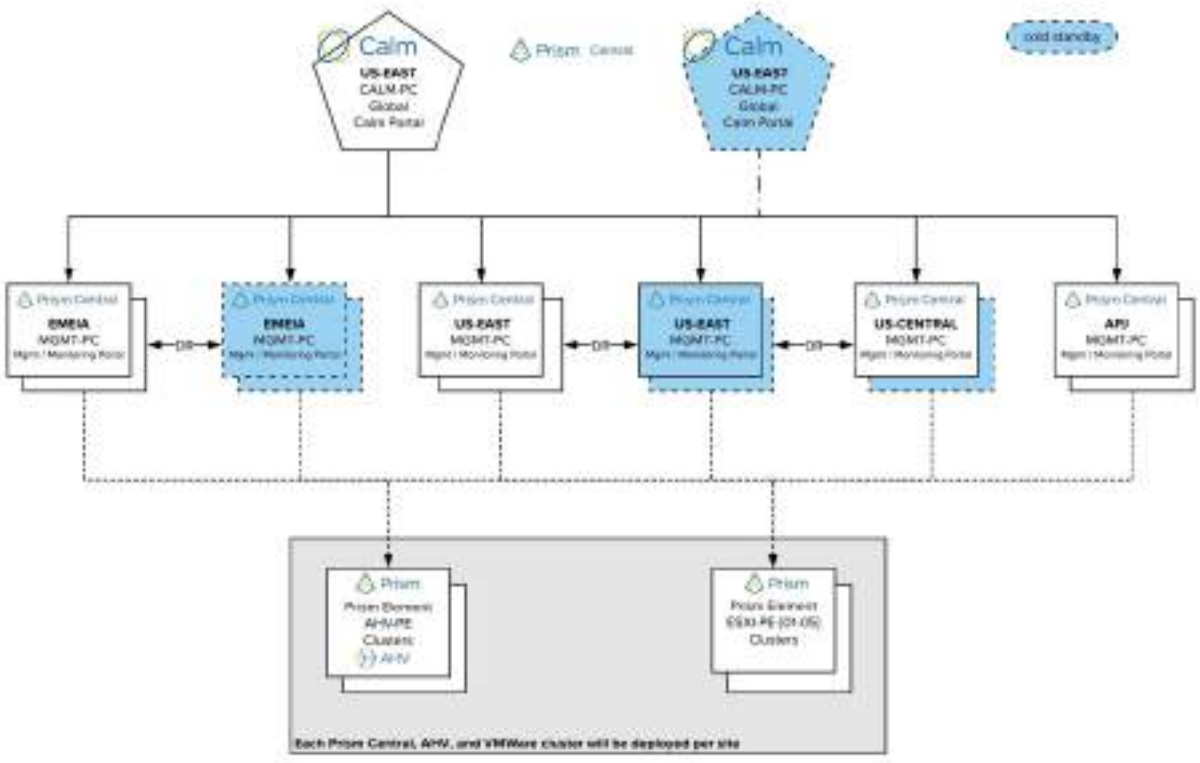


Figure 98: Global Enterprise Calm Deployment

Table 209: Calm Releases and Geographic Regions

CALM-006	DESIGN CALM ENVIRONMENT TO ALIGN WITH RELEASE METHODOLOGY AND GEOGRAPHIC REGIONS
Justification	This feature maximizes efficiency by allowing you to have one automation blueprint that can be chosen as a self-service request from end-users in the same cost center, but in different sites or geographies.
Implication	A Calm decision should be made while planning your infrastructure to establish physical clusters that align with your needs.

Nutanix Calm has the ability to set resource quotas for projects via its Policy Engine. Maximum quotas for compute, memory, and storage can be set for

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1246

projects so that the total amount provisioned by all users in the project does not exceed the threshold. When you enable the Policy Engine for a Calm instance, a new VM is created and deployed. For quota policy enforcement, VMs must be provisioned through Calm. In order to enforce the desired policy for VMs that are not provisioned through Calm, migrate the VMs to Calm once you have enabled the Policy Engine.

Table 210: Calm Policy Engine

CALM-007	ENABLE CALM POLICY ENGINE
Justification	Prevents teams from over-provisioning or hogging resources and allows you to better manage consumption among business units and projects.
Implication	You need an available IP address that belongs to the same network as that of your Prism Central VM for the Policy Engine VM.

Integration with Nutanix Beam enables showback for Calm without any additional licensing costs. Nutanix Beam is a SaaS product that helps customers optimize their multi-cloud spend. Cost calculations in Nutanix Beam are configured for you, and Beam will automatically calculate your compute, memory, and storage costs. Since Beam runs in the Public Cloud, the automatic configuration of your cost data requires an active internet connection to Prism Central. In the event you do not have an active internet connection, you can still leverage Beam showback features by manually entering your cost data. Showback is currently available for Nutanix and VMware environments.

Table 211: Showback with Nutanix Beam

CALM-008	ENABLE SHOWBACK VIA NUTANIX BEAM

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1247

Justification	Showback helps you control IT spend by tracking utilization of IT resources to each business unit. Reporting can identify how much each business unit is consuming and helps in budgeting and cost optimization. You may also be able to implement Chargeback processes whereby business units pay for their consumption on a monthly or yearly basis.
Justification	Showback helps you control IT spend by tracking utilization of IT resources to each business unit. Reporting can identify how much each business unit is consuming and helps in budgeting and cost optimization. You may also be able to implement Chargeback processes whereby business units pay for their consumption on a monthly or yearly basis.

Self-service enables end-users to create new workloads and manage existing workloads provisioned by Calm without accessing the administrative consoles or needing help from IT Admins with privileged access. Self-service can be achieved via a variety of mechanisms: the Calm Marketplace, the ServiceNow plugin for Nutanix Calm, or the self-service platform of your choice via Calm API integration. The Calm Marketplace is native to Nutanix Prism and included with Calm.

The ServiceNow plug-in for Calm may be ideal for companies who already use the ServiceNow ITSM platform; you can expose Calm services to all end-users that have access to ServiceNow. In addition, ServiceNow approvals, incidents, and CMDB updates are integrated with the Calm Plug-in. The ServiceNow Plug-in for Calm is available from the ServiceNow store and adds no additional Nutanix licensing costs. For customers who prefer to use an in -house self-service interface or some other third-party interface, Calm blueprints and runbooks can be invoked via REST API, enabling easy integration.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1248

Table 212: Self-Service with Calm

CALM-009	CHOOSE A METHOD FOR SELF-SERVICE
Justification	Self-service allows end-users to perform provisioning and Day 2 operations without the need for privileged access or assistance from IT Admins.
Implication	Potential third-party licenses needed for self-service integration are not provided by the Calm Marketplace.

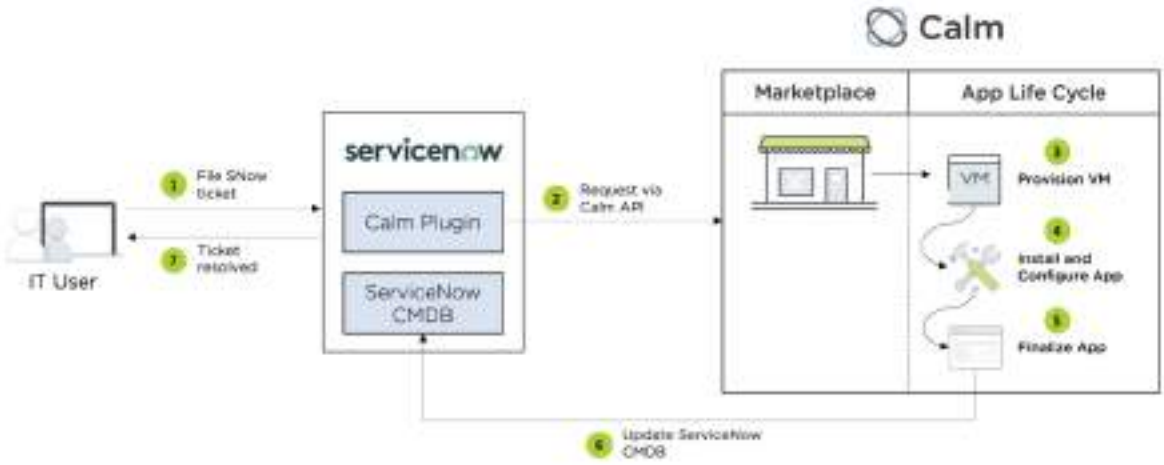


Figure 99: Self-Service with Calm

Karbon for Kubernetes and Container Support on Nutanix

Key Design Objectives

Table 213: Nutanix Karbon Design Objectives

DESIGN OBJECTIVES	DESCRIPTION	NEW / UPDATE / REASONING
Enable support for containers and Kubernetes	Nutanix Karbon enables teams to incorporate containers and Kubernetes as part of the Nutanix ecosystem with simplified provisioning and management.	New

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1249

Architecture Overview

Nutanix Karbon is an enterprise-grade Certified Kubernetes distribution that simplifies the provisioning, operations and lifecycle management of Kubernetes, all from within Nutanix Prism. Karbon is an opt-in service running on Prism Central; upon enablement, Karbon Core and Karbon UI docker containers are instantiated on Prism Central VM(s), allowing you to be up and running in 5 to 10 minutes.

Once enabled, Nutanix Karbon can deploy and manage Kubernetes clusters to any AHV cluster that's registered to Prism Central. Any number of Kubernetes clusters can be deployed with any configuration, assuming adequate resources on the physical clusters. Day 2 management operations, such as host OS upgrades, Kubernetes version upgrades, storage class management, and worker node additions or removals are feasible via the UI or APIs.

The UI provides a mechanism to download a hardened host OS image provided by Nutanix (which is similar to the CVM) in a single click. Nutanix quickly reacts to any published security vulnerability and will push out a new host OS image with the appropriate vulnerabilities patched. Karbon admins can quickly download these new host OS images, and initiate host OS upgrades to bring a given Kubernetes cluster to the updated OS level in a couple of clicks. Alternatively, if the vulnerability is at the Kubernetes level, admins can also easily perform a Kubernetes version upgrade.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1250

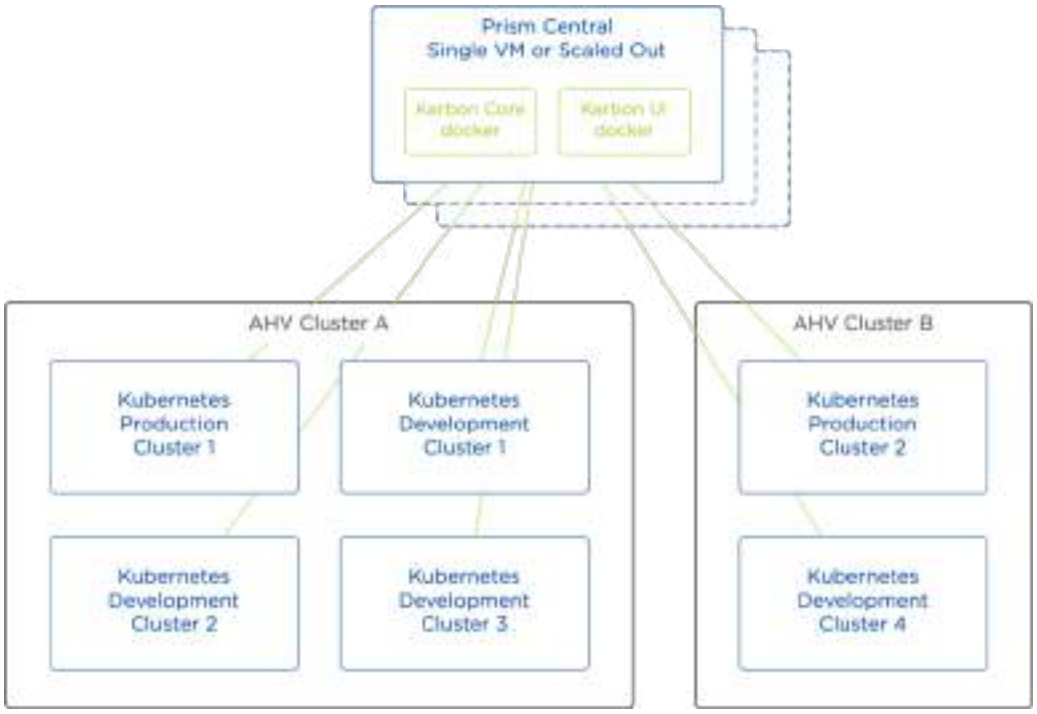


Figure 100: Karbon Provides a Single Control Plane for Multiple Kubernetes Clusters and Locations

Karbon can deploy both development and production Kubernetes clusters, depending upon use case. Development clusters are restricted to a single master node (which runs the Kubernetes control plane), a single ETCD node (Kubernetes' key-value store), and any number of worker nodes (which run end-user applications). The number of worker nodes can be specified during cluster creation and can be increased or decreased at any point in the cluster's life. Due to the single master and ETCD nodes, these clusters cannot tolerate failures in the control plane, and applications will experience downtime during upgrades. However, they're light on resources, making them perfect for development.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1251

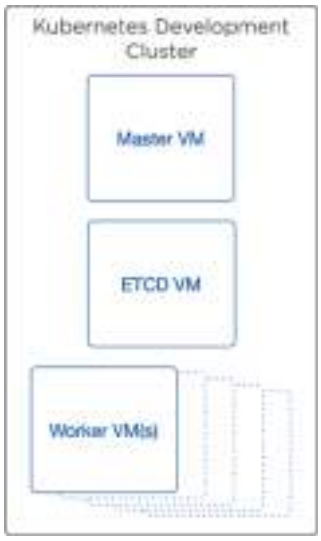


Figure 101: A Karbon Development Cluster is not Highly Available

Production Kubernetes clusters deployed by Nutanix Karbon have two master nodes in active-passive mode by default, utilizing VRRP for high availability. If the active master node goes down (either due to an upgrade or loss), the passive node will assume the virtual IP and the cluster will continue to function.

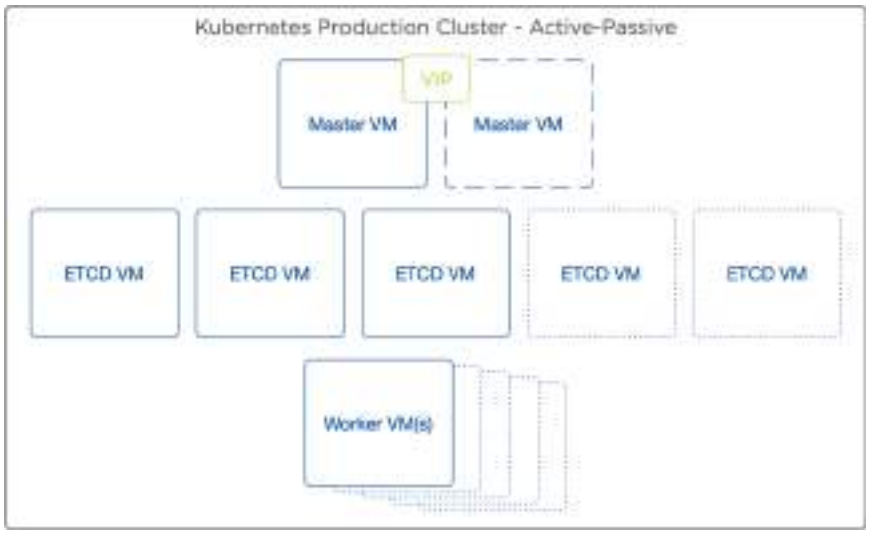


Figure 102: A Karbon Cluster for Production is Highly Available

Alternatively, if you have an external load balancer, anywhere from two to five master nodes can be deployed in an active-active configuration. This increases

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1252

performance, and as long as a single master node is online, the cluster continues to function.

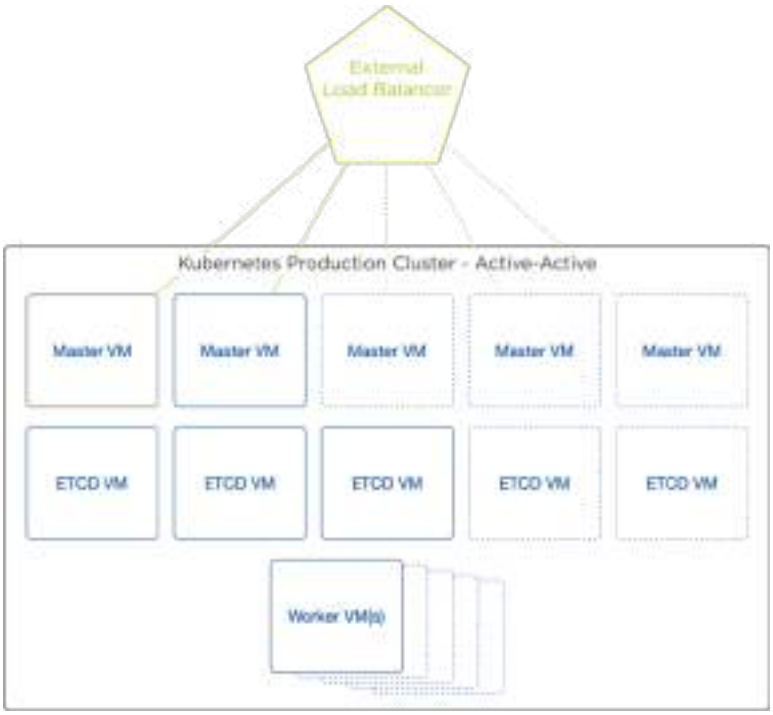


Figure 103: An External Load Balancer Enables Karbon to Have More than Two Master Nodes

Either three or five ETCD nodes can be deployed for production clusters; three enables the cluster to sustain a single ETCD node failure, and five enables two ETCD nodes to fail without causing a disruption. Stated differently, a quorum of two is required when three ETCD nodes are used, and a quorum of three is required when five nodes are used. As with development clusters, any number of worker nodes can be deployed at cluster creation, and later modified to scale with workload changes.

During deployment, admins are able to choose the physical network and VLAN which the nodes that make up the Kubernetes cluster belong to. All nodes must live in the same network. For development clusters, these networks can be backed by a DHCP server, or can utilize AHV managed networks (IPAM). For production clusters, you are required to select an AHV managed network. For Kubernetes cluster networking, either the Flannel or Calico CNIs can be utilized.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1253

Nutanix Karbon Kubernetes clusters have the Nutanix CSI driver installed during cluster creation for persistent storage. A default storage class based on Nutanix Volumes is also defined and created during cluster creation, which provides Read Write Once storage (RWO). After cluster creation, any number of additional storage classes based on either Nutanix Volumes or Nutanix Files, which provides Read Write Many (RWX), can be created.

Karbon admins are also able to download a secure, 24-hour valid kubeconfig file from the Karbon UI, which allows for kubectl usage, which is the standard Kubernetes command line interface. This effectively provides root access to the cluster. Utilizing this, Karbon admins can create Kubernetes authentication objects, such as a Role, ClusterRole, RoleBinding, and ClusterRoleBinding, for end users. End users are added (either directly or as part of group membership) via Active Directory as Nutanix Read-Only users within the role mapping configuration section of Prism Central. This allows end users to log into the Karbon UI and download kubeconfig files.

Once these authentication objects are appropriately created, Karbon end users can easily create and manage applications utilizing kubectl, assuming they have been granted privilege to do so. This includes, but is not limited to, creating Kubernetes deployments, services, persistent volume claims, persistent volumes, and stateful sets. Ultimately the types of objects end users can create or manage is dependent upon the roles configured for them by the Karbon admin.

Since Kubernetes is a cloud native technology, it is recommended to implement Business Continuity at the application level. This means running multiple instances of your applications in different regions so that, in the event of a disaster, the secondary application continues to operate. For environments or applications where this is not possible, open source tools like Velero can provide Business Continuity at the Kubernetes cluster level.

Nutanix Karbon is included in every licensed version of Nutanix software. The only requirements are at least one AHV cluster and Prism Central.

High-Level Design Considerations

When configuring Karbon, first determine the availability needs of your applications and Kubernetes clusters. Development and test workloads are

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1254

likely okay to run on development clusters with single points of failure. Any production workloads should run on production clusters designed to ensure that a single VM loss will not bring down an application or an entire cluster. Business critical workloads should be distributed across multiple production clusters in multiple availability zones to ensure availability in the event of a disaster.

Next, determine your preferred CNI, either Calico or Flannel. Generally, Flannel offers simpler configuration, while Calico has more features. It is possible to have some clusters with Flannel and some with Calico to address specific use cases, however this may complicate management.

It is recommended to use the latest version of Kubernetes supported by Karbon unless there's a specific reason for using an older version. When possible, upgrade existing Kubernetes clusters to newer versions of Kubernetes.

Utilize a consistent naming convention for Storage Classes, based on volume type (Volumes or Files), reclaim policy, file system, and performance.

Table 214: Minimize Admin Kubeconfig Use

KARBON-001	MINIMIZE USE OF THE ADMIN KUBECONFIG
Justification	The admin kubeconfig provides root access to the cluster, so regular use of it is a security vulnerability. It should only be used for initial cluster configuration. Use AD-based Prism Read-Only credentials (with the corresponding Role and RoleBinding) instead, or Kubernetes Service Accounts for automation use cases.
Implication	Configuration of Prism role mappings, and Kubernetes objects (such as Roles, ClusterRoles, RoleBindings, ClusterRoleBindings, and ServiceAccounts) must be performed before running end-user applications on a cluster.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1255

Table 215: Use Multiple Availability Zones for Production

KARBON-002	DISTRIBUTE PRODUCTION APPLICATIONS ACROSS AVAILABILITY ZONES
Justification	Production applications should run in an active-active or active-passive mode on multiple Nutanix clusters in different availability zones. In the event of a disaster, the secondary site can take over transparently.
Implication	A minimum of 2 AHV clusters and AZs are required.

Table 216: Use Namespaces to Segment Users and Apps

KARBON-003	UTILIZE KUBERNETES NAMESPACES TO SEGMENT USERS AND APPLICATIONS RATHER THAN CLUSTERS
Justification	Where possible, use of namespaces to segment work is preferable to reduce Kubernetes cluster sprawl and resource utilization.
Implication	This requires an approach to cluster configuration similar to that prescribed above in Karbon-001.

Table 217: Leave Room for a Worker Node to Fail

KARBON-004	LEAVE ENOUGH SPACE IN A CLUSTER TO TOLERATE A WORKER NODE FAILURE
Justification	Whether there is an unplanned outage, or a planned upgrade, sizing the cluster to tolerate a failure of a worker node allows applications to continue to run in the event of a failure.
Implication	At minimum, the cluster must be sized for n-+1, and workers must be added if the workload grows.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1256

Table 218: Use Consistent CIDRs

KARBON-005	UTILIZE CONSISTENT POD AND SERVICE CIDRS
Justification	Whether utilizing Calico or Flannel as the CNI provider, during cluster deployment the admin must provide a large (/16 by default) subnet for use by Kubernetes Pods and Services. While these are internal subnets which do not go over the wire, they must not overlap with physical host networking. It is recommended to utilize the same subnets for all clusters for consistency and to minimize the chance of IP overlap.
Implication	Two large subnets are needed for Karbon Kubernetes clusters which do not overlap with physical host networking.

Table 219: Keep the Host OS Updated

KARBON-006	UPGRADE THE HOST OS AS SOON AS POSSIBLE
Justification	Due to the nature of Common Vulnerabilities and Exposures (CVEs), it is critical to upgrade Host operating systems quickly whenever a new version is released. This greatly reduces the chances of a cluster being compromised.
Implication	For development clusters, an outage is required. For production clusters, there will be a single point of failure during upgrades.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1257

Era for Database as a Service

Key Design Objectives

Table 220: Nutanix Era Design Objectives

DESIGN OBJECTIVES	DESCRIPTION	UPDATE

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1258

Enable Database as a Service (DaaS	• Deliver Database as a Service (DBaaS) consumable via a user interface and REST API. • Perform a standardized and repeatable deployment of Postgres database instances. • Deploy and manage Postgres database instances in both: › HA mode › Single mode • Deploy Postgres HA instances across Nutanix clusters. • Protect (back up) database data to a location remote from the database instance. • Perform lifecycle and day2 operations for Postgres databases. • Provide copy data management functionality such as the ability to clone database instances. • Manage 100+ DB instances and DB VMs • Network communication is required between the Era management plane and the database instances managed by Era.	New

Architecture Overview

Era automates and simplifies database administration and brings one-click simplicity and invisible operations to database provisioning and lifecycle management, facilitating database as a service (DBaaS). Era

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1259

enables database administrators to perform operations such as database registration, provisioning, cloning, patching, restore, and much more. It allows administrators to define standards for database provisioning with end-state driven functionality that includes HA database deployments.

Era enables multi-cluster database management. Database administration for different databases across multiple Nutanix clusters can be performed with a single Era instance. With the extension of support for Nutanix Clusters, you can utilize all the capabilities of Era both in the cloud and on-prem.

The Era management plane operates on one or more VMs running in a Nutanix cluster with at least three Nutanix nodes (physical servers). The default Era management plane deployment in a single Nutanix cluster consists of one VM running all services:

- Front-end services (API, agent, web service).
- Back-end service (database or repository).

The following figure presents a logical implementation of Era DBaaS, including the Era management VM, database server VMs (DB), Nutanix cluster, and physical hardware

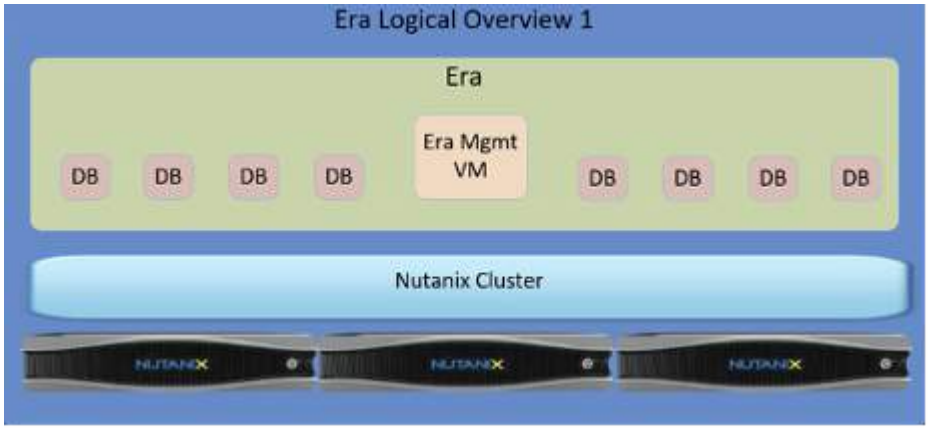


Figure 104: Nutanix Era DBaaS

In a multicluster Era environment, where Era manages database server VMs in multiple Nutanix clusters, the Era management plane requires one Era management agent VM running only the agent service in each additional Nutanix cluster it manages.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1260

The following figure expands on the previous one to include the two Nutanix clusters and two Era management agent VMs.

Figure 105: Nutanix Era VMs and DBs

It is possible to run the Era management plane in a highly available mode to avoid service disruption from a node failure. This is done by provisioning an HA PostgreSQL instance where Era deploys a multi-node PostgreSQL instance. One of the nodes in the cluster acts as the leader, and other nodes serve as replicas. The leader node is used for both read and write operations while the replicas are only used for read-only requests. When a primary node becomes unavailable, one of the replicas is promoted to the role of master, ensuring availability of the database for write operations.

When Era is deployed in a high availability (HA) configuration, it includes six VMs:

As described earlier, Era supports managing database instances across multiple Nutanix clusters. The figure below illustrates the Era management architecture in a multi-cluster scenario where C1, C2, and C3 are different Nutanix clusters.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1261

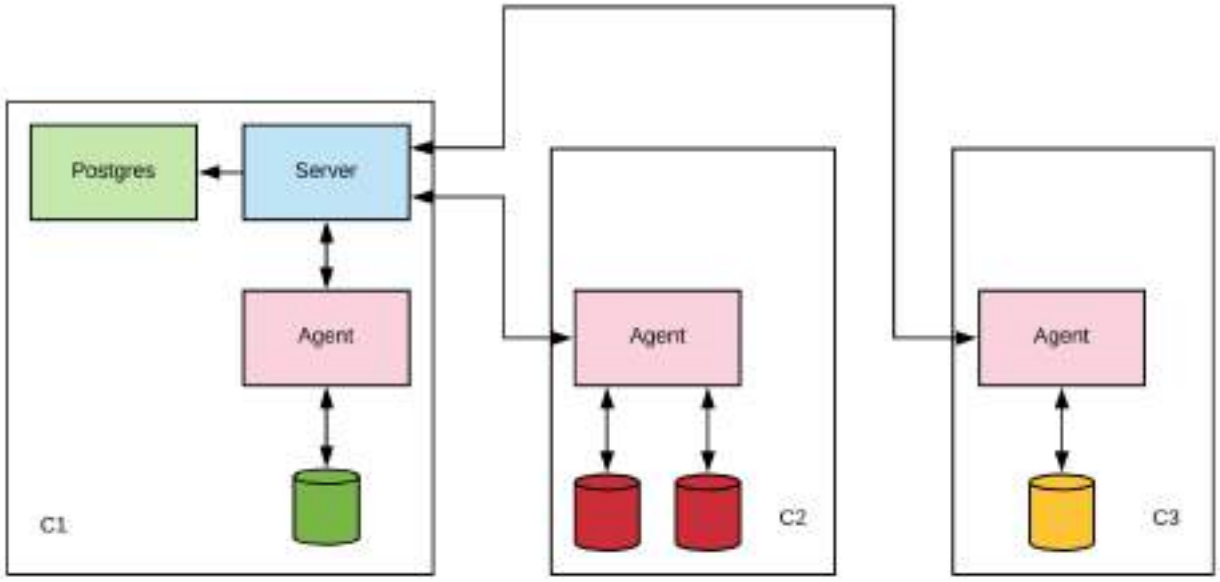


Figure 106: Era Management Layer in a Multi-Cluster Deployment

Based on the rich API provided by Era, you can automate any action available via the Era UI so that Era can easily be consumed from an overlying automation, self-service, or orchestration solution such as:

- Nutanix Calm
- ServiceNow
- VMware vRealize Automation

The Era management plane and the database instances managed by Era communicate during initial provisioning and registration, as well as during ongoing operation. Communication is mostly initiated from the database instances to the Era management plane, accept during provisioning and registration.

No specific hardware is required to run Era; it runs as a VM on any Nutanix AOS-supported hardware running Nutanix AHV or VMware ESXi.

Era employs role-based access control to govern access to an Era system. RBAC allows system administrators to restrict user access and limit the operations

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1262

they can perform. For example, a database operator can be granted access to only perform database-related operations.

With RBAC, you can add users either in Era or Active Directory and then later add those users to a group. Groups allow you to assign the same roles to multiple users at the same time. After adding a user, you can assign one or more roles to the user based on the operations they can perform.

There are multiple license options available for Era:

- License the entire Nutanix cluster
- License per physical CPU cores
- License per DB VM vCPU

High-Level Design Considerations

The design decisions presented in this section cover the Era management plane but not the database instances managed by Era.

Table 221: Era to Enable DBaaS

DBAAS-001	ENABLE DATABASE AS A SERVICE
Justification	Era can easily be integrated with overlying automation, self-service, and orchestration solutions.Era deploys DB instances with a predefined operating system, database engine binary and DB instance configuration in a repeatable fashion. Era can deploy and manage (clone, take a snapshot, perform log catchup, refresh) Postgres in single and highly availability mode in one or multiple Nutanix clusters. Snapshots of the managed database instances can be stored in the same Nutanix cluster where they are running or in remote Nutanix clusters.
Implication	N/A

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1263

Table 222: Era Hardware Requirements

DBAAS-002	MINIMUM HARDWARE REQS FOR NUTANIX CLUSTERS RUNNING ERA
Justification	The minimum configuration requirements shown below provide a solution with predictable performance. Since no specific performance requirements are established for this section, these requirements can serve as a baseline for running DB workloads.
Implication	Since workload characteristics are undefined the configuration below could be either too performant (increasing CapEx unnecessarily) or not performant enough and therefore need to be upgraded. Careful sizing should be performed for your intended DB workloads.

A Nutanix cluster supporting Era and database instances should meet the following minimum hardware requirements:

- Minimum 2.7GHz, 16-core CPUs
- An optimal memory configuration with minimum 768 GB memory per node. See Nutanix Physical Memory Configuration document for Nutanix NX recommendations.
- Minimum All flash storage
- Minimum 2x10 Gbps networks.

Table 223: Dedicated DB Clusters

DBAAS-003	USE DEDICATED NUTANIX CLUSTERS TO SUPPORT DATABASE WORKLOADS

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1264

Justification	The requirement to host more than 100 VMs justifies a minimum of two separate Nutanix clusters for database workloads to ensure that database workloads do not have to compete with non-database workloads for resources. The vCPU:pCPU ratio is typically lower for database workloads compared to other server virtualization workloads.
Implication	Hardware may be underutilized if not enough workloads are provisioned in the Nutanix clusters.

Table 224: HA Management Plane

DBAAS-004	DEPLOY ERA MANAGEMENT PLANE FOR HIGH AVAILABILITY
Justification	Provides the highest possible uptime for the Era management plane, ensuring that no changes are needed to address future changes in SLA uptime requirements. The solution protects against single-node failures.
Implication	When an Era VM providing front-end services or the hypervisor host (where the Era VM runs) becomes unavailable, there will be a short period of downtime for any user or service accessing Era.

Table 225: Management Network

DBAAS-005	PLACE ERA ON A SEPARATE MANAGEMENT NETWORK
Justification	The Era service is treated like any other management service and placed on a separate management network accordingly.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1265

Implication	Firewall openings between the network where an Era server is hosted and the network(s) where the DB workloads are hosted are required if the networks are not the same.

Table 226: Era Platform License

DBAAS-006	USE THE ERA PLATFORM LICENSE
Justification	The Platform license lets you run as many DB workloads in a cluster as permitted by the underlying hardware and your acceptable vCPU:pCPU ratio. In addition to the Era license, the Platform license also includes the Nutanix AOS Ultimate license, so both Era and AOS licenses are managed as one entity.
Implication	Some AOS Ultimate features may go unused.

Table 227: Active Directory Integration

DBAAS-007	ACTIVE DIRECTORY IS USED FOR USER, GROUP, AND SERVICE ACCOUNT ACCESS
Justification	Using AD provides a single source of truth for user, group, and service management for traceability and auditing purposes. The local Era admin account can be used to gain access to the environment for super admins if the Active Directory connection is lost.
Implication	Era requires a connection to Active Directory to provide end user functionality.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1266

Table 228: Active Directory Access

DBAAS-008	ACTIVE DIRECTORY GROUPS ARE USED TO PROVIDE ACCESS TO ERA
Justification	One place—Active Directory—is used to configure Era permissions (add and remove users from Active Directory groups) during normal operations.
Implication	Era requires a connection to Active Directory to provide end user functionality.

Table 229: Era Test Environment

DBAAS-009	AN ERA TEST ENVIRONMENT MUST EXIST
Justification	Upgrades and configuration changes must be applied and tested in a test environment before being applied in the production environment to avoid problems with new versions or upgrade processes.
Implication	An Era test system must be available.

Table 230: Service Windows

DBAAS-010	ERA UPGRADES ARE PERFORMED DURING SERVICE WINDOWS
Justification	There will be a very short service interruption during an upgrade. If a critical patch must be applied for stability or security reasons an upgrade can be performed during business hours after the service window is approved by the change control function
Implication	Could create some delay before a patch can be applied since a service window has to be requested.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1267

Table 231: Era Roles

DBAAS-0011	USE ERA SUPER ADMIN AND DATABASE ADMIN ROLES
Justification	Provides a clear division between those managing the Era solution and those consuming DBaaS
Implication	N/A

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1268

7. Conclusion

This document is intended to demonstrate valuable methods and practices that organizations, both large and small, can use to implement Nutanix Solutions to solve their IT and business problems. There is no one-size-fits-all solution for Nutanix Hyperconverged Infrastructure, and the contents of this document are informational only and intended to provide customers with suggested best practices from which they can design and evolve their private, hybrid, and multi-cloud solutions.

For more information on any details of this document, please visit our website at www.nutanix.com or reach out to our sales team. You may also contact one of our many global support phone numbers listed on our website.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1269

Appendix

Table of Design Decisions

The following table summarizes all the design decisions described in this document.

Table 232: Design Decisions

REFERENCE	DECISION NAME	DECISION
Region-001	Number of regions to be used	
AZ-001	Number of availability zones to be used	
DC-001	Number of datacenters to be used	
VRT-001	Choose Nutanix AHV or VMware ESXi as the hypervisor for your deployment.	
PFM-001	Management Cluster Architecture: Deploy a separate Management Cluster or share a cluster with other workloads. When choosing a separate management cluster, consider a redundant configuration.	
PFM-002	Mixed or dedicated workload per cluster.	
PFM-003	Select Nutanix software licensing level	
PFM-004	Select physical node vendor	
PFM-005	Select node model(s) per use case	
PFM-006	Number, type, and size of clusters	
PFM-007	Decide which workload domains will span a single or multiple racks	
NET-001	Use a large buffer datacenter switch at 10Gbps or faster.	

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1270

NET-002	Use a leaf-spine network topology for new environments.
NET-003	Populate each rack with two 10GbE or faster ToR switches.
NET-004	Avoid switch stacking to ensure network availability during individual device failure.
NET-005	Ensure that there are no more than three switches between any two Nutanix nodes in the same cluster.
NET-006	Reduce network oversubscription to achieve as close to a 1:1 ratio as possible.
NET-007	Configure the CVM and hypervisor VLAN as native, or untagged on server facing switch ports.
NET-008	Use tagged VLANs on the switch ports for all guest workloads.
NET-009	Use a Layer 2 network design.
NET-010	Connect at least one 10 GbE or faster NIC to each top-of-rack switch.
NET-011	Use a single br0 bridge with at least two of the fastest uplinks of the same speed.
NET-012	Use NICs of the same vendor within a bond
NET-013	Use VLANs to separate logical networks.
NET-014	Use active-backup uplink load balancing.
NET-015	Use standard 1,500-byte MTU and do not use jumbo frames.
NET-016	Use virtual distributed switch (vDS).
NET-017	Connect at least one 10 GbE NIC to each top-of-rack switch.
NET-018	Use a single vSwitch0 with at least two of the fastest uplinks of the same speed.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1271

NET-019	Use Route Based on Physical NIC Load uplink load balancing.
NET-020	Use standard 1,500-byte MTU and do not use jumbo frames.
CMP-001	If running a non-NUMA aware application on a VM, configure the VM's memory and vCPU to be within a NUMA node on AHV host.
STR-01	When creating vDisks in ESXi, always use thin- provisioned vDisks.
STR-02	When sizing a hybrid cluster, make sure to have enough usable SSD capacity to meet active data set of application.
STR-03	Do not mix node types from different vendors in the same cluster.
STR-04	Do not mix nodes that contain NVMe SSDs in same cluster with hybrid SSD/ HDD nodes.
STR-05	Minimum 2:1 HDD to SSD ratio required for Hybrid clusters.
STR-06	Size for N+1 node redundancy for storage and compute when sizing. For mission critical workloads that need higher SLAs, use N+2 node redundancy.
STR-07	Use FT=2 and RF=3 for workloads and clusters that need higher SLAs or for cluster sizes >32.
STR-08	Enable Inline Compression.
STR-09	Enable/Disable Deduplication.
VRT-001	Deploy scale-out Prism Central for enhanced cluster management.
VRT-002	Deploy prism central in each region or az using runbook dr automation.
VRT-003	Use VM-HA Guarantee.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1272

VRT-004	Deploy HA vCenter instance with embedded PSC to manage all ESXi based Nutanix clusters.
VRT-005	Deploy a vCenter in each region or AZ using runbook DR automation.
VRT-006	Enable EVC mode and set to the highest compatibility level the processors in the cluster will support.
VRT-007	Enable HA.
VRT-008	Enable DRS with default automation level.
VRT-009	Disable VM PDL and APD component protection.
VRT-010	Configure das.ignoreInsuffi-cientHbDatastore if one Nutanix container is presented to the ESXi hosts.
VRT-011	Disable Automation level for all CVMs.
VRT-012	Set host failures clusters tolerate to 1 for RF2 and to 2 for RF3
VRT-013	Set host isolation response to “Power off and restart VMs”.
VRT-014	Set host isolation response to “Leave Powered on” for CVMs.
VRT-015	Disable HA/DRS for each Nutanix CVM.
VRT-016	Disable SIOC.
DEP-001	A minimum of three NTP servers for all infrastructure components should be provided.
DEP-002	A minimum of two DNS Servers should be configured accessible to all infrastructure layers.
SEC-001	Use active directory authentication. This applies for user and service accounts.
SEC-002	Use SSL/TLS connection to Active Directory.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1273

SEC-003	Use signed Certificate Authority (CA) certificates for the components where certificates can be replaced. This can be either internal or external signed certificates.
SEC-004	Do not use Nutanix Cluster lockdown.
SEC-005	Do not use vSphere Cluster lockdown.
SEC-006	Enable CVM and hypervisor AIDE.
SEC-007	Configure SCMA to run hourly.
SEC-008	Stop unused ESXi services and close unused firewall ports.
SEC-009	Send log files to a highly available syslog infrastructure.
SEC-010	Include all Nutanix modules in the logging.
SEC-011	Use Error log level for the Nutanix components.
SEC-012	Use default esxi logging level, log rotation, and log file sizes.
SEC-013	If extra security and reliability are required, then use tcp for log transport. Otherwise, use the default syslog protocol, udp.
SEC-014	Use port 514 for logging.
SEC-015	Use VLAN for traffic separation of management and user workloads.
SEC-016	Place CVM and hypervisor on the same VLAN and subnet.
SEC-017	Place out of band management on separate VLAN or physical network.
SEC-018	Use the least privileged access approach when providing access. and Align RBAC structure and usage of default plus customer roles according to the company requirement.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1274

SEC-019	Align RBAC structure and usage of default plus custom roles according to the company requirements defined via SEC-019.
SEC-020	Do not use storage encryption.
SEC-021	Do not use a key management server.
OPS-001	Deploy Prism Central Pro for enhanced cluster management.
OPS-002	Review monthly capacity planning.
OPS-003	Perform updates after hours for performance or migration sensitive applications.
OPS-004	Utilize the current LTS branch.
OPS-005	Update to the next maintenance version 4 weeks after release. Update to the current patch version 2 weeks after release.
OPS-006	Maintain a pre-production environment for testing any changes needed (firmware, software, hardware) prior to executing the change actual production.
OPS-007	Configure alerts and alert policies in prism central, not prism element.
OPS-008	Utilize SMTP for alert transmission.
BCN-001	Utilize application- consistent snapshots when needed by the application
BCN-002	Place nearsync vm's in their own protection domain.
BCN-003	Configure snapshot schedules to be more frequent than the desired rpo
BCN-004	Configure snapshot schedules to retain the lowest number of snapshots while still meeting the retention policy.
BCN-005	Group applications together in unique protection domains. Keep number of vm's per protection domain as small as reasonably possible

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1275

BCN-006	Application requires RPO=0 and RTO near zero
BCN-007	Application requires zZero downtime DR avoidance solution
BCN-008	Application requires RPO=0
BCN-009	Provide RPO between 1 min and 15 min for the application
BCN-010	Application requires RPO=>1h
DCD-001	Decide on cluster licensing model for each ROBO (CBL or per-VM)
DCD-002	Decide on cluster type used (if not ROBO per- VM)
DCD-003	Decide whether to provide compute for ROBO failover
DCD-004	Decide on ROBO failover compute over commit
MULTI-NET-001	Calculate required storage replication bandwidth based on RPO.
MULTI-NET-002	Calculate application- specific bandwidth.
MULTI-NET-003	Place metro Availability and synchronous replication sites within the same region (Within 100km or less than 5msec RTT)
MULTI-NET-004	Place metro witness within 200msec
MULTI-NET-005	Do not use network segmentation for DR unless required. Routing segmentation is preferred over CVM segmentation
MULTI-NET-006	Ensure redundancy of each network device. Track the complete network path between protected sites.

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1276

MULTI-NET-007	Create and follow a redundancy test plan. Capture network components in plan.
MULTI-NET-008	Ensure that the link between protected sites and a witness does not use the link between sites.
MULTI-NET-009	For each workload, decide whether to keep the same IP addresses or change them during failover.
OPS-001	Use X-PLAY for low-code/no-code operational automation.
OPS-002	Monitor non-AOS VMs
OPS-003	Discover the applications running on your infrastructure
OPS-004	Monitor SQL Server from Prism
AWS-001	Create separate subnets for user VMS
AWS-002	Use AWS Direct Connect or create a second AWS cluster in a different AZ
AWS-003	Protect your AWS cluster by replication back to on-prem.
AWS-004	Plan your AWS VPC not to overlap with on-prem subnets
AWS-005	Allow outbound internet access through an existing connection to the internet to allow the cluster portal to manage your AWS cluster
AWS-006	Set AWS VPC limits to accommodate growth and auto-remediate features
FLOW-001	Use Microsegmentation with App-Type Policy to segment applications
FLOW-002	Use Microsegmentation with AD-Type Policy For VDI Deployments
FILES-001	Dedicate Nutanix clusters to file services workloads

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1277

FILES-002	Use Nutanix clusters with hybrid storage for Files
FILES-003	Use a minimum of 3 FSVMs
FILES-004	Use an N+1 configuration of FSVMs to physical nodes
FILES-005	Allocate more than the minimum FSVM CPU and memory recommended for your planned workload
FILES-006	Use the minimum number of file server instances for your needs
FILES-007	Place the file server storage network on the same VLAN as the eth0 interface of the controller VMs.
FILES-008	Place the FSVM client network so it uses the shortest network route for the majority of file services clients
FILES-009	Use Files distributed shares
FILES-010	Use file server share-level inline compression
FILES-011	Use AOS container-level erasure coding (EC-X)
FILES-012	Do not enable AOS container-level deduplication
FILES-013	Use telescoping snapshot schedules
FILES-014	Use the minimum number of DR snapshots needed for your RPO requirements
OBJECTS-001	Provide internal and external networks
OBJECTS-002	Choosing between mixed and dedicated Objects clusters
OBJECTS-003	Hybrid or all-flash Nutanix clusters for Objects?
OBJECTS-004	Enable compression
OBJECTS-005	Number of worker nodes

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1278

OBJECTS-006	Multiple object stores
OBJECTS-007	Multi-cluster object stores
OBJECTS-008	Enable versioning?
OBJECTS-009	WORM (write-once, read-many)
OBJECTS-010	Object lock
OBJECTS-011	Lifecycle policy
OBJECTS-012	Streaming replication
BAC-001	Choose a backup vendor to use with Nutanix Mine
BAC-002	Use Nutanix Objects as an archival tier for backups
CALM-001	Small or Large Calm deployment
CALM-002	Upgrade to the most recent version of Calm
CALM-003	Create separate Calm instances for development and production
CALM-004	Define processes for Calm DR and backup/restore
CALM-005	Align Calm project structure and RBAC configuration
CALM-006	Design Calm environment to align with release methodology and geographic regions
CALM-007	Enable the Calm Policy Engine
CALM-008	Enable Showback via Nutanix Beam
CALM-009	Choose a method for self-service
KARBON-001	Minimize use of the admin kubeconfig
KARBON-002	Distribute production applications across AZs
KARBON-003	Use Kubernetes namespaces to segment users and applications rather than clusters

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1279

KARBON-004	Leave enough space in a cluster to tolerate a worker node failure
KARBON-005	Utilize consistent pod and service CIDRs
KARBON-006	Upgrade the host OS as soon as possible
DBAAS-001	Enable Database as a Service (DBaaS)
DBAAS-002	Minimum hardware reqs for Nutanix clusters running Era
DBAAS-003	Use dedicated Nutanix Clusters for Database
DBAAS-004	Deploy Era management plane for HA
DBAAS-005	Place Era on a separate management network
DBAAS-006	Use the Era Platform license
DBAAS-007	Use Active Directory for user, group, and service account access
DBAAS-008	Use Active Directory groups to provide access to Era
DBAAS-009	Provide an Era test environment
DBAAS-010	Perform Era upgrades during service windows
DBAAS-011	Use Era super admin and database admin roles

© 2023 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1280

List of Figures

Figure 1: Nutanix Hybrid and Multicloud Strategy 7
Figure 2: Architecture Overview 13
Figure 3: Hyperconverged Infrastructure 14
Figure 4: A Nutanix Node 15
Figure 5: Chassis Configurations 16
Figure 6: Cluster Design 18
Figure 7: Business Continuity Layer 22
Figure 8: Designing for Security and Compliance 23
Figure 9: Nutanix Security 25
Figure 10: Regions 28
Figure 11: Availability Zones 28
Figure 12: Datacenters 29
Figure 13: Single Location 29
Figure 14: Multiple Locations 30
Figure 15: Active - Passive 30
Figure 16: Active - Active - Passive 31
Figure 17: Datacenter ROBO 32
Figure 18: Chain structure with Datacenter-ROBO-ROBO 33
Figure 19: Separate Management Clusters 39
Figure 20: Block and Pod Architecture 44
Figure 21: Example VDI Building Block 46
Figure 22: Planning the Technical Design 55
Figure 23: Management Plane Failure Domain 65

Figure 24: The Nutanix Cluster as a Failure Domain....66
Figure 25: Datacenter Rack and Server Room Failure Domains....67
Figure 26: Datacenter Building Failure Domain....69
Figure 27: Designing Datacenter Locations....69
Figure 28: Single Rack Single Workload Domain....74
Figure 29: Single Rack, Multiple Workload Domains....74
Figure 30: Multiple Racks, Single Workload Domain....76
Figure 31: Pure Layer 2 Design....82
Figure 32: Leaf Spine Topology....82
Figure 33: Core Aggregation Access Design....83
Figure 34: Layer 2 Network Design....88
Figure 35: Layer 3 Network Design....89
Figure 36: Layer 3 Network Design with Overlay....90
Figure 37: Logical View of Leaf Spine Scale....91
Figure 38: Leaf Switches Connected Using Link Aggregation....91
Figure 39: Rack Level View of Leaf Spine....92
Figure 40: Clusters Connecting to Different Aggregation Layers....94
Figure 41: AHV Networking....95
Figure 42: Relationship between the Components of the Nutanix Node....103
Figure 43: Example Host with 2 NUMA Nodes....104
Figure 44: Example of a Single NUMA Node....105
Figure 45: vCPU and Memory Assignment Spanning NUMA Boundaries....106
Figure 46: Best Performance vNUMA Configuration for Wide VMs....107
Figure 47: The Nutanix Control Plane....121
Figure 48: Small vs Large Prism Central VM Sizes....128
Figure 49: Scale Out Prism Central Deployment....129

Figure 50: vCenter Appliances....131
Figure 51: Life Cycle Manager....150
Figure 52: Foundation Pre-Configuration Service....152
Figure 53: Capacity Runway....154
Figure 54: Expansion Planning....155
Figure 55: Alert Email Configuration....159
Figure 56: General Guidance for Business Continuity....161
Figure 57: BCDR Workflow....161
Figure 58: Active-Active....163
Figure 59: Active-Passive....164
Figure 60: Disaster Recovery Decision Tree....175
Figure 61: Two AZ within the Same Region....179
Figure 62: Two AZ across Multiple Regions....180
Figure 63: Multiple AZ within a Single Region....181
Figure 64: Multiple AZ across Multiple Regions....182
Figure 65: Multiple AZ within a Single Region....183
Figure 66: Multiple AZ across Multiple Regions....184
Figure 67: Single Region....186
Figure 68: Multiple Regions....187
Figure 69: Latency Requirements....195
Figure 70: Network Routing....197
Figure 71: Network Redundancy....198
Figure 72: Single Piece of Conduit with Multiple WAN Links....200
Figure 73: Metro Witness Link Requirements....202
Figure 74: IT Ops Triangle....207
Figure 75: With Prism X-Play, a single trigger can precipitate multiple actions....208

Figure 76: Example Workflows Based on Various Triggers....211
Figure 77: Monitoring non-AOS VMs with Prism Ultimate....212
Figure 78: Monitoring SQL Server with Prism Ultimate....213
Figure 79: App Discovery....214
Figure 80: Nutanix Cloud Clusters on AWS....215
Figure 81: Nutanix Cloud Clusters on AWS Architecture....216
Figure 82: Example IP Address Assignment for an NC2 Deployment....218
Figure 83: Security Groups Used by NC2....221
Figure 84: Effects of a Quarantine Policy....227
Figure 85: Effects of an Isolation Policy....228
Figure 86: Illustration of an App-Type Policy....228
Figure 87: Using an AD-Type Policy to Secure a VDI Environment....229
Figure 88: Using an AD-Type Policy to Secure a VDI Environment....230
Figure 89: Example of a Nutanix Files Instance....233
Figure 90: Three Separate Nutanix Files Instances Deployed on a Single Cluster....234
Figure 91: Relationship Between File Server VMs, CVMs, and Cluster Nodes....235
Figure 92: Distributed Shares are Distributed Across Multiple Volume Groups and FSVMs....236
Figure 93: Standard Shares are Assigned to a Single FSVM and a Single Volume Group....236
Figure 94: Nutanix Objects Deployments....247
Figure 95: Internal and External Networks....248
Figure 96: Lookup Hints....248
Figure 97: Mine Deployments Across Datacenters or Regions....262
Figure 98: Global Enterprise Calm Deployment....269
Figure 99: Self-Service with Calm....272
Figure 100: Karbon Provides a Single Control Plane for Multiple Kubernetes Clusters and Locations....274

Figure 101: A Karbon Development Cluster is not Highly Available.....275

Figure 102: A Karbon Cluster for Production is Highly Available.....275

Figure 103: An External Load Balancer Enables Karbon to Have More than Two Master Nodes.....276

Figure 104: Nutanix Era DBaaS.....283

Figure 105: Nutanix Era VMs and DBs.....284

Figure 106: Era Management Layer in a Multi-Cluster Deployment.....285

List of Tables

Table 1: Cloud Configurations..... 6

Table 2: Architectural Principles..... 6

Table 3: Design Objectives of this Document for Private Cloud Implementations..... 8

Table 4: Design Decision Example..... 11

Table 5: Number of Regions to be used..... 34

Table 6: Number of Availability Zones to be used..... 34

Table 7: Number of Datacenters to be used..... 34

Table 8: RPO and RTO requirements..... 34

Table 9: Choose a Hypervisor..... 37

Table 10: Management Cluster Architecture..... 39

Table 11: Mixed or Dedicated Workloads Per Cluster..... 42

Table 12: Nutanix Software Licensing Level..... 48

Table 13: Physical Node Vendor..... 50

Table 14: Node Models..... 54

Table 15: Software Versions..... 56

Table 16: Cluster Size Design Considerations..... 57

Table 17: Maximum Limits for Management Plane Software Components in AHV Deployments 62

Table 18: Minimum and Maximum Number of Nodes in a Single AHV Cluster..... 62

Table 19: Maximum Limits for Management Plane Software Components in VMware Deployments..... 62

Table 20: Minimum and Maximum Number of Nodes in a Single vSphere Cluster..... 63

Table 21: Number of Clusters..... 63

Table 22: Management Plane Risk Mitigations..... 64

Table 23: Designing for Redundancy at the Cluster Level..... 66

Table 24: Datacenter Rack and Server Room Risk Mitigation.....67

Table 25: Datacenter Building Risk Mitigation.....68

Table 26: Two region implementation for DR..... 70

Table 27: Single region implementation for DR.....70

Table 28: Long term retention backups are placed in Region 2..... 71

Table 29: Three availability zones in two regions..... 71

Table 30: Two availability zones in Region 1.....72

Table 31: One availability zone in Region 1 to provide disaster recovery..... 72

Table 32: One availability zone in Region 2 hosts backups..... 73

Table 33: Pros and cons..... 77

Table 34: Workload Domains Spanning Single or Multiple Racks.....77

Table 35: Examples of Recommended Switch Models.....79

Table 36: Examples of Robo Or Smb Switch Models.....80

Table 37: Switches that are not acceptable.....80

Table 38: Using a Large Buffer Datacenter Switch at 10GBPS or Faster..... 81

Table 39: Using a Leaf-Spine Network Topology for New Environments..... 85

Table 40: Populate Each Rack with Two 10GBE or Faster TOR Switches..... 85

Table 41: Avoid Switch Stacking to Ensure Network Availability During Individual Device Failure..... 85

Table 42: Use No More Than Three Switches Between Two Nutanix Nodes in the Same Cluster.....86

Table 43: Reduce Network Oversubscription to Achieve a Near-1:1 Ratio.....86

Table 44: Configure CVM and Hypervisor VLAN on Server-facing Switch Ports.....86

Table 45: Use Tagged VLANs on Switch Ports for All Guest Workloads..... 87

Table 46: Use a Layer 2 Network Design..... 90

Table 47: Connecting NICs to TOR Switches....98
Table 48: Using Bridges with Uplinks....98
Table 49: Using NICs of the same vendor within a bond....98
Table 50: Using VLANs to separate logical networks....99
Table 51: Load Balancing....99
Table 52: Using Standard 1500 Byte MTU....99
Table 53: Use Virtual Distributed Switch (VDS)....100
Table 54: Connecting NICs to the TOR Switch....101
Table 55: Using Virtual Switches and Uplinks....101
Table 56: Load Balancing....102
Table 57: Using Standard 1500 Byte MTU....102
Table 58: Running Non-NUMA-aware Applications on a VM....104
Table 59: Minimum CPU and Memory Values as of AOS 5.15....108
Table 60: Creating vDisks in ESXi....109
Table 61: SSD Capacity Considerations When Sizing a Cluster....112
Table 62: Mixing Nodes from Different Vendors in the Same Cluster....113
Table 63: Mixing NVMe and Hybrid SSD/HDD Nodes in the Same Cluster....113
Table 64: HDD to SSD Ratio....114
Table 65: Sizing for Redundancy....114
Table 66: Data Awareness and Fault Tolerance Levels Supported....116
Table 67: Fault Tolerance for Workloads/Clusters with Higher SLAs....117
Table 68: Expected Overhead for EC-X vs Standard RF2/RF3....117
Table 69: Enabling Inline Compression for All Containers....119
Table 70: Enabling/Disabling Deduplication....119
Table 71: Deploying Prism Central for Enhanced Cluster Management....121
Table 72: Deploy Prism Central in Each Region or Az Using Runbook Dr Automation....121

Table 73: Using VM-HA Guarantee..... 122
Table 74: Managing ESXi-based Nutanix Clusters..... 123
Table 75: Deploy a vCenter in Region or Az Using Runbook Dr Automation..... 124
Table 76: Enabling EVC Mode..... 124
Table 77: Enabling HA..... 124
Table 78: Enabling DRS..... 125
Table 79: Disabling VM PDL and APD Component Protection..... 125
Table 80: Configuring DAS.IGNOREINSUFFICIENTHBDATASTORE..... 125
Table 81: Disabling Automation Level for All CVMs..... 126
Table 82: Setting Amount of Reserved Resources in the Cluster..... 126
Table 83: Setting Host Isolation Response for VMs..... 126
Table 84: Setting Host Isolation Response for the CVM..... 126
Table 85: Disabling HA/DRS for Each Nutanix CVM..... 127
Table 86: Disabling SIOC..... 127
Table 87: Prism Central Recommendations..... 130
Table 88: vCenter Server Recommendations..... 131
Table 89: NTP Servers for Infrastructure Components..... 132
Table 90: DNS Servers for Infrastructure Layers..... 133
Table 91: Active Directory Authentication..... 136
Table 92: Using SSL/TLS Connection to Active Directory..... 136
Table 93: Using a Certificate Authority..... 137
Table 94: Nutanix Cluster Lockdown..... 137
Table 95: vSphere Cluster Lockdown..... 138
Table 96: CVM and Hypervisor AIDE..... 138
Table 97: Configuring SCMA..... 138
Table 98: Unused ESXi Services and Unused Firewall Ports..... 139

Table 99: Logging....140
Table 100: Including All Nutanix Modules in Logging....140
Table 101: Error Log Level for Nutanix Components....140
Table 102: ESXi Logging Level, Rotation, and File Size....141
Table 103: Protocols for Log Transport....141
Table 104: Using Port 514 for Logging....141
Table 105: VLAN for Traffic Separation....142
Table 106: Place CVM and Hypervisor on Same VLAN and Subnet....142
Table 107: Place Out-of-band Management on a Separate VLAN or Physical Network....143
Table 108: Default Prism Central Roles....143
Table 109: Prism Element Default Roles....145
Table 110: Use Least-Privilege Approach when Determining Access....145
Table 111: Align RBAC to Company Structure....145
Table 112: Do Not Use Storage Encryption....147
Table 113: Do Not Use a Key Management Server....147
Table 114: Overview of Different Foundation Software Options....152
Table 115: Deploying Prism Pro for Enhanced Cluster Management....153
Table 116: Reviewing Monthly Capacity Planning....155
Table 117: Performing Updates....156
Table 118: Utilizing the Current LTS Branch....157
Table 119: Upgrading to Maintenance and Current Patch Versions....157
Table 120: Maintaining a Pre-Production Environment....158
Table 121: Configuring Alerts and Alert Policies....158
Table 122: Utilizing SMTP for Alert Transmission....159
Table 123: Utilizing Application-Consistent Snapshots....165
Table 124: Place Nearsync VMs in their Own Protection Domain....168

Table 125: Configure Snapshot Schedules to be More Frequent....169
Table 126: Configure Snapshot Schedules to Retain Lowest Number of Snapshots....169
Table 127: Schedule to Save Recovery Points....169
Table 128: Protection Domain Two-Site Support Matrix....170
Table 129: Protection Domain Multisite Support Matrix....171
Table 130: Protection Policy Two-Site Support....171
Table 131: Protection Policy Multisite Support Matrix....171
Table 132: Group Applications Together in Unique Protection Domains....172
Table 133: Application Requires RPO....176
Table 134: Application Requires Zero Downtime....177
Table 135: Application Requires RPO....177
Table 136: Provide RPO Between 1 and 15 Min....178
Table 137: Application Requires RPO....178
Table 138: Decide on Cluster Licensing Model....188
Table 139: Decide on Cluster Type Used....189
Table 140: Decide Whether to Provide Compute for ROBO Failover....189
Table 141: Decide on ROBO Failover Compute....189
Table 142: Required Networking Characteristics....192
Table 143: Bandwidth Needed for an RPO....193
Table 144: Calculate Required Storage Replication Bandwidth....194
Table 145: Calculate Application Specific Bandwidth....194
Table 146: Place Metro and Synchronous Replication Sites within the Same Region....195
Table 147: Place Metro Witness within 200msec....196
Table 148: Do Not Use Network Segmentation for DR....197
Table 149: Ensure Redundancy of Each Network Device....200
Table 150: Create and Follow a Redundancy Test Plan....201

Table 151: Ensure that the Link Between Protected Sites and a Witness does not Use the Link Between Sites....202
Table 152: For Each Workload Decide Whether to Maintain or Change....204
Table 153: Prism Ops Design Objectives....206
Table 154: Leverage X-Play Playbooks....210
Table 155: Monitor Non-AOS VMs....211
Table 156: Discover Applications with Prism Ultimate....212
Table 157: Monitor Microsoft SQL Server....212
Table 158: Nutanix Cloud Clusters Design Objectives....214
Table 159: Supported EC2 Bare-Metal Instances....219
Table 160: Separate Subnets....222
Table 161: Create Availability Zones....223
Table 162: Use Replication....223
Table 163: Don't Overlap Subnets....224
Table 164: Allow Outbound Internet Access....224
Table 165: Plan VPC Limits for Growth and Availability....225
Table 166: Flow Design Objectives....225
Table 167: Flow Policy Types....227
Table 168: Use Microsegmentation to Isolate Applications....231
Table 169: Use AD-Type Policy to Isolate VDI....231
Table 170: Nutanix Files Design Objectives....232
Table 171: Mixed or Dedicated Environments....237
Table 172: Choose Hybrid Clusters....238
Table 173: Minimum FSVMs....239
Table 174: N+1 Configuration....239
Table 175: CPU and Memory Allocation....240

Table 176: Minimum Number of File Servers..... 241
Table 177: File Server Storage Network.....241
Table 178: Shortest Route Between Client and Server..... 241
Table 179: Utilize Distributed Shares.....242
Table 180: Compression.....243
Table 181: Erasure Coding (EC-X).....243
Table 182: Deduplication..... 243
Table 183: Scheduling Snapshots..... 244
Table 184: Disaster Recovery..... 244
Table 185: Disaster Recovery.....245
Table 186: Design Objectives..... 245
Table 187: An Object Store Requires Internal and External Networks.....249
Table 188: Mixed or Dedicated Objects Clusters.....249
Table 189: Hybrid or All Flash Clusters.....250
Table 190: Enable Compression..... 251
Table 191: Number of Worker Nodes.....252
Table 192: Multiple Object Stores.....253
Table 193: Multi-Cluster Object Stores..... 253
Table 194: Enabling Versions.....254
Table 195: WORM..... 255
Table 196: Object Lock..... 256
Table 197: Lifecycle Policies.....256
Table 198: Streaming Replication.....257
Table 199: Nutanix Mine Design Objectives.....257
Table 200: Nutanix Mine Configurations.....258
Table 201: Choose a Backup Vendor.....260

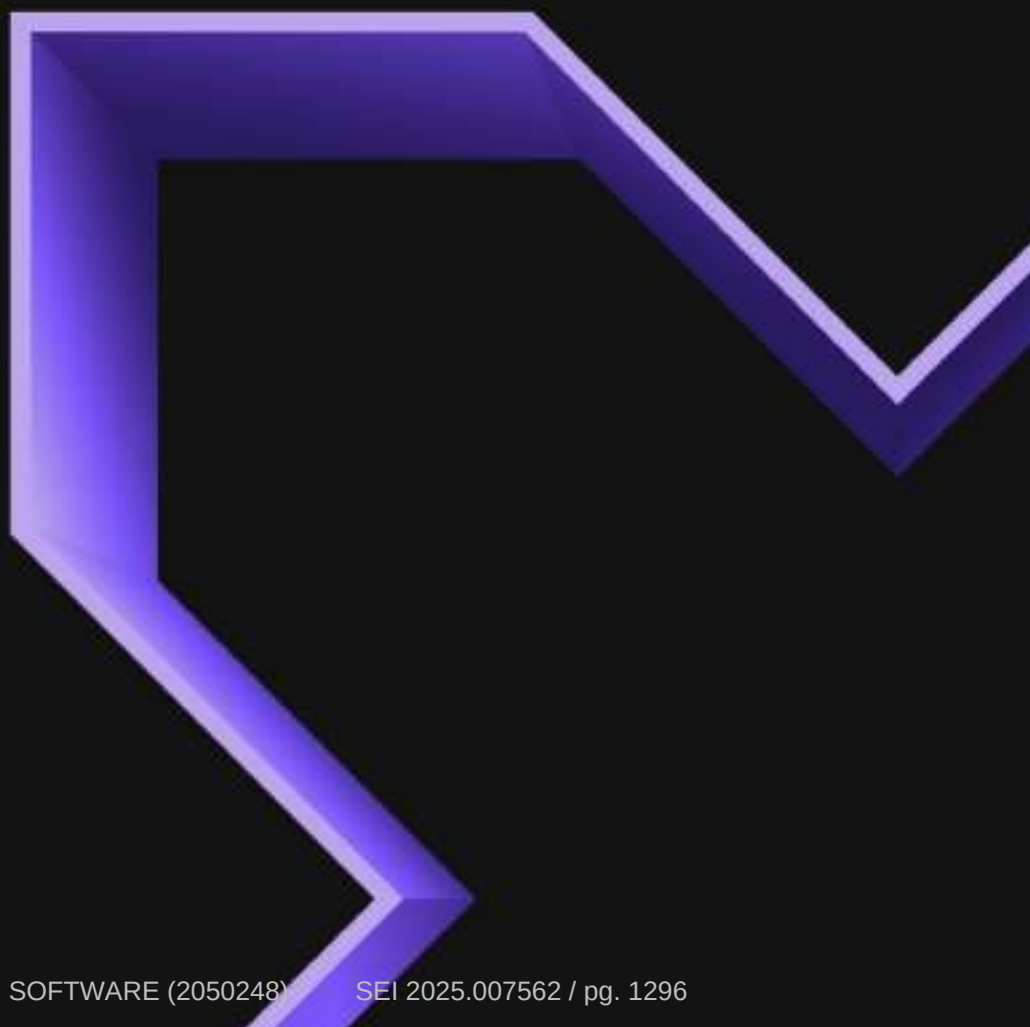
Table 202: Utilize Objects for Archival..... 261
Table 203: Nutanix Calm Design Objectives.....262
Table 204: Choose a Small or Large Calm Deployment.....264
Table 205: Upgrade to Most Recent Calm Version.....265
Table 206: Deploy Calm for Development and Production.....266
Table 207: Calm for DR and Backup..... 267
Table 208: Calm and RBAC Configurations..... 268
Table 209: Calm Releases and Geographic Regions.....269
Table 210: Calm Policy Engine..... 270
Table 211: Showback with Nutanix Beam.....270
Table 212: Self-Service with Calm.....272
Table 213: Nutanix Karbon Design Objectives.....272
Table 214: Minimize Admin Kubeconfig Use..... 278
Table 215: Use Multiple Availability Zones for Production.....279
Table 216: Use Namespaces to Segment Users and Apps..... 279
Table 217: Leave Room for a Worker Node to Fail..... 279
Table 218: Use Consistent CIDRs.....280
Table 219: Keep the Host OS Updated..... 280
Table 220: Nutanix Era Design Objectives..... 281
Table 221: Era to Enable DBaaS.....286
Table 222: Era Hardware Requirements.....287
Table 223: Dedicated DB Clusters.....287
Table 224: HA Management Plane.....288
Table 225: Management Network.....288
Table 226: Era Platform License..... 289
Table 227: Active Directory Integration.....289

Table 228: Active Directory Access..... 290
Table 229: Era Test Environment..... 290
Table 230: Service Windows.....290
Table 231: Era Roles..... 291
Table 232: Design Decisions.....293

AHV Administration Guide

AHV 10.0

January 24, 2025



NUTANIX

Contents

AHV Overview 6

Storage Overview 6
- AHV Turbo 7

Acropolis Dynamic Scheduling in AHV 8
- Disabling Acropolis Dynamic Scheduling 11
- Enabling Acropolis Dynamic Scheduling 11

Virtualization Management Web Console Interface 11
- Finding the AHV Version on Prism Element 11
- Finding the AHV Version on Prism Central 12

AHV Cluster Power Outage Handling 12

Serial Console Redirection to a Telnet Port 13

Node Management 14

Nonconfigurable AHV Components 14
- Nutanix Software 14
- AHV Settings 14

Controller VM Access 15
- Admin User Access to Controller VM 15
- Nutanix User Access to Controller VM 17
- Controller VM Password Complexity Requirements 18

AHV Host Access 19
- Initial Configuration 20
- Accessing the AHV Host Using the Admin Account 20
- Changing the Root User Password 21
- Changing Nutanix User Password 22
- AHV Host Password Complexity Requirements 22

Verifying the Cluster Health 23

Node Maintenance Mode 24
- Putting a Node into Maintenance Mode using Web Console 26
- Viewing a Node that is in Maintenance Mode 27
- Exiting a Node from the Maintenance Mode using Web Console 28
- Guest VM Status when Node is in Maintenance Mode 29
- Putting a Node into Maintenance Mode using CLI 30
- Exiting a Node from the Maintenance Mode Using CLI 32

Shutting Down a Node in a Cluster (AHV) 33

Starting a Node in a Cluster (AHV) 34

Rebooting an AHV Node in a Nutanix Cluster 35

Shutting Down an AHV Cluster 35

Starting Up an AHV Cluster 38

Changing CVM Memory Configuration (AHV) 39

Renaming an AHV Host 39

Changing the Name of the CVM Displayed in Prism 40

Adding an AHV Storage-Only Node 41

AHV Compute-Only Node Configuration 42

Reinstalling AHV on a Node 42

Host Network Management 46

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1297

Network Types....46
Network Traffic Types....48
Prerequisites for Configuring Networking....48
AHV Networking Recommendations....48
IP Address Management....55
Traffic Marking for Quality of Service....56
Layer 2 Network Management....59
About Virtual Switch....59
Virtual Switch Requirements....67
Virtual Switch Limitations....68
Virtual Switch Management....69
Change Interface Ring Buffer Sizes....78
Enabling LACP and LAG (AHV Only)....82
VLAN Configuration....84
IGMP Snooping....88
Traffic Redirection and Inspection....89
Traffic Mirroring on AHV Hosts....90
Virtual Switch Security with MAC Addresses....101
Forged MAC Transmits and MAC Address Changes....102
MAC Address Prefix....102
Adding a MAC Address Prefix....103
Removing the MAC Address Prefix....104
Enabling RSS Virtio-Net Multi-Queue by increasing the Number of VNIC Queues....105
Changing the IP Address, Network Mask, or Gateway of an AHV Host....108
Setting up the Environment to change the IP Address, Network Mask, or Gateway of an AHV Host....110

Virtual Machine Management....112

Supported Guest VM Types for AHV....112
Creating a VM (AHV)....112
Managing a VM (AHV)....117
Limitation for vNIC Hot-Unplugging....123
Shutting Down VMs using aCLI....124
Starting Up VMs using aCLI....124
VM Migration Specifications....125
Live Migration Cases....126
Live Migration Restrictions....126
Checking Live Migration Status of a VM....128
Verifying Affinity Policy Association....129
Defining Behaviour for Non-migratable VMs (GPU/CPU/PCI/Host Affinity configured VMs)....130
Multichannel Support for AHV Live Migration Performance....131
Adaptive CPU Management during Live Migration....133
On-Demand Cross-Cluster Live Migration....133
On-Demand Cross-Cluster Live Migration (OD-CCLM) Requirements....134
On-Demand Cross-Cluster Live Migration (OD-CCLM) Limitations....136
On-Demand Cross-Cluster Live Migration (OD-CCLM) Best Practices....137
Performing On-Demand CCLM....138
Virtual Machine Snapshots....139
Windows VM Provisioning....140
Nutanix VirtIO for Windows....140
Installing Windows on a VM....150
Windows Defender Credential Guard Support in AHV....153
Windows Subsystem for Linux (WSL2) Support on AHV....158
VM-Host Affinity Policies....160
VM-Host Affinity Policies Defined in Prism Element....160

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1298

VM-Host Affinity Policies Defined in Prism Central....161
Non-Migratable VMs....171
Disaster Recovery Specifications for VM-Host Affinity Policies....171
Role Based Access Control for VM-Host Affinity Policies....173
VM-VM Anti-Affinity Policies....174
Configuring Legacy VM-VM Anti-Affinity Policy....175
Removing Legacy VM-VM Anti-Affinity Policy....176
VM-VM Anti-Affinity Policies Defined in Prism Central....176
Disaster Recovery Specifications for VM-VM Anti-Affinity Policies....185
Performing Power Operations on VMs by Using Nutanix Guest Tools (aCLI)....186
UEFI Support for VM....187
Creating UEFI VMs by Using aCLI....188
Getting Familiar with UEFI Firmware Menu....189
Setting up Boot Device Order Using aCLI....193
Secure Boot Support for VMs....194
Secure Boot Considerations....194
Creating/Updating a VM with Secure Boot Enabled....195
Securing AHV VMs with Virtual Trusted Platform Module (aCLI)....195
Virtual Machine Network Management....198
Virtual Machine Memory and CPU Hot-Plug Configurations....198
Hot-Plugging the Memory and CPUs on Virtual Machines (AHV)....199
Disable CPU Hot-Plug on VMs....199
Disabling CPU Hot-Plug During VM Creation....200
Disabling CPU Hot-Plug in an Existing VM....200
Disable the SCSI Controller on VMs....201
Disabling SCSI Controller During VM Creation....201
Disabling SCSI Controller in an Existing VM....202
Virtual Machine Memory Management (vNUMA)....203
Enabling and Disabling vNUMA on Virtual Machines....203
GPU and vGPU Support....205
Supported GPUs....205
GPU Pass-Through for Guest VMs....205
NVIDIA GRID Virtual GPU Support on AHV....207
PXE Configuration for AHV VMs....216
Configuring the PXE Environment for AHV VMs....216
Configuring a VM to Boot over a Network....217
Uploading Files to DSF for Microsoft Windows Users....219
Enabling Load Balancing of vDisks in a Volume Group....219
VM High Availability in Acropolis....220
Enabling High Availability for the Cluster....221
Viewing list of restarted VMs after an HA event....222
Live vDisk Migration Across Storage Containers....223
Migrating a vDisk to Another Container....225
Memory Overcommit....227
Deployment Workflow....227
Requirements and Recommendations for Memory Overcommit....230
Limitations of Memory Overcommit....230
Total Memory Allocation Mechanism on Linux and Windows VM....231
Memory Overcommit Management....232
OVAs....236
OVA Restrictions....237
VM Generation UUID and BIOS UUID Support in AHV....237
Checking VM Generation UUID and BIOS UUID of a Guest VM....238
Automatic Cluster Selection for VM Placement....239
Supported Configuration Workflows for Automatic Cluster Selection....239
VM Policies with Automatic Cluster Selection....239

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1299

Automatic Cluster Selection Interaction with Self-Service Projects....239
Requirements for Automatic Cluster Selection....240
Limitations of Automatic Cluster Selection....240
Sample Scenarios for Automatic Cluster Selection....240
Advanced Processor Compatibility in AHV....242
Requirements for Advanced Processor Compatibility....243
Limitations and Considerations of Advanced Processor Compatibility....243
Supported Configuration Workflows for Advanced Processor Compatibility....244
Supported CPU Generation Names for Advanced Processor Compatibility....244
PCIe Passthrough for Guest VMs....246
Assigning a PCIe Device to a Guest VM....247
Deassigning a PCIe Device from a Guest VM....247
Listing PCIe Devices Attached to a Guest VM....248

VM Template Management....250
Limitations of VM Template Feature....250
Creating a VM Template....250
Deploying VM from a Template....253
Managing a VM Template....256

Copyright....260

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1300

AHV OVERVIEW

As the default option for Nutanix HCI, the native Nutanix hypervisor, AHV, represents a unique approach to virtualization that offers the powerful virtualization capabilities needed to deploy and manage enterprise applications. AHV complements the HCI value by integrating native virtualization along with networking, infrastructure, and operations management with a single intuitive interface - Nutanix Prism.

Virtualization teams find AHV easy to learn and transition to from legacy virtualization solutions with familiar workflows for VM operations, live migration, VM high availability, and virtual network management. AHV includes resiliency features, including high availability and dynamic scheduling without the need for additional licensing, and security is integral to every aspect of the system from the ground up. AHV also incorporates the optional Flow Security and Networking, allowing easy access to hypervisor-based network microsegmentation and advanced software-defined networking.

For information on how to deploy and create a cluster, see the Field Installation Guide. Once you create the cluster by using Foundation, you can use this guide to perform day-to-day management tasks.

AOS and AHV Compatibility

For information on the AOS and AHV compatibility with this release, see Compatibility and Interoperability Matrix.

Minimum Field Requirements for Nutanix Cloud Infrastructure (NCI)

For information on minimum field requirements for NCI, see Minimum Field Requirements for Nutanix Cloud Infrastructure (NCI) topic in *Acropolis Advanced Administration Guide*.

Limitations

For information on AHV configuration limitations, see Nutanix Configuration Maximums webpage.

Nested Virtualization

Nutanix only supports nested virtualization in specific use cases on Windows VMs. The use cases include Windows Defender Credential Guard and Windows Subsystem for Linux (WSL2). For more information, see Windows Defender Credential Guard Support in AHV on page 153 and Windows Subsystem for Linux (WSL2) Support on AHV on page 158.

Storage Overview

AHV uses a Distributed Storage Fabric to deliver data services such as storage provisioning, snapshots, clones, and data protection to VMs directly.

In AHV clusters, AOS passes all disks to the VMs as raw SCSI block devices. By that means, the I/O path is lightweight and optimized. Each AHV host runs an iSCSI redirector, which establishes a highly resilient storage path from each VM to storage across the Nutanix cluster.

QEMU is configured with the iSCSI redirector as the iSCSI target portal. Upon a login request, the redirector performs an iSCSI login redirect to a healthy Stargate (preferably the local one).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1301

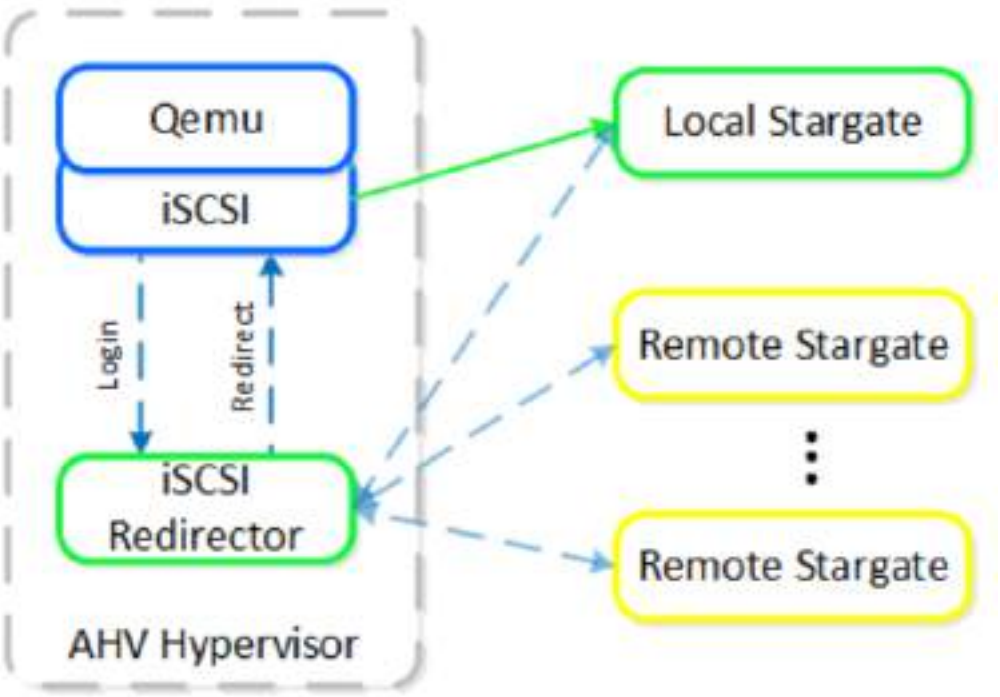


Figure 1: AHV Storage

AHV Turbo

AHV Turbo represents significant advances to the data path in AHV. AHV Turbo provides an I/O path that bypasses QEMU and services storage I/O requests, which lowers CPU usage and increases the amount of storage I/O available to VMs.

AHV Turbo represents significant advances to the data path in AHV.

When you use QEMU, all I/O travels through a single queue that can impact system performance. AHV Turbo provides an I/O path that uses the multi-queue approach to bypasses QEMU. The multi-queue approach allows the data to flow from a VM to the storage more efficiently. This results in a much higher I/O capacity and lower CPU usage. The storage queues automatically scale out to match the number of vCPUs configured for a given VM, and results in a higher performance as the workload scales up.

AHV Turbo is transparent to VMs and is enabled by default on VMs that runs in AHV clusters. For maximum VM performance, ensure that the following conditions are met:

- The latest Nutanix VirtIO package is installed for Windows VMs. For information on how to download and install the latest VirtIO package, see Installing or Upgrading Nutanix VirtIO for Windows.

  Note: No additional configuration is required at this stage.

- The VM has more than one vCPU.
- The workloads are multi-threaded.

  Note: Multi-queue is enabled by default in current Linux distributions. For details, refer your vendor-specific documentation for Linux distribution.

In addition to multi-queue approach for storage I/O, you can also achieve the maximum network I/O performance using the multi-queue approach for any vNICs in the system. For information about how to enable multi-queue and

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1302

set an optimum number of queues, see Enabling RSS Virtio-Net Multi-Queue by Increasing the Number of VNIC Queues.

> **Note:** Ensure that the guest operating system fully supports multi-queue before you enable it. For details, refer your vendor-specific documentation for Linux distribution.

Acropolis Dynamic Scheduling in AHV

Acropolis Dynamic Scheduling (ADS) proactively monitors your cluster for any compute and storage contentions or hotspots over a period of time. If ADS detects a problem, ADS creates a migration plan that eliminates hotspots in the cluster by migrating VMs from one host to another.

You can monitor the VM migration tasks from the **Tasks** dashboard in both Prism Element and Prism Central.

ADS provides the following advantages:

- ADS performs the runtime optimizations, including moving particular guest VMs and VGs to other AHV hosts to give all workloads the best possible access to resources.
- ADS can enable initial placement of the guest VM in cases when there is not enough space to power it on initially. In this case, the system invokes the ADS and attempts to de-fragment the cluster, which involves moving and rearranging the existing guest VMs to create space for the new guest VM.
- Nutanix Volumes uses ADS to balance sessions of the externally available iSCSI targets.

> **Note:**
>
> - ADS honors all the configured host affinity policies from Prism Central, VM-host affinities from Prism Element, VM-VM anti affinity policies, and HA policies.
>
> ADS ensures that the VM-VM anti-affinity and VM-Host affinity policies are always enforced during both initial VM placement and VM migrations to resolve resource contention. If any of these actions lead to either VM-VM anti-affinity or VM-Host affinity policy violation, then ADS rejects the VM placement or VM migration.
>
> For a user-initiated intra-cluster migration of the VM:
>
> - If the migration leads to non-compliance with the VM-VM anti-affinity policy, ADS performs the following actions:
>
> - Ignores compliance with VM-VM anti-affinity policy if a host is specified during manual migration.
> - Attempts to enforce the policy back into compliance on a commercially reasonable effort if a host is not specified during manual migration.
>
> - If the migration leads to non-compliance with the VM-Host affinity policy, ADS will not allow the migration to be completed.
> - ADS does not consider the nodes that are under maintenance.

By default, ADS is enabled, and Nutanix recommends that you keep this feature enabled. However, for information on how to disable the ADS feature, see Disabling Acropolis Dynamic Scheduling on page 11 and for information on how to enable the ADS feature if you previously disabled the feature, see Enabling Acropolis Dynamic Scheduling on page 11.

ADS monitors the following resources:

- VM CPU utilization that includes the total CPU usage of each guest VM and storage CPU utilization that includes the storage controller (Stargate) CPU usage per VM or iSCSI target for the last 10 minutes. Based on the last 10

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1303

minutes of data, ADS estimates whether a CPU hotspot exists or is going to exist on a node. This trend analysis ensures that ADS does not migrate the guest VMs when there are sudden spikes in CPU usage that tend to go away quickly. For example, in the case of a boot storm where the CPU usage increases but goes away quickly, ADS does not migrate the guest VM from the host.

- Memory utilization of the guest VMs when memory overcommit is enabled. ADS computes a differential value of the last 2 minutes using statistics such as the amount of accessed memory and guest swaps to identify the below memory overcommit aspects for the guest VMs:

  - Guest VMs needs more memory.
  - Guest VMs already has more memory assigned to them than the actual memory requirement.

  Based on these memory overcommit aspects, the host decides the exact memory allocation for the guest VM.

  For information on memory overcommit function, see Memory Overcommit on page 227.

- vGPU profiles to ensure the correct assignment to the compatible GPUs during hotspot mitigation. ADS migrates the guest VMs with virtual GPUs (vGPUs) only to the destination node that consists of the compatible GPUs. For more information, see ADS support for VMs with vGPUs on page 209.

ADS does not monitor the network usage, and memory when memory overcommit is not enabled.

How Acropolis Dynamic Scheduling Works

ADS performs the following tasks to resolve compute and storage contentions or hotspots:

- Gather statistics from the components it monitors.
- Checks the statistics for potential anomalies and determines how to resolve them, if possible.
- Invokes the tasks (for example, VM migrations) to resolve the situation.

Note:

- During initial VM placement, if AHV cannot place the guest VM directly on any node in the cluster, it initiates ADS to check whether a cluster de-fragmentation, which involves migrating or rearranging the existing guest VMs within the cluster, can create enough space for the new guest VM. However, if there are any existing hotspots and not enough space to accommodate the new guest VM in the cluster, the initial placement of the guest VM fails.
- During migration, a guest VM consumes resources on both the source and destination hosts as the High Availability (HA) reservation algorithm must protect the VM on both hosts.
- When multiple hosts are available, ADS checks the availability of attributes such as CPU, memory, storage-controller, and vGPUs usage on each AHV host and selects the AHV host that has the overall highest availability of these attributes for VM placement.

When Is a Hotspot Detected?

ADS performs the following actions to detect and mitigate the hotspot:

- Runs every 15 minutes to optimize CPU and storage utilization if there is a hotspot. For storage hotspots, the system computes average Stargate CPU usage over the last 10 minutes, and for CPU hotspots, the system computes average host CPU usage over the last 10 minutes. If the resource utilization of an AHV host remains greater than 85% for this span. ADS triggers migration tasks to remove the hotspot.
- Runs every 2 minutes for memory overcommit optimization.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1304

- Maintains the pace period of 21 minutes after completion of a migration plan to ensure that its future decisions only consider statistics resulting from the last migration plan. The pace period is the time duration after which the ADS is run again to capture the current cluster state.

  Note:

  - If any anomaly is detected and ADS cannot solve the issue (for example, because of limited CPU or storage resources), AHV does not generate the migration plan.
  - If the host, firmware, or AOS upgrade is in progress and if any resource contention occurs during the upgrade period, ADS does not perform any resource contention rebalancing. However, if memory overcommit is enabled for the guest VMs, ADS performs the memory overcommit optimization.

    During memory overcommit optimization, ADS, if required, increases the amount of memory allocated to guest VMs for which the memory overcommit function is enabled. The memory increase depends on the attributes such as the memory requirements of the other guest VMs on the host for which memory overcommit is not enabled and HA reservations configured in the cluster. For information on memory overcommit, see Memory Overcommit Management on page 232.

Following are the possible reasons if there is an obvious hotspot, but the guest VMs do not migrate:

- ADS cannot resolve a hotspot. For example, if there is a 3-node cluster with the following specifications:

  - First node: 1 VM with 70% CPU usage and 3 VMs with 10% CPU usage. This node has 100% of CPU usage.
  - Second node: 2 VMs with 40% CPU usage. This node has 80% of CPU usage.
  - Third node: 2 VMs with 40% CPU usage. This node also has 80% of CPU usage.

  In this situation, the other hosts (second node and third node) cannot mitigate the hotspot on first node. ADS does not prioritize one host or VM over others for contention, so it leaves the VM they are already hosted.

- The number of all-flash nodes in the cluster is less than the replication factor. If the cluster has an RF2 configuration, the cluster must have a minimum of two all-flash nodes for successful migration of VMs on all the all-flash nodes.

VM Migration Restrictions with ADS

ADS does not migrate the guest VMs that are configured with the below features as part of the resource contention remediation plan:

- Windows Defender Credential Guard. For more information, see Windows Defender Credential Guard Support in AHV on page 153.
- Virtual Non-Uniform Memory Access (vNUMA). For more information, see Virtual Machine Memory Management (vNUMA) on page 203
- GPU pass-through. For more information, see GPU Pass-Through for Guest VMs on page 205.
- CPU pass-through.

For information on VM live migration restrictions, see Live Migration Restrictions on page 126.

Migrations Audit

Prism Central displays the list of all the VM migration operations generated by ADS. After you log in to Prism Central, select the **Infrastructure** application from Application Switcher Function, and navigate to **Activity** > **Audits** to view the VM migrations list. You click **Modify Filters** and select **Migrate** checkbox in the **Operation Type** field in **Filters** pane to filter the list of migration tasks. The list displays all the VM migration tasks created by ADS with details such as the source and target host, VM name, and time of migration.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1305

Disabling Acropolis Dynamic Scheduling

Perform the procedure described in this topic to disable ADS. Nutanix recommends you keep ADS enabled.

Procedure

1. Log on to a Controller VM in your cluster with SSH.
2. Disable ADS.

```
nutanix@cvm$ acli ads.update enable=false
```

No action is taken by ADS to solve the contentions after you disable the ADS feature. You must manually take the remedial actions or you can enable the feature.

Enabling Acropolis Dynamic Scheduling

If you have disabled the ADS feature and want to enable the feature, perform the following procedure.

Procedure

1. Log onto a Controller VM in your cluster with SSH.
2. Enable ADS.

```
nutanix@cvm$ acli ads.update enable=true
```

Virtualization Management Web Console Interface

You can manage the virtualization management features by using the Prism GUI (Prism Element and Prism Central web consoles).

You can do the following by using the Prism web consoles:

- Configure network connections
- Create virtual machines
- Manage virtual machines (launch console, start/shut down, take snapshots, migrate, clone, update, and delete)
- Monitor virtual machines
- Enable VM high availability

For more information, see Prism Element Web Console Guide and Prism Central Infrastructure Guide.

Finding the AHV Version on Prism Element

You can see the installed AHV version in the Prism Element web console.

About this task

To view the AHV version installed on the host, do the following.

Procedure

1. Log in to Prism Element web console.
2. The **Hypervisor Summary widget** widget on the top left side of the **Home** page displays the AHV version.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1306

Finding the AHV Version on Prism Central

About this task

You can see the installed AHV version in Prism Central.

Procedure

To view the AHV version installed on any host in the clusters managed by Prism Central, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Hardware** > **Hosts** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
   The system displays the **List** tab by default with all the hosts across registered clusters.
3. Click the target host name for which you want to see the hypervisor version.
   The system displays the Host Details View with **Summary** tab.
4. Observe the Hypervisor Version field in the **Properties** widget to view the hypervisor version.

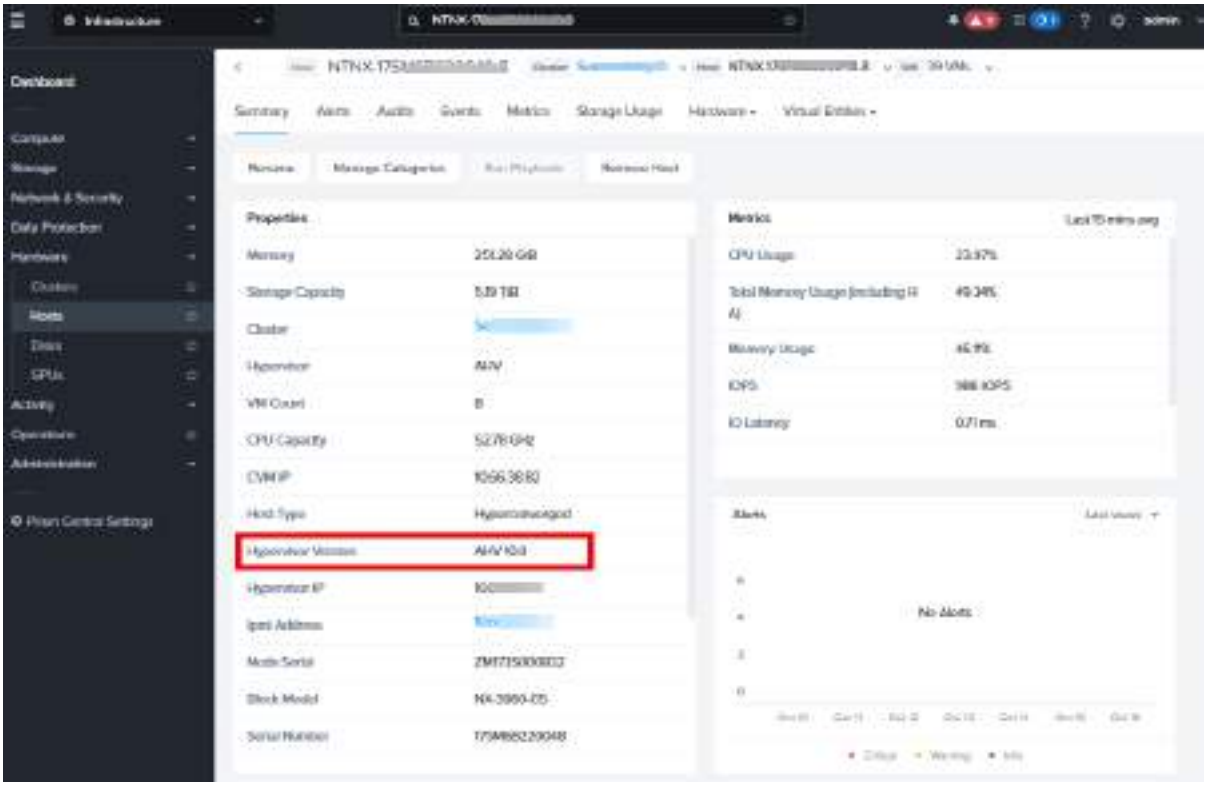


Figure 2: Hypervisor Version in Host Detail View

AHV Cluster Power Outage Handling

When a power outage occurs, the cluster goes down. After the power is restored, the Nutanix/AHV cluster is recovered by default in the following order of events:

1. Nodes have power restored - which could occur automatically or with manual intervention, depending on BIOS settings.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1307

2. The AHV host automatically starts the CVM.
3. The CVM connects to the host. The CVM can be the local CVM or another CVM in the cluster.
4. The CVM performs a series of checks to identify the VMs that were running on the hosts and applies the appropriate power-on actions.
5. The agent VMs which were previously running on the host are powered on.
6. The remaining user VMs (UVMs) which were previously running on the host are then inspected. If the UVMs were not protected by HA, then they are started. If the UVMs were protected by HA and were started on a different host, then a live migration is triggered to migrate the UVMs back to the recovered host.

Note:

- The powering on operation across hosts in case of cluster outage may not follow any order, and the checks from the CVM are also unordered. Each of the hosts are handled in parallel.
- There is no option to affect the VM start-up order or keep the VMs in powered down state.

Serial Console Redirection to a Telnet Port

The serial port is used for console redirection and to output all the AHV kernel messages to the COM port of the hardware.

To manage the serial port, log on to any CVM using SSH as the nutanix user and run the following commands:

Important: Ensure that you power cycle the VM after you add or detach a serial port for the VM, as the changes to the serial port configuration only take effect after the VM power cycle.

Table 1: Commands - Serial Port Management

Command	Description
`nutanix@cvm:~$ acli vm.serial_port_create vm name index=index type=serial port type`	Used to add a new serial port at COM1 in server mode. For example: `nutanix@cvm:~$ acli vm.serial_port_create my_vm index=0 type=kServer`
`nutanix@cvm:~$ acli vm.serial_port_delete vm name index`	Used to detach a serial port at COM1. For example: `nutanix@cvm:~$ acli vm.serial_port_delete my_vm 0`
Replace *vm name* with the VM name, *index* with the serial port index, and *type* with the serial port type.	

For information on how to capture the serial output for a Linux VM on AHV, see KB-4819.

Note: The system generates the console log of the CVM at /var/log/NTNX.serial.out.0. If a CVM is powered on, but not reachable via SSH or is in a boot loop, you can check this file to view the console output of the CVM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1308

NODE MANAGEMENT

Nonconfigurable AHV Components

The components listed here are configured by the Nutanix manufacturing and installation processes. Do not modify any of these components except under the direction of Nutanix Support.

Nutanix Software

Modifying any of the following Nutanix software settings may inadvertently constrain performance of your Nutanix cluster or render the Nutanix cluster inoperable.

- Local datastore name.
- Configuration and contents of any Controller VM (CVM) (except memory configuration to enable certain features).

Important: Note the following important considerations about CVMs.

- Do not delete the Nutanix CVM.
- Do not take a snapshot of the CVM for backup.
- Do not rename, modify, or delete the **admin** and **nutanix** user accounts of the CVM.
- Do not create additional CVM user accounts.

  Use the default accounts (**admin** or **nutanix**), or use `sudo` to elevate to the **root** account.
- Do not decrease CVM memory below recommended minimum amounts required for cluster and add-in features.

  Nutanix Cluster Checks (NCC), preupgrade cluster checks, and the AOS upgrade process detect and monitor CVM memory.
- Nutanix does not support the usage of third-party storage on the host part of Nutanix clusters.

  Normal cluster operations might be affected if there are connectivity issues with the third-party storage you attach to the hosts in a Nutanix cluster.
- Do not run any commands on a CVM that are not in the Nutanix documentation.

AHV Settings

Nutanix AHV is a cluster-optimized hypervisor appliance.

Alteration of the hypervisor appliance (unless advised by Nutanix Technical Support) is unsupported and may result in the hypervisor or VMs functioning incorrectly.

Unsupported alterations include (but are not limited to):

- Hypervisor configuration, including installed packages
- Controller VM virtual hardware configuration file (.xml file). Each AOS version and upgrade includes a specific Controller VM virtual hardware configuration. Therefore, do not edit or otherwise modify the Controller VM virtual hardware configuration file.
- iSCSI settings
- Open vSwitch settings

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1309

- Installation of third-party software not approved by Nutanix
- Installation or upgrade of software packages from non-Nutanix sources (using yum, rpm, or similar)
- Taking snapshots of the Controller VM
- Creating user accounts on AHV hosts
- Changing the timezone of the AHV hosts. By default, the timezone of an AHV host is set to UTC.
- Joining AHV hosts to Active Directory or OpenLDAP domains

Controller VM Access

Although each host in a Nutanix cluster runs a hypervisor independent of other hosts in the cluster, some operations affect the entire cluster.

Most administrative functions of a Nutanix cluster can be performed through the web console (Prism), however, there are some management tasks that require access to the Controller VM (CVM) over SSH. Nutanix recommends restricting Controller VM (CVM) SSH access with password or key authentication.

This topic provides information on how to access the CVM as an `admin` user and `nutanix` user.

> **Note:** The direct SSH access to CVM and Prism Central VM (PCVM) is disabled for the `root` user.

admin User Access

Use the `admin` user access for all tasks and operations that you must perform on the controller VM. As an `admin` user with default credentials, you cannot access nCLI. You must change the default password before you can use nCLI. Nutanix recommends that you do not create additional CVM user accounts. Use the default accounts (`admin` or `nutanix`), or use sudo to elevate to the `root` account.

For more information on `admin` user access, see Admin User Access to Controller VM on page 15.

nutanix User Access

Nutanix strongly recommends that you do not use the `nutanix` user access unless the procedure (as provided in a Nutanix Knowledge Base article or user guide) specifically requires the use of the `nutanix` user access.

For more information on `nutanix` user access, see Nutanix User Access to Controller VM on page 17.

You can perform most administrative functions of a Nutanix cluster through the Prism web consoles or REST API. Nutanix recommends using these interfaces whenever possible and disabling Controller VM SSH access with password or key authentication. Some functions, however, require logging on to a Controller VM with SSH. Exercise caution whenever connecting directly to a Controller VM as it increases the risk of causing cluster issues.

> **Warning:** When you connect to a Controller VM with SSH, ensure that the SSH client does not import or change any locale settings. The Nutanix software is not localized, and running the commands with any locale other than en_US.UTF-8 can cause severe cluster issues.
>
> To check the locale used in an SSH session, run /usr/bin/locale. If any environment variables are set to anything other than en_US.UTF-8, reconnect with an SSH configuration that does not import or change any locale settings.

Admin User Access to Controller VM

You can access the Controller VM as the admin user (admin user name and password) with SSH. For security reasons, the password of the admin user must meet Controller VM Password Complexity Requirements. When you log on to the Controller VM as the admin user for the first time, you are prompted to change the default password.

For information on setting a secure password, see Controller VM Password Complexity Requirements.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1310

After you have successfully changed the password, the new password is synchronized across all Controller VMs and interfaces (Prism web console, nCLI, and SSH).

Note:

- As an `admin` user, using the default credentials, you cannot access nCLI. If you are logging on as the `admin` user for the first time, you must log on through the Prism web console or SSH to the Controller VM. Also, you cannot change the default password of the `admin` user through nCLI. To change the default password of the `admin` user, you must log on through the Prism web console or SSH to the Controller VM.
- When you make an attempt to log in to the Prism web console for the first time after you upgrade to AOS 5.1 from an earlier AOS version, you can use your existing `admin` user password to log in and then change the existing password (you are prompted) to adhere to the password complexity requirements. However, if you are logging in to the Controller VM with SSH for the first time after the upgrade as the `admin` user, you must use the default `admin` user password (Nutanix/4u) and then change the default password (you are prompted) to adhere to the Controller VM Password Complexity Requirements.
- You cannot delete the `admin` user account.
- The default password for the `admin` user expires in (expiration age) 60 days. You can configure the minimum and maximum password expiration days based on your security requirement.

  Run the following commands to change the minimum and maximum password expiration days, respectively:

  - `nutanix@cvm$ sudo chage -m MIN-DAYS admin`
  - `nutanix@cvm$ sudo chage -M MAX-DAYS admin`

When you change the `admin` user password, you must update any applications and scripts using the `admin` user credentials for authentication. Nutanix recommends that you create a user assigned with the admin role instead of using the `admin` user for authentication. The Prism Element Web Console Guide describes authentication and roles.

Following are the default credentials to access a Controller VM.

Table 2: Controller VM Credentials

Interface	Target	User Name	Password
SSH client	Nutanix Controller VM	`admin`	Nutanix/4u
		`nutanix`	nutanix/4u
Prism web console	Nutanix Controller VM	`admin`	Nutanix/4u

Accessing the Controller VM Using the Admin User Account

About this task

Perform the following procedure to log on to the Controller VM by using the admin user with SSH for the first time.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1311

Procedure

1. Log on to the Controller VM with SSH by using the management IP address of the Controller VM and the following credentials.

   - User name: `admin`
   - Password: `Nutanix/4u`

   You are now prompted to change the default password.

2. Respond to the prompts, providing the current and new `admin` user password.

   ```
   Changing password for admin.
   Old Password:
   New password:
   Retype new password:
   Password changed.
   ```

   For information on setting a secure password, see Controller VM Password Complexity Requirements.

   For information on logging on to a Controller VM by using the `admin` user account through the Prism web console, see Logging Into The Web Console in the *Prism Element Web Console Guide*.

Nutanix User Access to Controller VM

You can access the Controller VM as the `nutanix` user (nutanix user name and password) with SSH. For security reasons, the password of the `nutanix` user must meet the Controller VM Password Complexity Requirements on page 18. When you log on to the Controller VM as the `nutanix` user for the first time, you are prompted to change the default password.

For information on setting a secure password, see Controller VM Password Complexity Requirements.

After you have successfully changed the password, the new password is synchronized across all Controller VMs and interfaces (Prism web console, nCLI, and SSH).

Note:

- As a `nutanix` user, you cannot access nCLI by using the default credentials. If you are logging in as the `nutanix` user for the first time, you must log on through the Prism web console or SSH to the Controller VM. Also, you cannot change the default password of the `nutanix` user through nCLI. To change the default password of the `nutanix` user, you must log on through the Prism web console or SSH to the Controller VM.
- When you make an attempt to log in to the Prism web console for the first time after you upgrade the AOS from an earlier AOS version, you can use your existing **nutanix** user password to log in and then change the existing password (you are prompted) to adhere to the password complexity requirements. However, if you are logging in to the Controller VM with SSH for the first time after the upgrade as the **nutanix** user, you must use the default `nutanix` user password (nutanix/4u) and then change the default password (you are prompted) to adhere to the Controller VM Password Complexity Requirements on page 18.
- You cannot delete the `nutanix` user account.
- For enhanced access restrictions for the `nutanix` user, consider enabling the **Cluster Lockdown** feature. For more information, see Controlling Cluster Access section in *Security Guide*.

  Important: Nutanix does not recommend changing the password expiry setting for the `nutanix` user account. An expired `nutanix` user account can cause cluster stability issues.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1312

When you change the `nutanix` user password, you must update any applications and scripts using the `nutanix` user credentials for authentication. Nutanix recommends that you create a user assigned with the nutanix role instead of using the `nutanix` user for authentication. The Prism Element Web Console Guide describes authentication and roles.

Following are the default credentials to access a Controller VM.

Table 3: Controller VM Credentials

Interface	Target	User Name	Password
SSH client	Nutanix Controller VM	`admin`	Nutanix/4u
		`nutanix`	nutanix/4u
Prism web console	Nutanix Controller VM	`admin`	Nutanix/4u

Accessing the Controller VM Using the Nutanix User Account

About this task

Perform the following procedure to log on to the Controller VM by using the nutanix user with SSH for the first time.

Procedure

1. Log on to the Controller VM with SSH by using the management IP address of the Controller VM and the following credentials.
   - User name: `nutanix`
   - Password: `nutanix/4u`

   You are now prompted to change the default password.
2. Respond to the prompts, providing the current and new `nutanix` user password.

   ```
   Changing password for nutanix.
   Old Password:
   New password:
   Retype new password:
   Password changed.
   ```

   For information on setting a secure password, see Controller VM Password Complexity Requirements.

   For information on logging on to a Controller VM by using the nutanix user account through the Prism web console, see Logging Into The Web Console in the *Prism Element Web Console Guide*.

Controller VM Password Complexity Requirements

The password must meet the following complexity requirements:

- At least eight characters long.
- At least one lowercase letter.
- At least one uppercase letter.
- At least one number.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1313

- At least one special character.

  Note: Ensure that the following conditions are met for the special characters usage in the CVM password:

  - The special characters are appropriately used while setting up the CVM password. In some cases, for example when you use *! followed by a number* in the CVM password, it leads to a special meaning at the system end, and the system may replace it with a command from the bash history. In this case, you may generate a password string different from the actual password that you intend to set.
  - The special character used in the CVM password are ASCII printable characters only. For information on ACSII printable characters, refer *ASCII printable characters (character code 32-127)* article on ASCII code website.

- At least four characters difference from the old password.
- Must not be among the last 5 passwords.
- Must not have more than 2 consecutive occurrences of a character.
- Must not be longer than 199 characters.

If a password for an account (CVM account) is entered five times unsuccessfully within a 15-minute period, the account is locked for 15 minutes.

AHV Host Access

You can perform most of the administrative functions of a Nutanix cluster using the Prism web consoles or REST API. Nutanix recommends using these interfaces whenever possible. Some functions, however, require logging on to an AHV host with SSH.

Note: From AOS 5.15.5 with AHV 20190916.410 onwards, AHV has two new user accounts—`admin` and `nutanix`.

Nutanix provides the following users to access the AHV host:

- `root`—It is used internally by the AOS. The root user is used for the initial access and configuration of the AHV host.
- `admin`—It is used to log on to an AHV host. The admin user is recommended for accessing the AHV host.
- `nutanix`—It is used internally by the AOS and must not be used for interactive login.

Exercise caution whenever connecting directly to an AHV host as it increases the risk of causing cluster issues.

Following are the default credentials to access an AHV host:

Table 4: AHV Host Credentials

Interface	Target	User Name	Password
SSH client	AHV Host	root	nutanix/4u
		admin	There is no default password for admin. You must set it during the initial configuration.
		nutanix	nutanix/4u

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1314

Initial Configuration

About this task

The AHV host is shipped with the default password for the `root` and `nutanix` users, which must be changed using SSH when you log on to the AHV host for the first time. After changing the default passwords and the `admin` password, all subsequent logins to the AHV host must be with the `admin` user.

Perform the following procedure to change `admin` user account password for the first time:

> **Note:** Perform this initial configuration on all the AHV hosts.

Procedure

1. Use SSH and log on to the AHV host using the `root` account.

```
$ ssh root@<AHV Host IP Address>
Nutanix AHV
root@<AHV Host IP Address> password: # default password nutanix/4u
```

2. Change the default `root` user password.

```
root@ahv# passwd root
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

3. Change the default `nutanix` user password.

```
root@ahv# passwd nutanix
Changing password for user nutanix.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

4. Change the `admin` user password.

```
root@ahv# passwd admin
Changing password for user admin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Accessing the AHV Host Using the Admin Account

About this task

After setting the `admin` password in the Initial Configuration on page 20, use the `admin` user for all subsequent logins.

Perform the following procedure to access the AHV host using the `admin` account.

Procedure

1. Log on to the AHV host with SSH using the `admin` account.

```
$ ssh admin@ <AHV Host IP Address>
Nutanix AHV
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1315

2. Enter the `admin` user password configured in the Initial Configuration on page 20.

```
admin@<AHV Host IP Address> password:
```

Changing Admin User Password

About this task

Perform these steps to change the `admin` password on every AHV host in the cluster:

Procedure

1. Log on to the AHV host using the `admin` account with SSH.
2. Enter the `admin` user password configured in the Initial Configuration on page 20.
3. Run the sudo command to change to `admin` user password.

```
$ sudo passwd admin
```

4. Respond to the prompts and provide the new password.

```
[sudo] password for admin:
Changing password for user admin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

> **Note:** Repeat this step for each AHV host.

See AHV Host Password Complexity Requirements on page 22 to set a secure password.

Changing the Root User Password

About this task

Perform these steps to change the `root` password on every AHV host in the cluster:

Procedure

1. Log on to the AHV host using the `admin` account with SSH.
2. Run the sudo command to change to `root` user.
3. Change the `root` password.

```
root@ahv# passwd root
```

4. Respond to the prompts and provide the current and new root password.

```
Changing password for root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

> **Note:** Repeat this step for each AHV host.

See AHV Host Password Complexity Requirements on page 22 to set a secure password.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1316

Changing Nutanix User Password

About this task

Perform these steps to change the `nutanix` password on every AHV host in the cluster:

Procedure

1. Log on to the AHV host using the `admin` account with SSH.
2. Run the sudo command to change to `root` user.
3. Change the `nutanix` password.

   ```
   root@ahv# passwd nutanix
   ```

4. Respond to the prompts and provide the current and new `nutanix` password.

   ```
   Changing password for nutanix.
   New password:
   Retype new password:
   passwd: all authentication tokens updated successfully.
   ```

   > **Note:** Repeat this step for each AHV host.

   See AHV Host Password Complexity Requirements on page 22 to set a secure password.

AHV Host Password Complexity Requirements

The password you choose must meet the following complexity requirements:

- In configurations with high-security requirements, the password must contain:
  - At least 15 characters.
  - At least one upper case letter (A–Z).
  - At least one lower case letter (a–z).
  - At least one digit (0–9).
  - At least one printable ASCII special (non-alphanumeric) character. For example, a tilde (~), exclamation point (!), at sign (@), number sign (#), or dollar sign ($).
  - At least eight characters different from the previous password.
  - At most three consecutive occurrences of any given character.
  - At most four consecutive occurrences of any given class.

The password cannot be the same as the last five passwords.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1317

- In configurations without high-security requirements, the password must contain:
  - At least eight characters.
  - At least one upper case letter (A–Z).
  - At least one lower case letter (a–z).
  - At least one digit (0–9).
  - At least one printable ASCII special (non-alphanumeric) character. For example, a tilde (~), exclamation point (!), at sign (@), number sign (#), or dollar sign ($).
  - At least three characters different from the previous password.
  - At most three consecutive occurrences of any given character.

The password cannot be the same as the last five passwords.

In both types of configuration, if a password for an account is entered five times unsuccessfully within a 15-minute period, the account is locked for 15 minutes.

Verifying the Cluster Health

Before you perform operations such as restarting a CVM or AHV host and putting an AHV host into maintenance mode, check if the cluster can tolerate a single-node failure.

Before you begin

Ensure that you are running the most recent version of NCC.

About this task

> **Note:** If you see any critical alerts, resolve the issues by referring to the indicated KB articles. If you are unable to resolve any issues, contact Nutanix Support.

Perform the following steps to avoid unexpected VM downtime or performance issues.

Procedure

1. Review and resolve any critical alerts. Do one of the following:
   - » In the Prism Element web console, go to the **Alerts** page.
   - » Log on to a Controller VM (CVM) with SSH and display the alerts.

     ```
     nutanix@cvm$ ncli alert ls
     ```

     > **Note:** If you receive alerts indicating expired encryption certificates or a key manager is not reachable, resolve these issues before you shut down the cluster. If you do not resolve these issues, data loss of the cluster might occur.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1318

2. Verify if the cluster can tolerate a single-node failure. Do one of the following:

   » In the Prism Element web console, in the **Home** page, check the status of the **Data Resiliency Status** dashboard.

   Verify that the status is **OK**. If the status is anything other than **OK**, resolve the indicated issues before you perform any maintenance activity.

   » Log on to a Controller VM (CVM) with SSH and check the fault tolerance status of the cluster.

   ```
   nutanix@cvm$ ncli cluster get-domain-fault-tolerance-status type=node
   ```

   An output similar to the following is displayed:

   ```
   Domain Type               : NODE
       Component Type            : STATIC_CONFIGURATION
       Current Fault Tolerance   : 1
       Fault Tolerance Details   :
       Last Update Time          : Wed Nov 18 14:22:09 GMT+05:00 2015

       Domain Type               : NODE
       Component Type            : ERASURE_CODE_STRIP_SIZE
       Current Fault Tolerance   : 1
       Fault Tolerance Details   :
       Last Update Time          : Wed Nov 18 13:19:58 GMT+05:00 2015

       Domain Type               : NODE
       Component Type            : METADATA
       Current Fault Tolerance   : 1
       Fault Tolerance Details   :
       Last Update Time          : Mon Sep 28 14:35:25 GMT+05:00 2015

       Domain Type               : NODE
       Component Type            : ZOOKEEPER
       Current Fault Tolerance   : 1
       Fault Tolerance Details   :
       Last Update Time          : Thu Sep 17 11:09:39 GMT+05:00 2015

       Domain Type               : NODE
       Component Type            : EXTENT_GROUPS
       Current Fault Tolerance   : 1
       Fault Tolerance Details   :
       Last Update Time          : Wed Nov 18 13:19:58 GMT+05:00 2015

       Domain Type               : NODE
       Component Type            : OPLOG
       Current Fault Tolerance   : 1
       Fault Tolerance Details   :
       Last Update Time          : Wed Nov 18 13:19:58 GMT+05:00 2015

       Domain Type               : NODE
       Component Type            : FREE_SPACE
       Current Fault Tolerance   : 1
       Fault Tolerance Details   :
       Last Update Time          : Wed Nov 18 14:20:57 GMT+05:00 2015
   ```

   The value of the **Current Fault Tolerance** column must be at least 1 for all the nodes in the cluster.

Node Maintenance Mode

You are required to gracefully place a node into the maintenance mode or non-operational state for reasons such as making changes to the network configuration of a node, performing manual firmware upgrades or replacements, performing CVM maintenance or any other maintenance operations.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1319

Entering and Exiting Maintenance Mode

You can only place one node at a time in maintenance mode for each cluster. When a host is in maintenance mode, the CVM is placed in maintenance mode as part of the node maintenance operation and any associated replication factor 1 enabled VMs are powered-off. The cluster marks the host as unschedulable so that no new VM instances are created on it. When a node is placed in the maintenance mode from the Prism Element web console, an attempt is made to evacuate VMs from the host. If the evacuation attempt fails, the host remains in the *entering maintenance mode* state, where it is marked unschedulable, waiting for user remediation.

When a host is placed in the maintenance mode, the non-migratable VMs (for example, pinned or replication factor 1 enabled VMs which have affinity towards a specific node) are powered-off while live migratable or high availability (HA) VMs are moved from the original host to other hosts in the cluster. After exiting the maintenance mode, all non-migratable guest VMs are powered on again and the live migrated VMs are automatically restored on the original host.

> **Note:** VMs with CPU passthrough or PCI passthrough, pinned VMs (with host affinity policies), and replication factor 1 enabled VMs are not migrated to other hosts in the cluster when a node undergoes maintenance. Click **View these VMs** link to view the list of VMs that cannot be live-migrated.

For information on how to place a node under maintenance, see Putting a Node into Maintenance Mode using Web Console on page 26.

You can also place an AHV host under maintenance mode or exit an AHV host from maintenance mode through the CLI.

> **Note:** Using the CLI method to place an AHV host under maintenance only places the hypervisor under maintenance mode. The CVM is up running in this method. To place the entire node under maintenance, Nutanix recommends using the UI method (through Prism Element web console or Prism Central).

- For information on how to use the CLI method to place an AHV host in maintenance mode, see Putting a Node into Maintenance Mode using CLI on page 30 .
- For information on how to use the CLI method to exit a node from the maintenance mode, see Exiting a Node from the Maintenance Mode Using CLI on page 32 .

Exiting a Node from Maintenance Mode

For information on how to remove a node from the maintenance mode, see Exiting a Node from the Maintenance Mode using Web Console on page 28.

Viewing a Node under Maintenance Mode

For information on how to view the node under maintenance mode, see Viewing a Node that is in Maintenance Mode on page 27.

UVM Status When Node under Maintenance Mode

For information on how to view the status of UVMs when a node is undergoing maintenance operations, see Guest VM Status when Node is in Maintenance Mode on page 29.

Best Practices and Recommendations

Nutanix strongly recommends using the **Enter Maintenance Mode** option on the Prism Element web console to place a node under maintenance.

Known Issues and Limitations

- With a minimum AOS release of 6.1.2, 6.5.1 or 6.6, you can only place one node at a time in maintenance mode for each cluster.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1320

- Entering or exiting a node under maintenance from the CLI is not equivalent to entering or exiting the node under maintenance from the Prism Element web console. For example, placing a node under maintenance from the CLI places the AHV host and CVM under maintenance while the CVM continues to remain powered on.

  Warning: You must exit the node from maintenance mode using the same method that you have used to put the node into maintenance mode. For example, if you put the node into maintenance mode using CLI, you must use CLI to exit the node from maintenance mode. Similarly, if you put the node into maintenance mode using web console, you must use the web console to exit the node from maintenance mode.

  If you put the node in maintenance mode using CLI and attempt to exit it using web console or if you put the node in maintenance mode using web console and attempt to exit it using CLI, the maintenance workflow breaks, and activities such as node upgrade and coming up of the CVM service after exiting maintenance mode get impacted.

Putting a Node into Maintenance Mode using Web Console

Before you begin

Check the cluster status and resiliency before putting a node under maintenance. You can also verify the status of the UVMs. For more information, see Guest VM Status when Node is in Maintenance Mode on page 29.

About this task

As the node enter the maintenance mode, the following high-level tasks are performed internally.

- The AHV host initiates entering the maintenance mode.
- The HA VMs are live migrated.
- The pinned and replication factor 1 enabled VMs are powered-off.
- The AHV host completes entering the maintenance mode.

  Note: At this stage, the AHV host is not shut down. For information on how to shut down the AHV host, see Shutting Down a Node in a Cluster (AHV). You can list all the hosts in the cluster by running nutanix@cvm$ acli host.list command, and note the value of *Hypervisor IP* for the node you want to shut down.

- The CVM enters the maintenance mode.
- The CVM is shut down.

Perform the following steps to put the node into maintenance mode.

Procedure

1. Login to the Prism Element web console.
2. On the home page, select **Hardware** from the drop-down menu.
3. Go to the **Table** > **Host** view.
4. Select the node which you intend to put under maintenance.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1321

5. Click the **Enter Maintenance Mode** option.
   The **Host Maintenance** window appears with a prompt to power-off all VMs that cannot be live migrated.

   > **Note:** VMs with CPU passthrough, PCI passthrough, pinned VMs (with host affinity policies), and replication factor 1 are not migrated to other hosts in the cluster when a node undergoes maintenance. Click **View these VMs** link to view the list of VMs that cannot be live-migrated.

6. Select the **Power-off VMs that can not migrate** checkbox to enable the **Enter Maintenance Mode** button.
7. Click the **Enter Maintenance Mode** button.

   - A revolving icon appears as a tool tip beside the selected node and also in the Host Details view. This indicates that the host is entering the maintenance mode.
   - The revolving icon disappears and the **Exit Maintenance Mode** option is enabled after the node completely enters the maintenance mode.
   - You can also monitor the progress of the node maintenance operation through the newly created Host enter maintenance and Enter maintenance mode tasks which appear in the task tray.

     > **Note:** In case of a node maintenance failure, certain rolled-back operations are performed. For example, the CVM is rebooted. But the live migrated are not restored to the original host.

What to do next

Once the maintenance activity is complete, you can perform any of the following.

- View the nodes under maintenance. For more information, see Viewing a Node that is in Maintenance Mode on page 27.
- View the status of the UVMs. For more information, see Guest VM Status when Node is in Maintenance Mode on page 29.
- Remove the node from the maintenance mode. For more information, see Exiting a Node from the Maintenance Mode using Web Console on page 28.

Viewing a Node that is in Maintenance Mode

About this task

> **Note:** This procedure is the same for AHV and ESXi nodes.

Perform the following steps to view a node under maintenance.

Procedure

1. Login to the Prism Element web console.
2. On the home page, select **Hardware** from the drop-down menu.
3. Go to the **Table** > **Host** view.
4. Observe the icon along with a tool tip that appears beside the node which is under maintenance. You can also view this icon in the host details view.
5. Alternatively, view the node under maintenance from the **Hardware** > **Diagram** view.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1322

What to do next

You can:

- View the status of the guest VMs. For more information, see Guest VM Status when Node is in Maintenance Mode on page 29.
- Remove the node from the maintenance mode. For more information, see Exiting a Node from the Maintenance Mode using Web Console on page 28Exiting a Node from the Maintenance Mode (vSphere).

Exiting a Node from the Maintenance Mode using Web Console

After you perform any maintenance activity, exit the node from the maintenance mode.

About this task

> **Warning:** You must exit the node from maintenance mode using the same method that you have used to put the node into maintenance mode. For example, if you put the node into maintenance mode using CLI, you must use CLI to exit the node from maintenance mode. Similarly, if you put the node into maintenance mode using web console, you must use the web console to exit the node from maintenance mode.
>
> If you put the node in maintenance mode using CLI and attempt to exit it using web console or if you put the node in maintenance mode using web console and attempt to exit it using CLI, the maintenance workflow breaks, and activities such as node upgrade and coming up of the CVM service after exiting maintenance mode get impacted.

As the node exits the maintenance mode, the following high-level tasks are performed internally.

- The CVM is powered on.
- The CVM is taken out of maintenance.
- The host is taken out of maintenance.

> **Note:** The AHV host is shut down during Putting a Node into Maintenance Mode using Web Console on page 26 and it is required to power on the AHV host. For information on how to power on the AHV host, see Starting a Node in a Cluster (AHV).

After the host exits the maintenance mode, the replication factor 1 enabled VMs continue to be powered on and the VMs migrate to restore host locality.

For more information, see Guest VM Status when Node is in Maintenance Mode on page 29 to view the status of the UVMs.

Perform the following steps to remove the node into maintenance mode.

Procedure

1. On the Prism Element web console home page, select **Hardware** from the drop-down menu.
2. Go to the **Table** > **Host** view.
3. Select the node which you intend to remove from the maintenance mode.
4. Click the **Exit Maintenance Mode** option.
   The **Host Maintenance** window appears.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1323

5. Click the **Exit Maintenance Mode** button.

   - A revolving icon appears as a tool tip beside the selected node and also in the Host Details view. This indicates that the host is exiting the maintenance mode.
   - The revolving icon disappears and the **Enter Maintenance Mode** option is enabled after the node completely exits the maintenance mode.
   - You can also monitor the progress of the exit node maintenance operation through the newly created Host exit maintenance and Exit maintenance mode tasks which appear in the task tray.

What to do next

Once a node exits the maintenance mode, you can perform any of the following.

- View the status of node under maintenance. For more information, see Viewing a Node that is in Maintenance Mode on page 27.
- View the status of the UVMs. For more information, see Guest VM Status when Node is in Maintenance Mode on page 29.

Guest VM Status when Node is in Maintenance Mode

The following scenarios demonstrate the behavior of three guest VM types - high availability (HA) VMs, pinned VMs, and replication factor 1 enabled VMs, when a node enters and exits a maintenance operation. The HA VMs are live VMs that can migrate across nodes if the host server goes down or reboots. The pinned VMs have the host affinity set to a specific node. The replication factor 1 enabled VMs have affinity towards a specific node or a Controller VM (CVM). To view the status of the guest VMs, go to **VM** > **Table**.

> **Note:** The following scenarios are the same for AHV and ESXi nodes.

Scenario 1: Guest VMs before Node Entering Maintenance Mode

All the guest VMs are powered-on and reside on the same host.

Scenario 2: Guest VMs during Node Maintenance Mode

As the node enter the maintenance mode, the following high-level tasks are performed internally.

1. The host initiates entering the maintenance mode.
2. The HA VMs are live migrated.
3. The pinned and replication factor 1 enabled VMs are powered-off.
4. The AHV host completes entering the maintenance mode.
5. The CVM enters the maintenance mode.
6. The CVM is shut down.

Scenario 3: Guest VMs after Node Exiting Maintenance Mode

As the node exits the maintenance mode, the following high-level tasks are performed internally.

1. The CVM is powered on.
2. The CVM is taken out of maintenance.
3. The host is taken out of maintenance.

After the host exits the maintenance mode, the replication factor 1 enabled VMs continue to be powered on and the VMs migrate to restore host locality.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1324

Putting a Node into Maintenance Mode using CLI

You are required to put a node into maintenance mode for reasons such as making changes to the network configuration of a node, performing manual firmware upgrades, or any other.

Before you begin

> **Caution:** Verify the data resiliency status of your cluster. If the cluster only has replication factor 2 (RF2), you can only shut down one node for each cluster. If an RF2 cluster would have more than one node shut down, shut down the entire cluster.

About this task

When a host is put in maintenance mode:

- AOS marks the host as unschedulable so that no new VM instances are created on it. Next, an attempt is made to evacuate VMs from the host.

  If the evacuation attempt fails, the host remains in the "entering maintenance mode" state, where it is marked unschedulable, waiting for user remediation. You can shut down VMs on the host or move them to other nodes. Once the host has no more running VMs, it is in maintenance mode.

- VMs are moved from that host to other hosts in the cluster. After exiting maintenance mode, those VMs are automatically returned to the original host, eliminating the need to manually move them. However, some VMs cannot be migrated to other hosts. For more information, see Non-Migratable VMs.

  You can choose to shut down such VMs while putting the node into maintenance mode.

Agent VMs are always shut down if you put a node in maintenance mode and are powered on again after exiting maintenance mode.

Perform the following steps to put the node into maintenance mode.

Procedure

1. Use SSH to log on to a Controller VM in the cluster.
2. Determine the IP address of the node you want to put into maintenance mode.

   ```
   nutanix@cvm$ acli host.list
   ```

   Note the value of **Hypervisor IP** for the node you want to put in maintenance mode.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1325

3. Put the node into maintenance mode.

```
nutanix@cvm$ acli host.enter_maintenance_mode hypervisor-IP-address [wait="{ true |
 false }" ] [non_migratable_vm_action="{ acpi_shutdown | block }" ]
```

> **Note:** Never put Controller VM and AHV hosts into maintenance mode on single-node clusters. It is recommended to shutdown user VMs before proceeding with disruptive changes.

Replace *hypervisor-IP-address* with either the IP address or host name of the AHV host you want to shut down.

The following are optional parameters for running the `acli host.enter_maintenance_mode` command:

- **wait**: Set the **wait** parameter to **true** to wait for the host evacuation attempt to finish.
- **non_migratable_vm_action**: By default the **non_migratable_vm_action** parameter is set to **block**, which means the non-migratable VMs are shut down when you put a node into maintenance mode. For more information on non-migratable VMs, see Non-Migratable VMs.

  > **Note:** VMs with host affinity policies are also not migrated to other hosts in the cluster, if any of the following condition is met:
  >
  > - The hosts that are configured as part of VM-Host affinity policy are not available.
  > - The hosts that are part of VM-Host affinity policy does not have the sufficient resources to run the VM.

  If you want to automatically shut down such VMs, set the **non_migratable_vm_action** parameter to **acpi_shutdown**.

4. Verify if the host is in the maintenance mode.

```
nutanix@cvm$ acli host.get host-ip
```

In the output that is displayed, ensure that **node_state** equals to **EnteredMaintenanceMode** and **schedulable** equals to **False**.

Do not continue if the host has failed to enter the maintenance mode.

5. See Verifying the Cluster Health on page 23 to once again check if the cluster can tolerate a single-node failure.

6. Put the CVM into the maintenance mode.

```
nutanix@cvm$ ncli host edit id=host-ID enable-maintenance-mode=true
```

Replace *host-ID* with the ID of the host.

This step prevents the CVM services from being affected by any connectivity issues.

7. Determine the ID of the host.

```
nutanix@cvm$ ncli host list
```

An output similar to the following is displayed:

```
Id                        : aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee::1234
Uuid                      : ffffffff-gggg-hhhh-iiii-jjjjjjjjjjj
Name                      : XXXXXXXXXX-X
IPMI Address              : X.X.Z.3
Controller VM Address     : X.X.X.1
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1326

```
Hypervisor Address        : X.X.Y.2
```

In this example, the host ID is 1234.

Wait for a few minutes until the CVM is put into the maintenance mode.

8. Verify if the CVM is in the maintenance mode.

   Run the following command on the CVM that you put in the maintenance mode.

   ```
   nutanix@cvm$ genesis status | grep -v "\[\]"
   ```

   An output similar to the following is displayed:

   ```
   nutanix@cvm$ genesis status | grep -v "\[\]"
   2021-09-24 05:28:03.827628: Services running on this node:
     genesis: [11189, 11390, 11414, 11415, 15671, 15672, 15673, 15676]
     scavenger: [27241, 27525, 27526, 27527]
     xmount: [25915, 26055, 26056, 26074]
     zookeeper: [13053, 13101, 13102, 13103, 13113, 13130]
   nutanix@cvm$
   ```

   Only the Genesis, Scavenger, Xmount, and Zookeeper processes must be running (process ID is displayed next to the process name).

   Do not continue if the CVM has failed to enter the maintenance mode, because it can cause a service interruption.

What to do next

Perform the maintenance activity. Once the maintenance activity is complete, remove the node from the maintenance mode. See Exiting a Node from the Maintenance Mode Using CLI on page 32 for more information.

Exiting a Node from the Maintenance Mode Using CLI

After you perform any maintenance activity, exit the node from the maintenance mode.

About this task

> **Warning:** You must exit the node from maintenance mode using the same method that you have used to put the node into maintenance mode. For example, if you put the node into maintenance mode using CLI, you must use CLI to exit the node from maintenance mode. Similarly, if you put the node into maintenance mode using web console, you must use the web console to exit the node from maintenance mode.
>
> If you put the node in maintenance mode using CLI and attempt to exit it using web console or if you put the node in maintenance mode using web console and attempt to exit it using CLI, the maintenance workflow breaks, and activities such as node upgrade and coming up of the CVM service after exiting maintenance mode get impacted.

Perform the following to exit the host from the maintenance mode.

Procedure

1. Remove the CVM from the maintenance mode.

   a. Determine the ID of the host.

   ```
   nutanix@cvm$ ncli host list
   ```

   An output similar to the following is displayed:

   ```
   Id                        : aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee::1234
   Uuid                      : ffffffff-gggg-hhhh-iiii-jjjjjjjjjjj
   Name                      : XXXXXXXXXX-X
   ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1327

```
IPMI Address              : X.X.Z.3
Controller VM Address     : X.X.X.1
Hypervisor Address        : X.X.Y.2
```

In this example, the host ID is 1234.

a. From any other CVM in the cluster, run the following command to exit the CVM from the maintenance mode.

```
nutanix@cvm$ ncli host edit id=host-ID enable-maintenance-mode=false
```

Replace *host-ID* with the ID of the host.

> **Note:** The command fails if you run the command from the CVM that is in the maintenance mode.

b. Verify if all the processes on all the CVMs are in the UP state.

```
nutanix@cvm$ cluster status | grep -v UP
```

Do not continue if the CVM has failed to exit the maintenance mode.

2. Remove the AHV host from the maintenance mode.

a. From any CVM in the cluster, run the following command to exit the AHV host from the maintenance mode.

```
nutanix@cvm$ acli host.exit_maintenance_mode hypervisor-IP-address
```

Replace *hypervisor-IP-address* with the new IP address of the host.

This command migrates (live migration) all the VMs that were previously running on the host back to the host.

b. Verify if the host has exited the maintenance mode.

```
nutanix@cvm$ acli host.get hypervisor-IP-address
```

In the output that is displayed, ensure that **node_state** equals to **kAcropolisNormal** or **AcropolisNormal** and **schedulable** equals to **True**.

Contact Nutanix Support if any of the steps described in this document produce unexpected results.

Shutting Down a Node in a Cluster (AHV)

Before you begin

> **Caution:** Verify the data resiliency status of your cluster. If the cluster only has replication factor 2 (RF2), you can only shut down one node for each cluster. If an RF2 cluster would have more than one node shut down, shut down the entire cluster.

See Verifying the Cluster Health on page 23 to check if the cluster can tolerate a single-node failure. Do not proceed if the cluster cannot tolerate a single-node failure.

About this task

Perform the following procedure to shut down a node.

Procedure

1. Put the node into maintenance mode as described in Putting a Node into Maintenance Mode using Web Console on page 26.
2. Log on to the AHV host with SSH.
3. Shut down the host.

```
root@ahv# shutdown -h now
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1328

What to do next

See Starting a Node in a Cluster (AHV) on page 34 for instructions about how to start a node, including how to start a CVM and how to exit a node from maintenance mode.

Starting a Node in a Cluster (AHV)

About this task

Procedure

1. On the hardware appliance, power on the node. The CVM starts automatically when your reboot the node.
2. If the node is in maintenance mode, log on to Prism Web Console and remove the node from the maintenance mode.

   See Exiting a Node from the Maintenance Mode using Web Console on page 28 for more information.
3. Log on to another CVM in the Nutanix cluster with SSH.
4. Verify that the status of all services on all the CVMs are Up.

   ```
   nutanix@cvm$ cluster status
   ```

   If the Nutanix cluster is running properly, output similar to the following is displayed for each node in the Nutanix cluster.

   ```
   CVM:host IP-Address Up
                                   Zeus   UP       [9935, 9980, 9981, 9994, 10015,
   10037]
                             Scavenger   UP       [25880, 26061, 26062]
                               Xmount   UP       [21170, 21208]
                       SysStatCollector   UP       [22272, 22330, 22331]
                              IkatProxy   UP       [23213, 23262]
                       IkatControlPlane   UP       [23487, 23565]
                          SSLTerminator   UP       [23490, 23620]
                        SecureFileSync   UP       [23496, 23645, 23646]
                                 Medusa   UP       [23912, 23944, 23945, 23946, 24176]
                    DynamicRingChanger   UP       [24314, 24404, 24405, 24558]
                                Pithos   UP       [24317, 24555, 24556, 24593]
                            InsightsDB   UP       [24322, 24472, 24473, 24583]
                                Athena   UP       [24329, 24504, 24505]
                               Mercury   UP       [24338, 24515, 24516, 24614]
                                Mantle   UP       [24344, 24572, 24573, 24634]
                            VipMonitor   UP       [18387, 18464, 18465, 18466, 18474]
                              Stargate   UP       [24993, 25032]
                  InsightsDataTransfer   UP       [25258, 25348, 25349, 25388, 25391,
   25393, 25396]
                                 Ergon   UP       [25263, 25414, 25415]
                               Cerebro   UP       [25272, 25462, 25464, 25581]
                               Chronos   UP       [25281, 25488, 25489, 25547]
                               Curator   UP       [25294, 25528, 25529, 25585]
                                 Prism   UP       [25718, 25801, 25802, 25899, 25901,
   25906, 25941, 25942]
                                   CIM   UP       [25721, 25829, 25830, 25856]
                          AlertManager   UP       [25727, 25862, 25863, 25990]
                              Arithmos   UP       [25737, 25896, 25897, 26040]
                               Catalog   UP       [25749, 25989, 25991]
                             Acropolis   UP       [26011, 26118, 26119]
                                 Uhura   UP       [26037, 26165, 26166]
                                  Snmp   UP       [26057, 26214, 26215]
                     NutanixGuestTools   UP       [26105, 26282, 26283, 26299]
   ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1329

```
                          MinervaCVM   UP       [27343, 27465, 27466, 27730]
                       ClusterConfig   UP       [27358, 27509, 27510]
                            Aequitas   UP       [27368, 27567, 27568, 27600]
                          APLOSEngine   UP       [27399, 27580, 27581]
                               APLOS   UP       [27853, 27946, 27947]
                               Lazan   UP       [27865, 27997, 27999]
                              Delphi   UP       [27880, 28058, 28060]
                                Flow   UP       [27896, 28121, 28124]
                             Anduril   UP       [27913, 28143, 28145]
                               XTrim   UP       [27956, 28171, 28172]
                       ClusterHealth   UP       [7102, 7103, 27995, 28209,28495,
 28496, 28503, 28510,
28573, 28574, 28577, 28594, 28595, 28597, 28598, 28602, 28603, 28604, 28607, 28645,
 28646, 28648, 28792,
28793, 28837, 28838, 28840, 28841, 28858, 28859, 29123, 29124, 29127, 29133, 29135,
 29142, 29146, 29150,
29161, 29162, 29163, 29179, 29187, 29219, 29268, 29273]
```

Rebooting an AHV Node in a Nutanix Cluster

About this task

The **Request Reboot** operation in the Prism Element web console gracefully restarts the selected nodes one after the other.

> **Note:** Reboot host is a graceful restart workflow. Hosts are automatically put into maintenance mode and all the user VMs are migrated to another host when you perform a reboot operation for a host. There is no impact on the user workload due to the reboot operation.

Procedure

To reboot the nodes in the cluster, perform the following steps:

1. Log on to the Prism Element web console.
2. Click **Settings** from the drop-down menu of the Prism Element web console and then select **Reboot**.
3. In the **Request Reboot** window, select the checkbox associated with the nodes you want to restart, and click **Reboot**.

   A progress bar is displayed that indicates the progress of the restart of each node.

Shutting Down an AHV Cluster

You might need to shut down an AHV cluster to perform a maintenance activity or tasks such as relocating the hardware.

Before you begin

Ensure that you meet the following prerequisites before you shut down the cluster:

- IPMI password is accessible as it is required to perform power actions through IPMI.
- The NCC is upgraded to the most recent version.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1330

- The NCC health check is performed on the cluster.

  Log on to a Controller VM (CVM) with SSH and run the complete NCC health check.

  ```
  nutanix@cvm$ ncc health_checks run_all
  ```

  If you receive any failure or error messages, resolve those issues by referring to the KB articles indicated in the output of the NCC check results. If you are unable to resolve these issues, contact Nutanix Support.

  > **Warning:** If you receive alerts indicating expired encryption certificates or that the external Key Management Service (KMS) is inaccessible, it is imperative to resolve these issues prior to shutting down the cluster. Neglecting these issues may lead to potential data loss for the cluster.

About this task

Shut down an AHV cluster in the following sequence.

Procedure

1. Shut down the services or VMs associated with AOS features or Nutanix products. For example, shut down all the Nutanix file server VMs (FSVMs). For more information, see the features or product documentation.
2. Power off all the running guest VMs in the cluster from within the guest OS.

   > **Note:** If you are running multiple VMs, you can shut down all the guest VMs in the cluster by using the Prism Element web console or by using a CLI. For more information, see *Managing a VM through Prism Central* or *Shutting Down VMs using aCLI* in *Managing a VM (AHV)* section.

   a. Log on to a CVM in the cluster with SSH.

   b. Verify if all the guest VMs are shut down.

   ```
   nutanix@CVM$ acli vm.list power_state=on
   ```

   c. If any VMs are on, consider powering off the VMs from within the guest OS. To force shut down the VMs through AHV using a CLI see *Shutting Down VMs using aCLI*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1331

3. Stop the Nutanix cluster.

   a. Log on to any CVM in the cluster with SSH.

   b. Stop the cluster.

   ```
   nutanix@cvm$ cluster stop
   ```

   c. Verify if the cluster services have stopped.

   ```
   nutanix@CVM$ cluster status
   ```

   The output displays the message The state of the cluster: stop, which confirms that the cluster has stopped.

   Note: Some system services may continue to run even after the cluster has stopped successfully:

   - Zeus
   - Scavenger
   - Xmount
   - VIPMonitor
   - IkatProxy

   You can observe the status of these system services in the output logs:

   ```
   The state of the cluster: stop
                                        Lockdown mode: Disabled  CVM:
    10.xx.x.xxx Up
                                        Zeus UP  [13130, 13326, 13327,
    13347]
                                        Scavenger UP  [15015, 15141, 15142,
    15143]
                                        Xmount UP  [15012, 15121, 15122,
    15147]
                                        IkatProxy UP  [1917, 1116, 111]
                                        VipMonitor UP  [25898, 25899,
    25900, 25901, 25904]
                                        SysStatCollector DOWN       []
                                        IkatControlPlane DOWN       []
                                        SecureFileSync DOWN       []
                                        Medusa DOWN       []
                                        DynamicRingChanger DOWN       []
                                        Pithos DOWN       []
                                        InsightsDB DOWN       []
                                        Athena DOWN       []
                                        Mercury DOWN       []
                                        Mantle DOWN       []
                                        VipMonitor   UP       [207546,
    204567, 20448, 20549, 204784]
   ```

4. Shut down all the CVMs in the cluster. Perform the following steps for each CVM in the cluster.

   a. Log on to each CVM in the cluster with SSH and shut down that CVM.

   ```
   nutanix@cvm$ sudo shutdown -P now
   ```

   b. Ping each CVM (ping *cvm_ip_addr*) to verify that all CVMs are shut down.
   Replace *cvm_ip_addr* with the CVM IP address.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1332

5. Shut down each node in the cluster. Perform the following steps for each node in the cluster.

   a. Log on to the IPMI web console of each node.

   b. Under **Remote Control** > **Power Control**, select **Power Off Server - Orderly Shutdown** to gracefully shut down the node.

      Note: The navigation path, tabs, and UI layout in IPMI web console can vary based on the hardware used at your site.

   c. Ping each host (`ping hypervisor_ip_addr`) to verify that all AHV hosts are shut down.

      Replace `hypervisor_ip_addr` with the hypervisor IP address.

6. Complete the maintenance activity or any other tasks.

What to do next

Starting Up an AHV Cluster on page 38.

Starting Up an AHV Cluster

You might need to start up an AHV cluster after a maintenance activity or tasks such as relocating the hardware is completed.

Before you begin

Ensure that you meet the following prerequisites before you shut down the cluster:

- IPMI password is accessible as it is required to perform power actions through IPMI.

About this task

Start up an AHV cluster in the following sequence.

Procedure

1. Start all the nodes in the cluster.

   a. Press the power button on the front of the block for each node.

   b. Log on to the IPMI web console of each node.

   c. On the **System** tab, check the **Power Control** status to verify if the node is powered on.

      Note: The navigation path, tabs, and UI layout in IPMI web console can vary based on the hardware used at your site.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1333

2. Start the cluster.

   a. Wait for approximately 5 minutes after you start the last node to allow the cluster services to start.
      All CVMs start automatically after you start all the nodes.

   b. Log on to any CVM in the cluster with SSH.

   c. Start the cluster.

      ```
      nutanix@cvm$ cluster start
      ```

   d. Verify that all the cluster services are in the UP state.

      ```
      nutanix@cvm$ cluster status
      ```

3. Start the guest VMs from within the guest OS, you can also use the Prism Element web console or CLI. For more information, see *Managing a VM through Prism Central* or *Starting Up VMs using aCLI* in *Managing a VM (AHV)* section.

   > **Note:** If you are running many VMs, you can start the VMs by using a CLI. For more information, see *Starting Up VMs using aCLI*.

4. Start the services or VMs associated with AOS features or Nutanix products. For example, start all the FSVMs. See the documentation of those features or products for more information.

5. Verify if all guest VMs are powered on by using the Prism Element web console.

Changing CVM Memory Configuration (AHV)

About this task

You can increase the memory reserved for each Controller VM in your cluster by using the 1-click Controller VM Memory Upgrade available from the Prism Element web console. Increase memory size depending on the workload type or to enable certain AOS features. See the Increasing the Controller VM Memory Size topic in the *Prism Element Web Console Guide* for CVM memory sizing recommendations and instructions about how to increase the CVM memory.

Renaming an AHV Host

You can rename an AHV host from Prism Central.

About this task

The minimum supported versions to rename an AHV host from Prism Central are AOS 6.6 for the registered Prism Element (with recommended AHV version) and 2022.9 for Prism Central. For information on the recommended AHV version based on the AOS release and hardware model, see Compatibility and Interoperability Matrix.

To rename an AHV host from Prism Central, perform the following steps:

Procedure

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Hardware** > **Hosts** .
   The system displays the **List** tab by default with all the hosts across registered clusters.

3. Select the target host checkbox, and choose **Rename** from the **Actions** dropdown menu.
   The system displays the **Rename Host** window.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1334

4. Enter a new name for the host in the **New Host Name** field, and click **Save**.

   You must adhere to the following rules for the host name:

   - Allowed characters are: uppercase letters (A-Z), lowercase letters (a-z), decimal digits (0-9), dots (.), and hyphens (-).
   - The host name must start and end with a number or letter.
   - A minimum of one character and a maximum of 63 characters are allowed.
   - Successive dots are not allowed. Each dot-separated string must follow the first two rules.

   Note: Once the AHV host rename task is complete, it might take a few minutes for the changes to propagate from the host to Prism Central.

Changing the Name of the CVM Displayed in Prism

You can change the CVM name that is displayed in Prism. The procedure described in this document does not change the CVM name that is displayed in the terminal or console of an SSH session.

About this task

You can change the CVM name by using the `change_cvm_display_name` script. Run this script from a CVM other than the CVM you want to rename. When you run the `change_cvm_display_name` script, AOS performs the following steps:

- **1.** Checks if the new name starts with **NTNX-** and ends with **-CVM**. The CVM name must have only letters, numbers, and dashes (-).
  2. Checks if the CVM has received a shutdown token.
  3. Powers off the CVM. The script does not put the CVM or host into maintenance mode. Therefore, the VMs are not migrated from the host and continue to run with the I/O operations redirected to another CVM while the current CVM is in a powered off state.
  4. Changes the CVM name, enables auto-start, and powers on the CVM.

Procedure

Perform the following steps to change the CVM name displayed in Prism:

1. Log in to the CVM other than the CVM you want to rename using SSH.
2. Change the name of the CVM.

   ```
   nutanix@cvm$ change_cvm_display_name --cvm_ip=CVM-IP --cvm_name=new-name
   ```

   Replace *CVM-IP* with the IP address of the CVM whose name you want to change and *new-name* with the new name for the CVM.

   The CVM name must have only letters, numbers, and dashes (-), and must start with **NTNX-** and end with **-CVM**.

   Note: Do not run this command from the CVM you want to rename, because the script powers off the CVM. In this case, when the CVM is powered off, you lose connectivity to the CVM from the SSH console and the script abruptly ends.

What to do next

For clusters running AOS 6.8.x and AHV 20230302.100173 or newer version, the following additional configuration steps are required:

1. Log in to the AHV host associated with the renamed CVM using SSH.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1335

2. Update the CVM name in the `cvm_config.json` file using the following command:

   ```
   root@ahv# jq '.name = "new-cvm-name"' /etc/nutanix/config/cvm_config.json > /etc/
   nutanix/config/cvm_config.json.tmp
   ```

   Replace *new-cvm-name* with the new CVM name.
3. Verify whether the CVM name is updated in the /etc/nutanix/config/cvm_config.json.tmp file.
4. Replace the original `cvm_config.json` file with the new version using the following command:

   ```
   root@ahv# mv /etc/nutanix/config/cvm_config.json.tmp /etc/nutanix/config/
   cvm_config.json
   ```

Adding an AHV Storage-Only Node

Add a storage-only (SO) node if you want to add a node to increase data storage on your Nutanix cluster, but do not want any AHV VMs to run on that node.

About this task

AOS never schedules any VMs on the SO node. Therefore, the SO node configuration ensures that no additional compute resources such as CPUs are consumed from the Nutanix cluster. In this way, you can meet the compliance and licensing requirements of your virtual applications.

Note the following points about the SO node configuration.

Note:

- Ensure that at any given time, the cluster has a minimum of three nodes (SO nodes or otherwise) in function. To add your first SO node to the Nutanix cluster, the cluster must comprise of at least three schedulable nodes.
- You can add any number of SO nodes to your Nutanix cluster.
- If you want a node that is already a part of the cluster to work as the SO node, remove that node from the cluster and then add that node as the SO node.
- If you no longer need a node to work as the SO node, remove the node from the cluster.
- Foundation allocates the maximum resources to Controller VM (CVM) of the SO node as follows:
  - CVM vCPU = Number of physical host CPUs minus 2, limited to a maximum of 22 vCPUs.

    Note: This is applicable till Foundation version 5.3.x. From Foundation version 5.4 onwards, the capping of maximum 22 vCPUs is not applicable.
  - CVM memory = Available RAM minus 16 GiB, limited to a maximum of 256 GiB.

    Note:

    - This is applicable from Foundation version 5.3 and above. In the earlier Foundation versions, the memory allocation happens without capping to 256 GiB.
    - A capping of maximum 256 GiB is applied, and Foundation allocates the maximum possible vRAM to CVM. For example, if the available RAM is 512 GiB, the system allocates a maximum of 256 GiB and never considers the 512-16 = 496 GiB value.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1336

However, if you change the system allocated vRAM, the vRAM gets overridden with the supplied value.

Note: Minimum Foundation version of 5.3 supports these limits with NUMA pinnings or alignments. Earlier Foundation versions with a minimum version of 5.0 support these limits but not NUMA pinnings or alignments.

Procedure

You can add the SO node to a cluster using the **Expand Cluster** operation from Prism Web Console.

For information on how to add the SO node to a cluster, see the Expanding a Cluster topic in *Prism Element Web Console Guide*.

AHV Compute-Only Node Configuration

The Nutanix cluster uses the resources (CPUs and memory) of a compute-only (CO) node exclusively for computing purposes. A compute-only (CO) node allows you to seamlessly and efficiently expand the computing capacity (CPU and memory) of your AHV cluster.

Use Cases of AHV Compute-Only Nodes

CO nodes enable you to achieve more control and value from restrictive licenses such as Oracle. There is no Controller VM (CVM) running on the CO node (VMs use CVMs running on the HCI nodes to access disks). When a CO node is part of a Nutanix Hyperconverged Infrastructure (HCI) cluster, then license cores of the CO nodes are used only for the application VMs.

Applications or databases that are licensed on a per CPU core basis require the entire node to be licensed and that also includes the cores on which the CVM runs. With CO nodes, you get a much higher ROI on the purchase of your database licenses (such as Oracle and Microsoft SQL Server) since the CVM does not consume any compute resources.

AHV CO nodes support the following two types of deployments:

- AHV CO node with AHV HCI node. For more information, see Deployment Specifications and Considerations for Compute-Only and Storage-Only Nodes in the *Prism Element Web Console Guide*.
- AHV CO node with AHV Storage-only (SO) node. For more information, see Optimized Database Solution in the *Prism Element Web Console Guide*.

Reinstalling AHV on a Node

This section describes how to reinstall AHV on a node.

About this task

This procedure prompts you to upload the AHV ISO image. You can download it from the AHV Downloads page.

Note: Starting with AHV 10.0, the AHV download is provided through a single zip file containing the AHV Installer (ISO) and Open Source Disclosure files. You can extract the AHV ISO file from the AHV installer zip file for workflows requiring the AHV ISO file.

Procedure

To reinstall AHV on a node, perform the following steps:

1. Log in to Prism Element Web Console.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1337

2. Navigate to **Hardware** > **Diagram** view, and select the node on which you want to reinstall AHV
3. Click **Repair Host Boot Disk**.
4. From the window, select **Continue without snapshot**.
5. Click **Next**.
   The system displays the **Download Phoenix Image** window.
6. Click **Download** to download the phoenix.iso.

   > **Note:** Keep the **Repair Host Boot Disk** window open, and do not click **Next** until you have started the node with the downloaded phoenix.iso in the next step.

7. Bring up the node with the phoenix.iso file. For more information, see Starting the Node from the Phoenix Image.
8. Click **Next**.
   If you have closed the **Repair Host Boot Disk** window after downloading the phoenix.iso image in step 6 on page 43, repeat step 2 on page 43 to step 5 on page 43 , and then click **Next**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1338

9. Click **Choose file** to upload the AHV ISO.

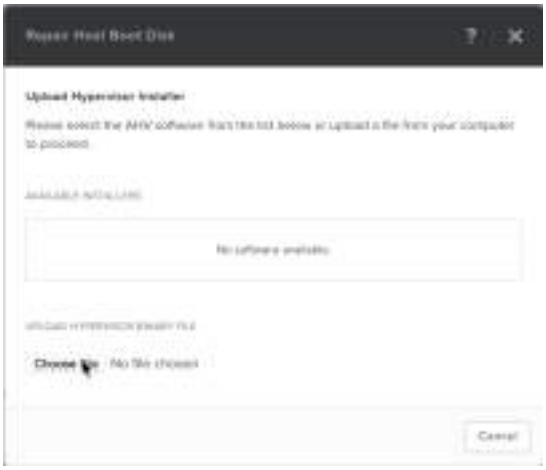


Figure 3: Choose File Menu

a. In the file search window or finder window, go to the location of the appropriate AHV ISO file and select the file.

   The file that you select appears in the **Available Installers** menu. The checksum completes.

b. From the **Available Installers** menu, click **Proceed**.

Figure 4: Available AHV Installers Menu

10. If the prompt Are you sure you wish to repair the boot disk for this node? appears, click Yes.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1339

11. Monitor the boot disk repair process.

    The system performs the repair prechecks, and starts the node imaging process. The imaging duration is 30 to 40 minutes.

    You can check the status in the **Tasks** menu, in a console window, or by clicking **Repair Host Boot Disk**.

Figure 5: Tasks Menu Status View

12. Review or change the following settings, if required:

    a. AHV host IP address.

       Check the AHV host IP address is correctly assigned as per the preferred network design for that cluster. If the AHV host IP address is incorrect, update the IP address. For more information, see Changing the IP Address, Network Mask, or Gateway of an AHV Host on page 108.

    b. AHV host name.

       The hypervisor host name might change. This is expected and does not affect functionality. You can change it back to the preferred host name. For more information, see Renaming an AHV Host on page 39.

    c. CVM name

       The CVM name might change. This change is expected and does not affect cluster functionality. You can change it back to the preferred host name. For more information, see Changing the Name of the CVM Displayed in Prism on page 40.

    d. vRAM allocation for the CVM.

       Verify the vRAM allocation for the CVM and change it if needed.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1340

HOST NETWORK MANAGEMENT

Network management in an AHV cluster consists of the following tasks:

- Configuring Layer 2 switching through virtual switch and Open vSwitch bridges. When configuring virtual switch vSwitch, you configure bridges, bonds, and VLANs.
- Optionally changing the IP address, netmask, and default gateway that were specified for the hosts during the imaging process.

Flow Virtual Networking, enabled and managed in Prism Central instance that manages the AHV clusters, also provides networking support to the AHV clusters. Powered by the Network Controller and Network Gateway appliance, Flow Virtual Networking drives network virtualization to offer a seamless network experience with enhanced security. It is a software-defined network virtualization solution providing overlay capabilities for the on-premises AHV clusters. It integrates tools to deploy networking features like Virtual LANs, Virtual Private Cloud (VPC), Virtual Private Network (VPN), Layer 2 Virtual Network Extension using VPN or VTEP, Border Gateway Protocol sessions to support flexible app-driven networking that focuses on VMs and applications.

Network Controller

The Network Controller is defined as networking component of Prism Central that manages and controls configuration, monitoring and optimization of network resources for Flow Virtual Networking. It provides programmability, automation, and centralized control for configuring and managing network flows.

Network Controller is necessary to use centralized VLAN management, Flow Virtual Networking and .Flow Network Security 2.0.

Network Gateway

The Network Gateway appliance is deployed along with the Network Controller when you install or upgrade Prism Central. It is used to create VPN, VTEP, or BGP gateways to connect subnets using VPN connections, Layer 2 subnet extensions over VPN or VTEP, or over BGP sessions.

For more information about Flow Virtual Networking, see the Flow Virtual Networking Guide.

Network Types

AHV Networks

VLAN Basic Subnets (or Basic VLANs)

VLAN Basic Subnets, also known as Basic VLANs, refer to the AHV networking based VLANs that Acropolis creates while creating the AHV clusters (VLAN0 - default VLAN that is used to network the Controller VMs and AHV hosts) or the AHV networking based VLANs that you create to network the guest VMs using the **Network Configuration** page in Prism Element Web Console.

VLAN Basic Subnets (Virtual LANs or networks) supported by AHV are of two types:

Virtual Networks (Layer 2)

Each VM network interface is bound to a virtual network. Each virtual network is bound to a single VLAN; trunking VLANs to a virtual network is not supported. Networks are designated by the Layer 2 type (`vlan`) and the VLAN number.

By default, each virtual network maps to virtual switch such as the default virtual switch `vs0`. However, you can change this setting to map a virtual network to a custom virtual switch. The user is responsible for ensuring that the specified virtual switch exists on all hosts, and that the physical switch ports for the virtual switch uplinks are properly configured to receive VLAN-tagged traffic.

For more information about virtual switches, see About Virtual Switch on page 59.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1341

A VM NIC must be associated with a virtual network. You can change the virtual network of a vNIC without deleting and recreating the vNIC.

Managed Networks (Layer 3)

A virtual network can have an IPv4 configuration, but it is not required. A virtual network with an IPv4 configuration is a *managed network*; one without an IPv4 configuration is an *unmanaged network*. A VLAN can have at most one managed network defined. If a virtual network is managed, every NIC is assigned an IPv4 address at creation time.

A managed network can optionally have one or more non-overlapping DHCP pools. Each pool must be entirely contained within the network's managed subnet.

If the managed network has a DHCP pool, the NIC automatically gets assigned an IPv4 address from one of the pools at creation time, provided at least one address is available. Addresses in the DHCP pool are not reserved. That is, you can manually specify an address belonging to the pool when creating a virtual adapter. If the network has no DHCP pool, you must specify the IPv4 address manually.

All DHCP traffic on the network is rerouted to an internal DHCP server, which allocates IPv4 addresses. DHCP traffic on the virtual network (that is, between the guest VMs and the Controller VM) does not reach the physical network, and vice versa.

A network must be configured as managed or unmanaged when it is created. It is not possible to convert one to the other.

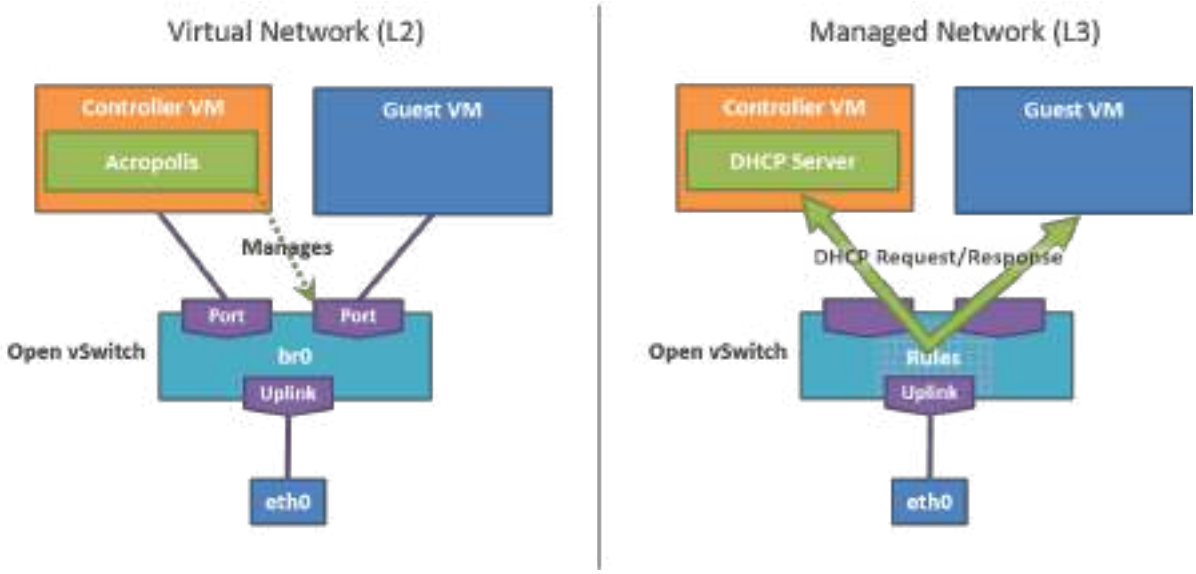


Figure 6: AHV Networking Architecture

Network Controller based Networks on Prism Central

Overlay Networks

You can create an IP-based Overlay subnet for a VPC. An Overlay network is a virtualized network that is configured on top of an underlying virtual or physical network. Examples of Overlay networks are:

- You can create a special purpose multicast network as an Overlay network within an existing network.
- A peer-to-peer network or a VPN.

An important assumption for an Overlay network is that the underlying network is fully connected. Nutanix provides the capability to create Overlay network-based VPCs.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1342

For more information, see *Overlay networks* in Essential Concepts.

VLAN Networks

Starting with Prism Central pc.2023.3 with AOS 6.7 and AHV 20230302.198, Network Controller 3.0.0 and later versions support the creation of VLANs (VLAN Subnets) on the Network Controller. The Network Controller also supports migration of VLAN Basic Subnets to VLAN Subnets subject to support and limitations information provided in the *VLAN Subnets Support* section.

VLAN Subnets (VLANs)

Create or manage the VLAN Subnets (VLANs) or Network Controller managed VLANs using the Network Controller on Prism Central. You can only create or manage these VLAN Subnets in Prism Central. You cannot use Prism Element Web Console to create or manage these VLAN Subnets.

> **Note:** Clusters with CO nodes do not support the creation of VLAN Subnets.

For more information on the features that VLAN Subnets support, see *VLAN Subnets Support* in the Flow Virtual Networking Guide.

vNIC Subnet Change

You cannot change the VLAN Subnet associated with the VM vNIC. Instead, delete the VM vNIC and create a new vNIC and associate this to the new VLAN Subnet.

You can change the VLAN Basic Subnet associated with the VM vNIC to another VLAN Basic subnet.

You cannot update the VLAN ID of a VLAN Subnet or a VLAN Basic Subnet.

Network Traffic Types

This section describes network traffic types in Nutanix clusters.

The network traffic is classified into the following types:

- East/West (Intra-VPC) traffic - Network traffic that is sent and received on the AHV host internal port br0 by default. The intra-VPC traffic is Geneve encapsulated and stays within the VPC. The intra-VPC traffic is also called East/West traffic because it is sent between nodes within the cluster.
- North/South (ingress/egress) traffic: Network traffic that enters or exits the VPC. The external subnet determines the virtual switch and VLAN for this traffic type

For information on configuring a virtual switch to route the network traffic of both types, see Configuring Virtual Switch for VPC Traffic Types.

Prerequisites for Configuring Networking

Change the configuration from the factory default to the recommended configuration. See AHV Networking Recommendations on page 48.

AHV Networking Recommendations

Nutanix recommends that you perform the following OVS configuration tasks from the Controller VM, as described in this documentation:

- Viewing the network configuration
- Configuring uplink bonds with desired interfaces using the Virtual Switch (VS) configurations.
- Assigning the Controller VM to a VLAN

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1343

For performing other network configuration tasks such as adding an interface to a bridge and configuring LACP for the interfaces in a bond, follow the procedures described in the AHV Networking best practices documentation.

Nutanix recommends that you configure the network as follows:

Table 5: Recommended Network Configuration

Network Component	Best Practice
Virtual Switch	Do not modify the OpenFlow tables of any bridges configured in any VS configurations in the AHV hosts. Do not rename default virtual switch vs0. You cannot delete the default virtual switch vs0. Do not delete or rename OVS bridge br0. Do not modify the native Linux bridge virbr0.
Switch Hops	Nutanix nodes send storage replication traffic to each other in a distributed fashion over the top-of-rack network. One Nutanix node can, therefore, send replication traffic to any other Nutanix node in the cluster. The network should provide low and predictable latency for this traffic. Ensure that there are no more than three switches between any two Nutanix nodes in the same cluster.
Switch Fabric	A switch fabric is a single leaf-spine topology or all switches connected to the same switch aggregation layer. The Nutanix VLAN shares a common broadcast domain within the fabric. Connect all Nutanix nodes that form a cluster to the same switch fabric. Do not stretch a single Nutanix cluster across multiple, disconnected switch fabrics. Every Nutanix node in a cluster should therefore be in the same L2 broadcast domain and share the same IP subnet.
WAN Links	A WAN (wide area network) or metro link connects different physical sites over a distance. As an extension of the switch fabric requirement, do not place Nutanix nodes in the same cluster if they are separated by a WAN.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1344

Network Component	Best Practice
VLANs	Add the Controller VM and the AHV host to the same VLAN. Place all CVMs and AHV hosts in a cluster in the same VLAN. VLANs can be tagged or untagged based on the VLAN ID used as per IEEE 802.1Q standard. When you assign the VLAN ID 0 to a VLAN, then it is a native or untagged VLAN. Assign a VLAN ID between 1-4094 to make it a tagged VLAN. By default the VLAN for CVM and AHV host is untagged, displayed as VLAN 0. This effectively places the CVM and AHV hosts on the native VLAN configured on the upstream physical switch. **Note:** Do not add any other device (including guest VMs) to the VLAN to which the CVM and hypervisor host are assigned. Isolate guest VMs on one or more separate VLANs. Nutanix recommends configuring the CVM and hypervisor host VLAN as the native, or untagged, VLAN on the connected switch ports. This native VLAN configuration allows for easy node addition and cluster expansion. By default, new Nutanix nodes send and receive untagged traffic. If you use a tagged VLAN for the CVM and hypervisor hosts instead, you must configure that VLAN while provisioning the new node, before adding that node to the Nutanix cluster. Use tagged VLANs for all guest VM traffic and add the required guest VM VLANs to all connected switch ports for hosts in the Nutanix cluster. Limit guest VLANs for guest VM traffic to the smallest number of physical switches and switch ports possible to reduce broadcast network traffic load. If a VLAN is no longer needed, remove it.
Default VS bonded port (br0-up)	Aggregate the fastest links of the same speed on the physical host to a VS bond on the default vs0 and provision VLAN trunking for these interfaces on the physical switch. By default, interfaces in the bond in the virtual switch operate in the recommended active-backup mode. **Note:** The mixing of bond modes across AHV hosts in the same cluster is not recommended and not supported.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1345

Network Component	Best Practice

1 GbE and 10 GbE interfaces (physical host)	Ensure you do not form a NIC combination or mix NICs in any of the following ways in the same bond:
	• NIC models from different vendors.
	• NICs operating at different speeds.
	• NICs with different drivers. To verify the NIC driver in use, run the following command on the AHV host for each NIC:
	`root@ahv# ethtool -i <nic-name>`
	In the above command, replace `<nic-name>` with the NIC name available at your site.
	If 10 GbE or faster uplinks are available, Nutanix recommends that you use them instead of 1 GbE uplinks.
	Recommendations for 1 GbE uplinks are as follows:
	• If you plan to use 1 GbE uplinks, do not include them in the same bond as the 10 GbE interfaces.
	• If you choose to configure only 1 GbE uplinks, when migration of memory-intensive VMs becomes necessary, power off and power on in a new host instead of using live migration. In this context, memory-intensive VMs are VMs whose memory changes at a rate that exceeds the bandwidth offered by the 1 GbE uplinks.
	Nutanix recommends the manual procedure for memory-intensive VMs because live migration, which you initiate either manually or by placing the host in maintenance mode, might appear prolonged or unresponsive and might eventually fail.
	Use the aCLI on any CVM in the cluster to start the VMs on another AHV host:
	`nutanix@cvm$ acli vm.on vm_list host=host`
	Replace `vm_list` with a comma-delimited list of VM names and replace `host` with the IP address or UUID of the target host.
	• If you must use only 1GbE uplinks, add them into a bond to increase bandwidth and use the balance-TCP (LACP) or balance-SLB bond mode.

IPMI port on the hypervisor host	Do not use VLAN trunking on switch ports that connect to the IPMI interface. Configure the switch ports as access ports for management simplicity.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1346

Network Component	Best Practice
Upstream physical switch	Nutanix does not recommend the use of Fabric Extenders (FEX) or similar technologies for production use cases. While initial, low-load implementations might run smoothly with such technologies, poor performance, VM lockups, and other issues might occur as implementations scale upward (see Knowledge Base article KB1612). Nutanix recommends the use of 10Gbps, line-rate, non-blocking switches with larger buffers for production workloads. Cut-through versus store-and-forward selection depends on network design. In designs with no oversubscription and no speed mismatches you can use low-latency cut-through switches. If you have any oversubscription or any speed mismatch in the network design, then use a switch with larger buffers. Port-to-port latency should be no higher than 2 microseconds. Use fast-convergence technologies (such as Cisco PortFast) on switch ports that are connected to the hypervisor host.
Physical Network Layout	Use redundant top-of-rack switches in a traditional leaf-spine architecture. This simple, flat network design is well suited for a highly distributed, shared-nothing compute and storage architecture. Add all the nodes that belong to a given cluster to the same Layer-2 network segment. Other network layouts are supported as long as all other Nutanix recommendations are followed.
Jumbo Frames	The Nutanix CVM uses the standard Ethernet MTU (maximum transmission unit) of 1,500 bytes for all the network interfaces by default. The standard 1,500 byte MTU delivers excellent performance and stability. Nutanix does not support configuring the MTU on network interfaces of a CVM to higher values. You can enable jumbo frames (MTU of 9,000 bytes) on the physical network interfaces of AHV hosts and guest VMs if the applications on your guest VMs require them. If you choose to use jumbo frames on hypervisor hosts, be sure to enable them end to end in the desired network and consider both the physical and virtual network infrastructure impacted by the change. If you try to configure, on the default virtual switch vs0, an MTU value that does not fall within the range of 1500 ~ 9000 bytes, Prism displays an error and fails to apply the configuration.
Controller VM	Do not remove the Controller VM from either the OVS bridge br0 or the native Linux bridge virbr0.
Rack Awareness and Block Awareness	Block awareness and rack awareness provide smart placement of Nutanix cluster services, metadata, and VM data to help maintain data availability, even when you lose an entire block or rack. The same network requirements for low latency and high throughput between servers in the same cluster still apply when using block and rack awareness. **Note:** Do not use features like block or rack awareness to stretch a Nutanix cluster between different physical sites.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1347

Network Component	Best Practice
Oversubscription	Oversubscription occurs when an intermediate network device or link does not have enough capacity to allow line rate communication between the systems connected to it. For example, if a 10 Gbps link connects two switches and four hosts connect to each switch at 10 Gbps, the connecting link is oversubscribed. Oversubscription is often expressed as a ratio—in this case 4:1, as the environment could potentially attempt to transmit 40 Gbps between the switches with only 10 Gbps available. Achieving a ratio of 1:1 is not always feasible. However, you should keep the ratio as small as possible based on budget and available capacity. If there is any oversubscription, choose a switch with larger buffers. In a typical deployment where Nutanix nodes connect to redundant top-of-rack switches, storage replication traffic between CVMs traverses multiple devices. To avoid packet loss due to link oversubscription, ensure that the switch uplinks consist of multiple interfaces operating at a faster speed than the Nutanix host interfaces. For example, for nodes connected at 10 Gbps, the inter-switch connection should consist of multiple 10 Gbps or 40 Gbps links.

The virtual switch aggregates the same bridges on all nodes in the cluster. The bridge (for example, br1) connects to the physical port such as eth3 (Ethernet port) through the corresponding uplink (for example, br1-up). The uplink ports of the bridges are connected to the same physical network. For example, vs0 is mapped to the br0 bridge, in turn connected through uplink br0-up to various (physical) Ethernet ports on different nodes.

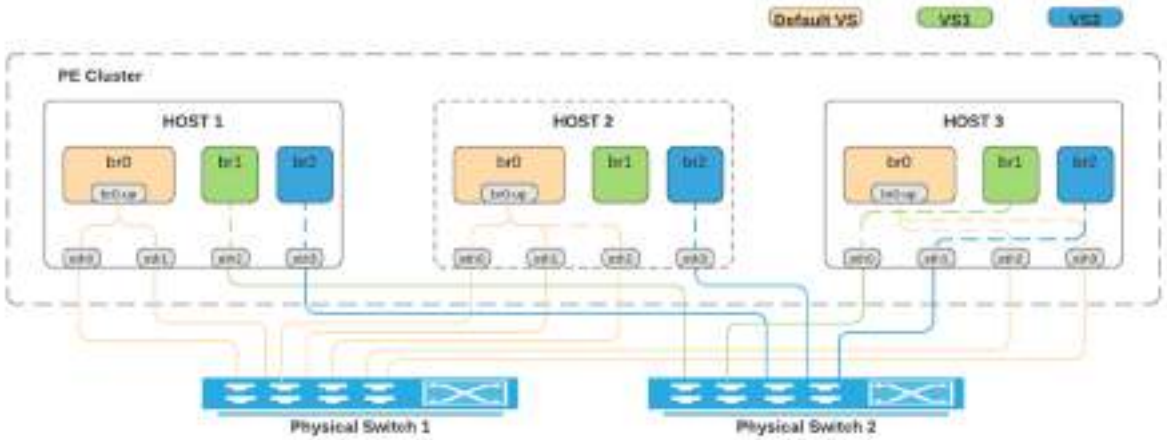


Figure 7: Virtual Switch

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1348

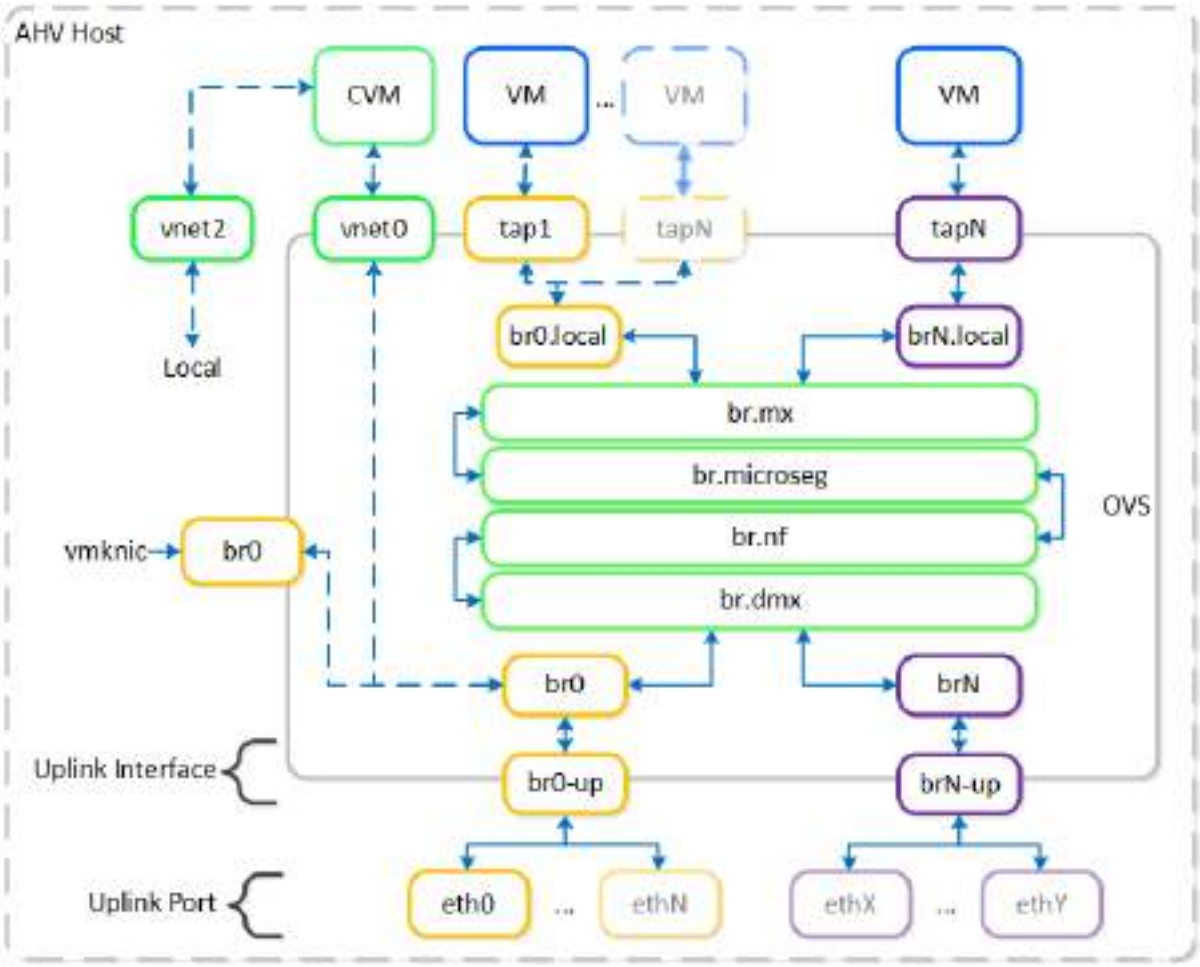


Figure 8: AHV Bridge Chain

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1349

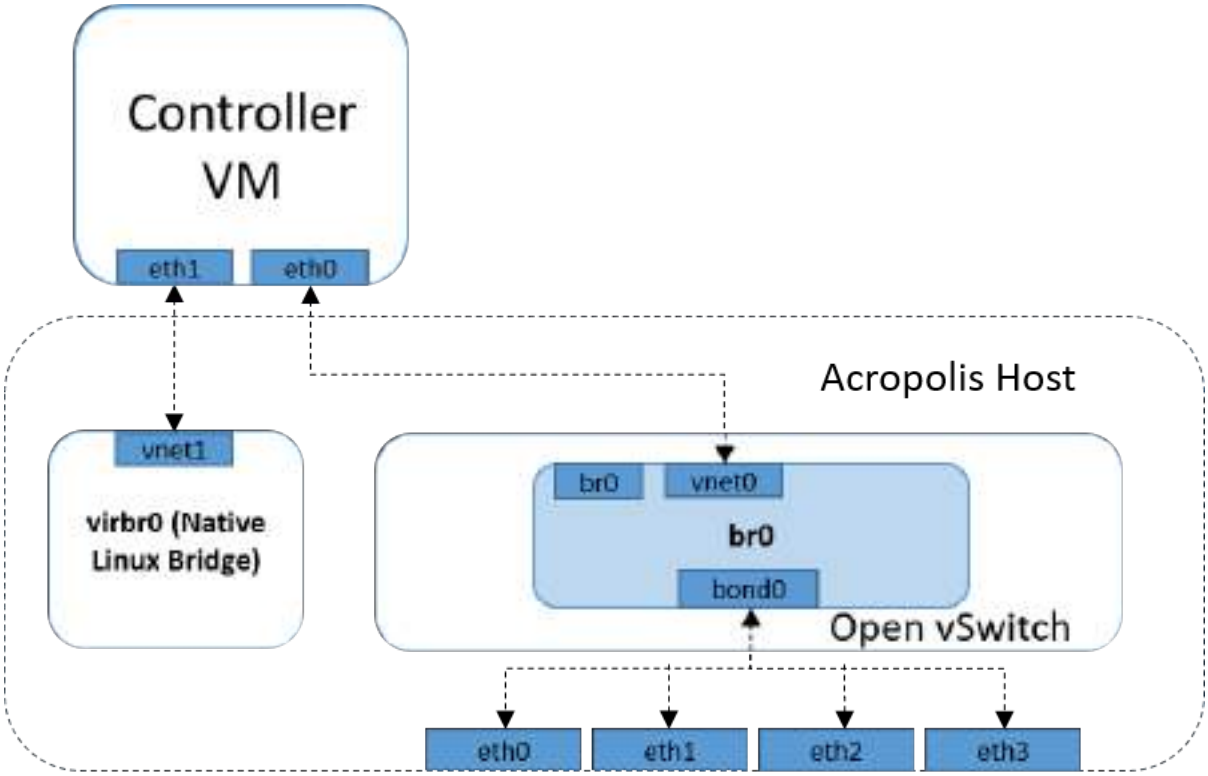


Figure 9: Default factory configuration of Open vSwitch in AHV

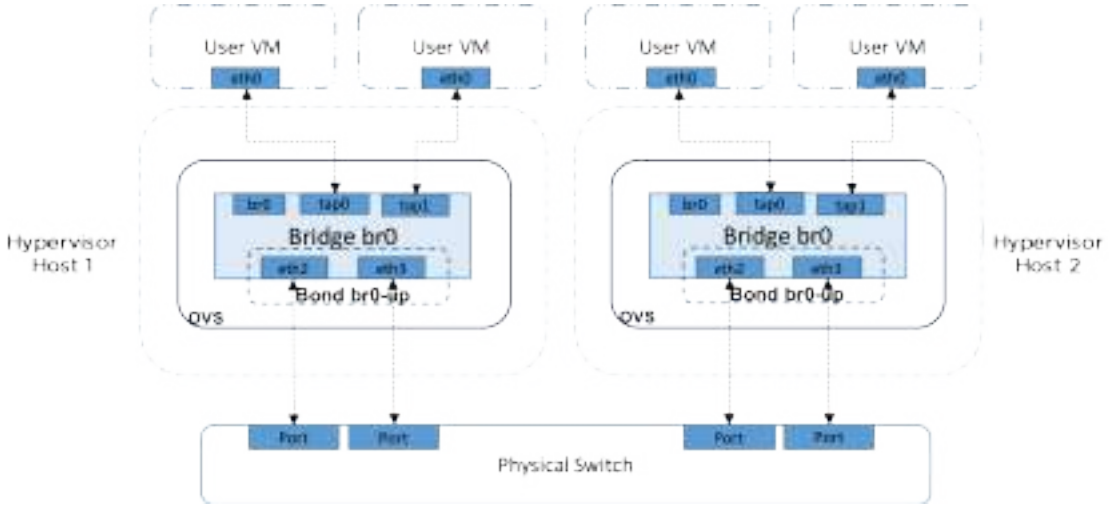


Figure 10: Open vSwitch Configuration

IP Address Management

IP Address Management (IPAM) is a feature of AHV that allows it to assign IP addresses automatically to VMs by using DHCP. You can configure each virtual network with a specific IP address subnet, associated domain settings, and IP address pools available for assignment to VMs.

An AHV network is defined as a managed network or an unmanaged network based on the IPAM setting.

Managed Network

Managed network refers to an AHV network in which IPAM is enabled.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1350

Unmanaged Network

Unmanaged network refers to an AHV network in which IPAM is not enabled or is disabled.

To enable IPAM, you can select the **Enable IP Address Management** checkbox in the **Create Subnet** window, when you create a virtual network for the guest VMs. For more information, see Configuring a Virtual Network for Guest VM Interfaces in the *Prism Element Web Console Guide*.

> **Note:** You can enable IPAM only when you are creating a virtual network. You cannot enable or disable IPAM for an existing virtual network.

IPAM enabled or disabled status has implications. For example, when you want to reconfigure the IP address of a Prism Central VM, the procedure to do so may involve additional steps for managed networks (that is, networks with IPAM enabled) where the new IP address belongs to an IP address range different from the previous IP address range. See Reconfiguring the IP Address and Gateway of Prism Central VMs in *Prism Central Infrastructure Guide*.

Traffic Marking for Quality of Service

To prioritize outgoing (or egress) traffic as required, you can configure quality of service on the traffic for a cluster.

There are two distinct types of outgoing or egress traffic:

- Management traffic (mgmt)
- Data services (data-svc)

Data services traffic consists of the following protocols:

Table 6: Data Services Protocols

Protocol	Port	Nutanix Services
NFS	Source ports (TCP): 445, 2049, 20048, 20049, 20050, and 7508. Source ports (UDP): 2049, 20048, 20049, 20050, and 7508. Source and Destination ports (TCP for Replicator-dr): 7515.	-Nutanix Files-
SMB	Source ports (TCP): 445, 2049, 20048, 20049, 20050, and 7508. Source ports (UDP): 2049, 20048, 20049, 20050, and 7508. Source and Destination ports (TCP for Replicator-dr): 7515.	-Nutanix Files-
Cluster-to-cluster replications (external or inter-site)	Destination Ports: 2009 and 2020 on CVM.	Stargate and Cerebro
Node-to-node replications (internal or intra-site)	Destination Ports: 2009 and 2020 on CVM.	Stargate and Cerebro

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1351

Protocol	Port	Nutanix Services
iSCSI	Source Ports: 3260,3261,3205 on CVM. Destination Ports: 3260,3261,3205 on AHV.	Nutanix Files and Volumes

Traffic other than data services traffic is management traffic. Traffic marking for QoS is disabled by default.

When you enable QoS, you can mark both the types of traffic with QoS values. AOS considers the values in hexadecimal even if you provide the values in decimal. When you view or get the QoS configuration enabled on the cluster, nCLI provides the QoS values in hexadecimal format (0xXX where XX is hexadecimal value in the range 00–3f).

> **Note:** Set any QoS value in the range 0x0–0x3f. The default QoS values for the traffic are as follows:
>
> - Management traffic (mgmt) = 0x10
> - Data services (data-svc) = 0xa

Configuring Traffic Marking for QoS

Configure Quality of Service (QoS) for management and data services traffic using nCLI.

About this task

To perform the following operations for QoS on the egress traffic of a cluster, use the nCLI commands in this section:

- Enable traffic marking for QoS on the cluster. QoS traffic marking is disabled by default.
- View or get the QoS configuration enabled on the cluster.
- Set QoS values for all traffic types or specific traffic types.
- Disable QoS on the cluster.

When you run any of the QoS configuration commands and the command succeeds, the console displays the following output indicating the successful command run:

```
QoSUpdateStatusDTO(status=true, message=null)
```

Where:

- status=true indicates that the command succeeded.
- message=null indicates that there is no error.

When you run any of the QoS configuration commands and the command fails, the console displays the following sample output indicating the failure:

```
QoSUpdateStatusDTO(status=false, message=QoS is already enabled.)
```

Where:

- status=false indicates that the command failed.
- message=QoS is already enabled. indicates why the command failed. This sample error message indicates that the `net enable-qos` command failed because QoS enable command was run again when QoS is already enabled.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1352

Procedure

- To enable QoS on a cluster, run the following command:

```
ncli> net enable-qos [data-svc="data-svc value"][mgmt="mgmt value"]
```

If you run the command as `net enable-qos` without the options, AOS enables QoS with the default values (mgmt=0x10 and data-svc=0xa).

> **Note:** After you run the `net enable-qos` command, if you run it again, the command fails and AOS displays the following output:
>
> `QoSUpdateStatusDTO(status=false, message=QoS is already enabled.)`

> **Note:** If you need to change the QoS values after you enable it , run the `net edit-qos` command with the option (`data-svc` or `mgmt` or both as necessary).

> **Note:** Set any QoS value in the range 0x0–0x3f.

- To view or get the QoS configuration enabled on a cluster, run the following command:

```
ncli> net get-qos
```

> **Note:** When you get the QoS configuration enabled on the cluster, nCLI provides the QoS values in hexadecimal format (0xXX where XX is hexadecimal value in the range 00–3f).

A sample output on the console is as follows:

```
QoSDTO(status=true, isEnabled=true, mgmt=0x10, dataSvc=0xa, message=null)
```

> **Note:**
>
> Where:
>
> - status=true indicates that the `net get-qos` command passed. status=false indicates that the `net get-qos` command failed. See the message= value for the failure error message.
> - isEnabled=true indicates that QoS is enabled. isEnabled=false indicates that QoS is not enabled.
> - mgmt=0x10 indicates that QoS value for Management traffic (*`mgmt`* option) is set to 0x10 (represented in hexadecimal value as 0x10. If you disabled QoS, then this parameter is displayed as mgmt=null.
> - dataSvc=0xa indicates that QoS value for data services traffic (*`data-svc`* option) is set to 0xa (represented in hexadecimal value as 0xa. If you disabled QoS, then this parameter is displayed as dataSvc=null.
> - message=null indicates there is no error message. message= parameter provides the command failure error message if the command fails.

- To set the QoS values for the traffic types on a cluster after you enabled QoS on the cluster, run the following command:

```
ncli> net edit-qos [data-svc="data-svc value"][mgmt="mgmt value"]
```

You can provide QoS values between 0x0-0x3f for one or both the options. The value is hexadecimal representation of a value between decimal 0-63 both inclusive.

- To disable QoS on a cluster, run the following command:

```
ncli> net disable-qos
```

```
QoSDTO(status=true, isEnabled=false, mgmt=null, dataSvc=null, message=null)
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1353

Layer 2 Network Management

AHV uses virtual switch (VS) to connect the Controller VM, the hypervisor, and the guest VMs to each other and to the physical network. Virtual switch is configured by default on each AHV node and the VS services start automatically when you start a node.

To configure virtual networking in an AHV cluster, you need to be familiar with virtual switch. This documentation gives you a brief overview of virtual switch and the networking components that you need to configure to enable the hypervisor, Controller VM, and guest VMs to connect to each other and to the physical network.

About Virtual Switch

Virtual switches or VS are used to manage multiple bridges and uplinks.

The VS configuration is designed to provide flexibility in configuring virtual bridge connections. A virtual switch (VS) defines a collection of AHV nodes and the uplink ports on each node. It is an aggregation of the same OVS bridge on all the compute nodes in a cluster. For example, vs0 is the default virtual switch is an aggregation of the br0 bridge and br0-up uplinks of all the nodes.

After you configure a VS, you can use the VS as reference for physical network management instead of using the bridge names as reference.

For overview on Virtual Switch, see Virtual Switch Considerations on page 62.

For information on OVS, see About Open vSwitch on page 66.

Virtual Switch Workflow

A virtual switch (VS) defines a collection of AHV compute nodes and the uplink ports on each node. It is an aggregation of the same OVS bridge on all the compute nodes in a cluster. For example, vs0 is the default virtual switch is an aggregation of the br0 bridge of all the nodes.

The system creates the default virtual switch vs0 connecting the default bridge br0 on all the hosts in the cluster during installation of or upgrade to the compatible versions of AOS and AHV. Default virtual switch vs0 has the following characteristics:

- The default virtual switch cannot be deleted.
- The default bridges br0 on all the nodes in the cluster map to vs0. Thus, vs0 is not empty. It has at least one uplink configured.
- The default management connectivity to a node is mapped to default bridge br0 that is mapped to vs0.
- The default virtual switch is configured with the **Active-Backup** uplink bond type.

  For more information about bond types, see the Bond Type table.
- The default parameter values of vs0 being **Name**, **Description**, **MTU** and **Bond Type** can be modified subject to aforesaid characteristics.

The virtual switch aggregates the same bridges on all nodes in the cluster. The bridge (for example, br1) connects to the physical port such as eth3 (Ethernet port) through the corresponding uplink (for example, br1-up). The uplink ports of the bridges are connected to the same physical network. For example, vs0 is mapped to the br0 bridge, in turn connected via uplink br0-up to various (physical) Ethernet ports on different nodes.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1354

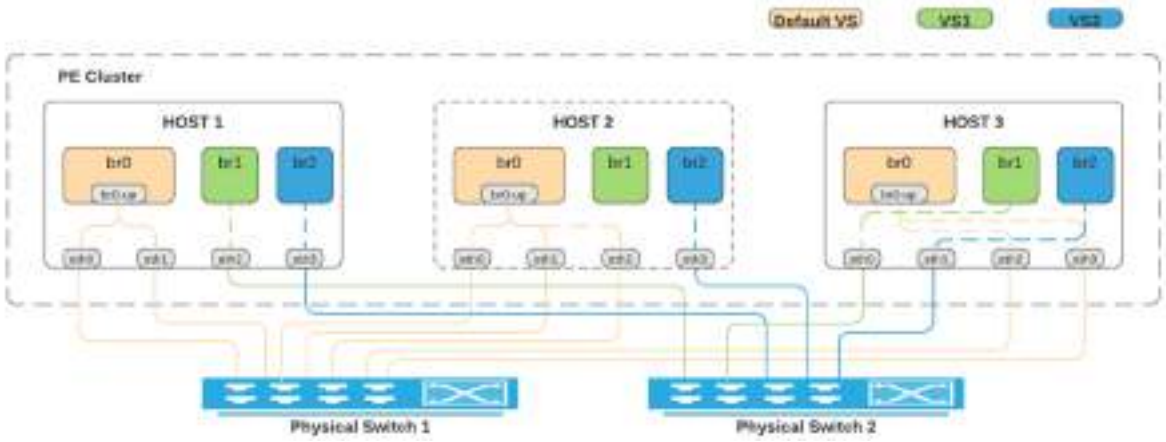


Figure 11: Virtual Switch

Uplink configuration uses bonds to improve traffic management. The bond types are defined for the aggregated OVS bridges. A new bond type - No uplink bond - provides a no-bonding option. A virtual switch configured with the No uplink bond uplink bond type has 0 or 1 uplinks.

When you configure a virtual switch with any other bond type, you must select at least two uplink ports on every node.

If you change the uplink configuration of vs0, AOS applies the updated settings to the hosts in the cluster one after the other (the rolling update process).

> **Important:** When you select the **Standard** method, only the hosts that have been updated with virtual switch configurations are restarted.

When you select the **Standard** configuration method to update the virtual switch configurations in a cluster, AOS performs the tasks:

1. Puts the node in maintenance mode (migrates VMs out of the node)
2. Applies the updated settings
3. Checks connectivity with the default gateway
4. Exits maintenance mode
5. Proceeds to apply the updated settings to the next node

> **Note:**
>
> Do not create, update or delete any virtual switch when the AOS or AHV upgrade process is running.

Table 7: Bond Types

Bond Type	Use Case	Maximum VM NIC Throughput	Maximum Host Throughput
Active-Backup	Recommended. Default configuration, which transmits all traffic over a single active adapter.	10 GB	10 GB

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1355

Bond Type	Use Case	Maximum VM NIC Throughput	Maximum Host Throughput
Active-Active with MAC pinning Also known as balance-slb	Works with caveats for multicast traffic. Increases host bandwidth utilization beyond a single 10 GB adapter. Places each VM NIC on a single adapter at a time. Do not use this bond type with link aggregation protocols such as LACP.	10 GB	20 GB
Active-Active Also known as LACP with balance-tcp	LACP and link aggregation required. Increases host and VM bandwidth utilization beyond a single 10 GB adapter by balancing VM NIC TCP and UDP sessions among adapters. Also used when network switches require LACP negotiation. The default LACP settings are: • Speed—Fast (1s) • Mode—Active fallback-active-backup • Priority—Default. This is not configurable.	20 GB	20 GB
No Uplink Bond	No uplink or a single uplink on each host. Virtual switch configured with the No uplink bond uplink bond type has 0 or 1 uplinks. When you configure a virtual switch with any other bond type, you must select at least two uplink ports on every node.	-	-

Note the following points about the uplink configuration.

- Virtual switches are not enabled in a cluster that has one or more compute-only nodes. See Virtual Switch Limitations on page 68 and Virtual Switch Requirements on page 67.
- If you select the **Active-Active** policy, you must manually enable LAG and LACP on the corresponding ToR switch for each node in the cluster.
- If you reimage a cluster with the **Active-Active** policy enabled, the default virtual switch (vs0) on the reimaged cluster is once again the **Active-Backup** policy. The other virtual switches are removed during reimage.
- Nutanix recommends configuring LACP with fallback to active-backup or individual mode on the ToR switches. The configuration and behavior varies based on the switch vendor. Use a switch configuration that allows both switch interfaces to pass traffic after LACP negotiation fails.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1356

Virtual Switch Considerations

Virtual Switch Deployment

A virtual switch configuration or configuration change is deployed using rolling update of the clusters. After the virtual switch configuration (creation or update) is received and execution starts, the hosts are first put into maintenance mode before the virtual switch configuration is made or modified on the node. This is called the **Standard** method of configuring a virtual switch.

> **Important:** When you select the **Standard** method, only the hosts that have been updated with virtual switch configurations are restarted.

> **Note:** If you are modifying an existing bond, AHV removes the bond and then re-creates the bond with the specified interfaces.
>
> Ensure that the interfaces you want to include in the bond are physically connected to the Nutanix appliance before you run the command described in this topic. If the interfaces are not physically connected to the Nutanix appliance, the interfaces are not added to the bond.
>
> Ensure that the pre-checks listed in *LCM Prechecks* section of the Life Cycle Manager Guide and the *Always* and *Host Disruptive Upgrades* types of pre-checks listed KB-4409 pass for Virtual Switch deployments.

The VS configuration is stored and re-enforced at system reboot.

The VM NIC configuration also displays the VS details. When you **Update VM** configuration or **Create NIC** for a VM, the NIC details show the virtual switches that can be associated. This view allows you to change a virtual network and the associated virtual switch.

To change the virtual network, select the virtual network in the **Subnet Name** dropdown list in the **Create NIC** or **Update NIC** dialog box.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1357

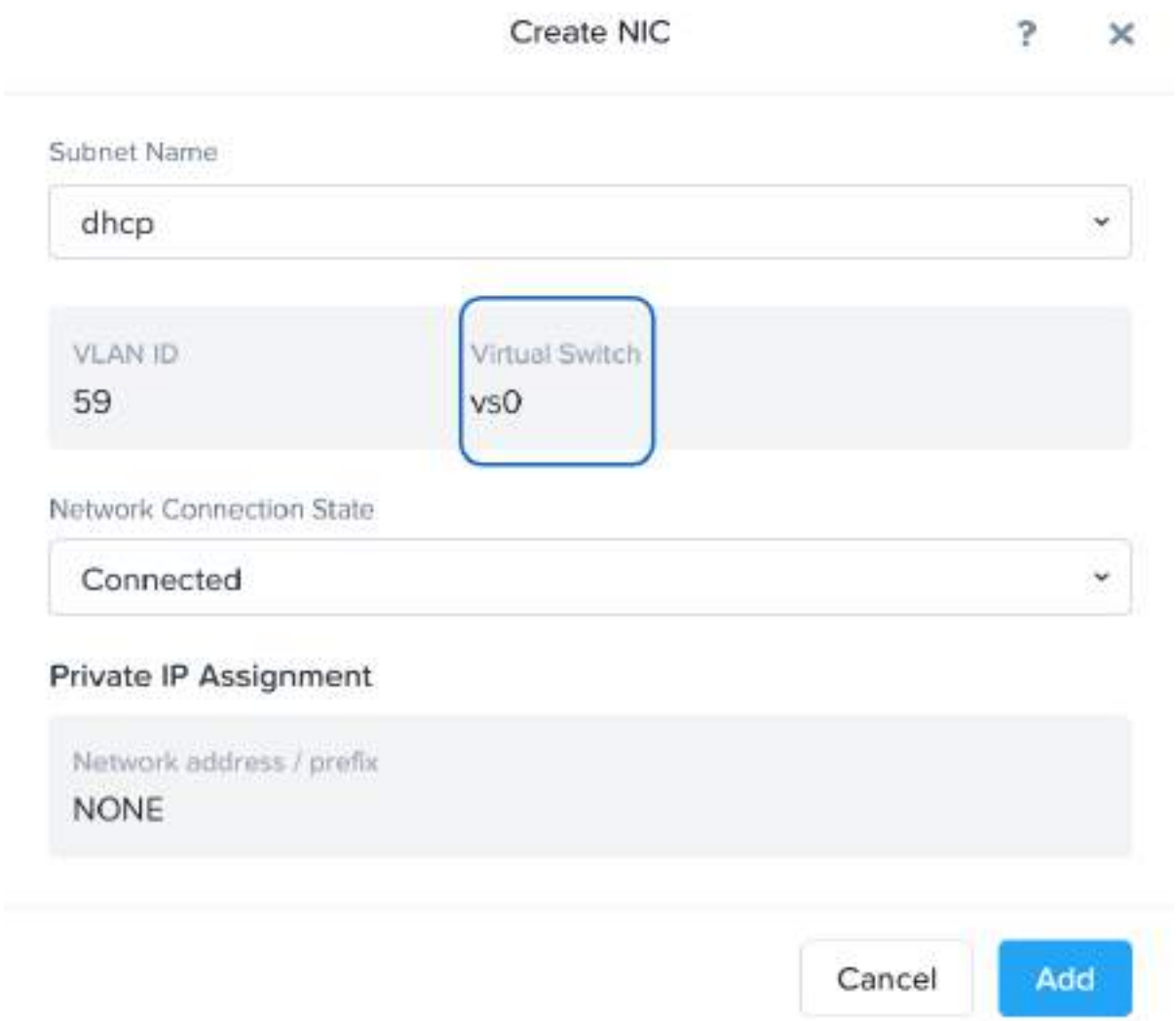


Figure 12: Create NIC - Virtual Switch Details

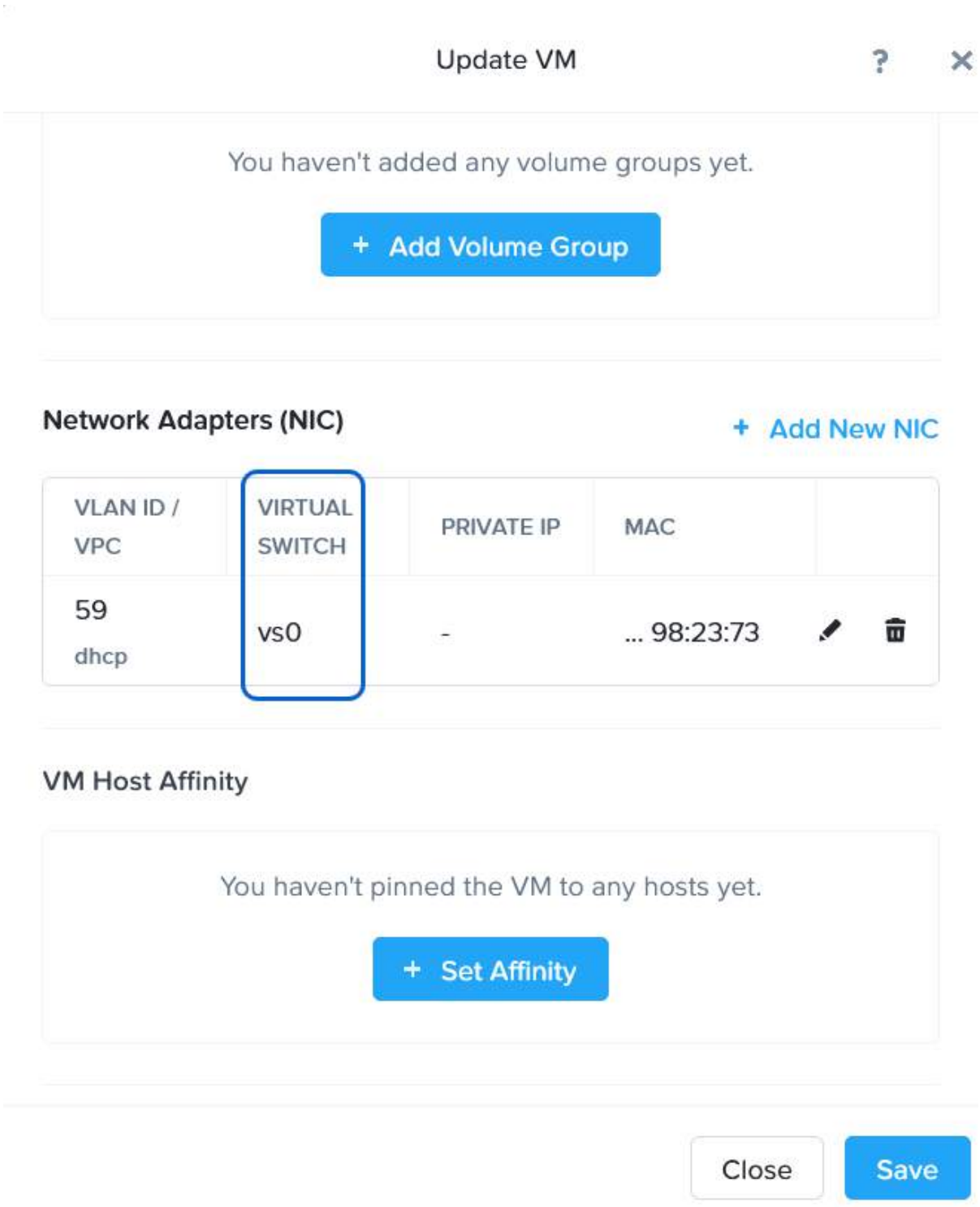


Figure 13: Update VM - Virtual Switch Details

Impact of Installation or Upgrade to Compatible AOS and AHV Versions

For information on minimum and compatible AOS and AHV versions, see Virtual Switch Requirements on page 67.

When you upgrade the AOS to a compatible version from an older version, the upgrade process:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1359

- Triggers the creation of the default virtual switch vs0, which is mapped to bridge br0on all the nodes.
- Validates bridge br0 and its uplinks for consistency in terms of MTU and bond-type on every node.

  If valid, it adds the bridge br0 of each node to the virtual switch vs0.

  If br0 configuration is not consistent, the system generates an NCC alert which provides the failure reason and necessary details about it.

  The system migrates only the bridge br0 on each node to the default virtual switch vs0 because the connectivity of bridge br0 is guaranteed.
- Does not migrate any other bridges to any other virtual switches during upgrade. You need to manually migrate the other bridges after install or upgrade is complete.

  Note:

  Do not create, update or delete any virtual switch when the AOS or AHV upgrade process is running.

Bridge Migration

After upgrading to a compatible version of AOS, you can migrate bridges other than br0 that existed on the nodes. When you migrate the bridges, the system converts the bridges to virtual switches.

For more information, see *Virtual Switch Migration Requirements* in Virtual Switch Requirements on page 67.

Note: You can migrate only those bridges that are present on every compute node in the cluster. For more information, see Migrating Bridges after Upgrade in *Prism Element Web Console Guide*.

Cluster Scaling Impact

VS management for cluster scaling (addition or removal of nodes) is seamless.

Node Removal

When you remove a node, the system detects the removal and automatically removes the node from all the VS configurations that include the node and generates an internal system update. For example, a node has two virtual switches, vs1 and vs2, configured apart from the default vs0. When you remove the node from the cluster, the system removes the node for the vs1 and vs2 configurations automatically with internal system update.

Node Addition

When you add a new node or host to a cluster, the bridges or virtual switches on the new node are treated in the following manner:

Note: If a host already included in a cluster is removed and then added back, it is treated as a new host.

- The system validates the default bridge br0 and uplink bond br0-up to check if it conforms to the default virtual switch vs0 already present on the cluster.

  If br0 and br0-up conform, the system includes the new host and its uplinks in vs0.

  If br0 and br0-up do not conform,then the system generates an NCC alert.
- The system does not automatically add any other bridge configured on the new host to any other virtual switch in the cluster.

  It generates NCC alerts for all the other non-default virtual switches.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1360

- You can manually include the host in the required non-default virtual switches. Update a non-default virtual switch to include the host.

  For information on updating a virtual switch in Prism Element Web Console, see Configuring a Virtual Network for Guest VM Interfaces in the *Prism Element Web Console Guide*.

  For information on updating a virtual switch in Prism Central, see Network Connections in the *Prism Central Infrastructure Guide*.

VS Management

You can manage virtual switches from Prism Central or Prism Web Console. You can also use aCLI or REST APIs to manage them. For more information, see the Acropolis API Reference and Command Reference guides.

You can also use the appropriate aCLI commands for virtual switches from the following list:

- net.create_virtual_switch
- net.list_virtual_switch
- net.get_virtual_switch
- net.update_virtual_switch
- net.delete_virtual_switch
- net.migrate_br_to_virtual_switch
- net.disable_virtual_switch

About Open vSwitch

Open vSwitch (OVS) is an open-source software switch implemented in the Linux kernel and designed to work in a multiserver virtualization environment. By default, OVS behaves like a Layer 2 learning switch that maintains a MAC address learning table. The hypervisor host and VMs connect to virtual ports on the switch.

Each hypervisor hosts an OVS instance, and all OVS instances combine to form a single switch.

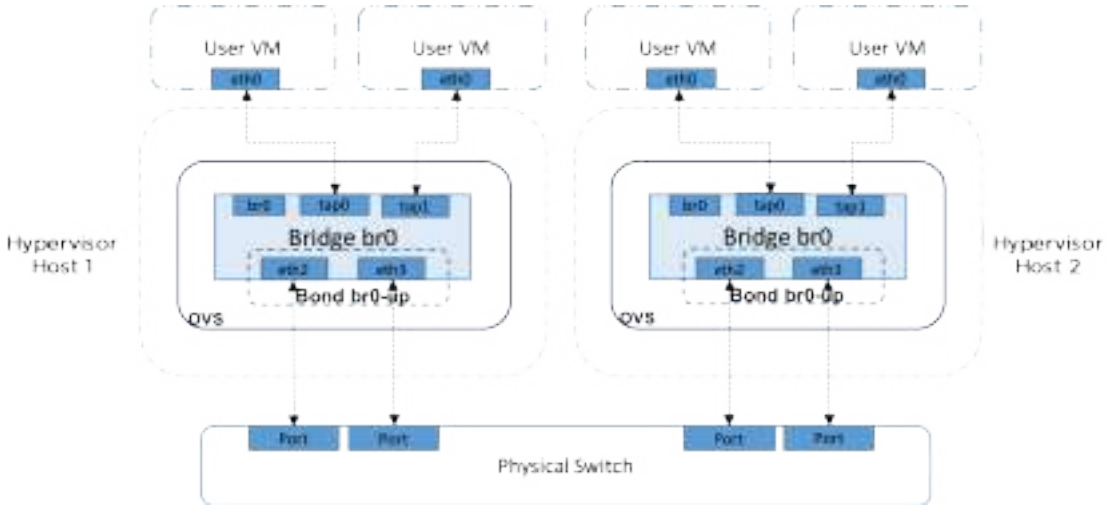


Figure 14: Open vSwitch

Default Factory Configuration

The factory configuration of an AHV host includes a default OVS bridge named br0 (configured with the default virtual switch vs0) and a native Linux bridge called virbr0.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1361

Bridge br0 includes the following ports by default:

- An internal port with the same name as the default bridge; that is, an internal port named br0. This is the access port for the hypervisor host.
- A bonded port named br0-up. The bonded port aggregates all the physical interfaces available on the node. For example, if the node has two 10 GbE interfaces and two 1 GbE interfaces, all four interfaces are aggregated on br0-up. This configuration is necessary for Foundation to successfully image the node regardless of which interfaces are connected to the network.

> **Note:**
>
> Before you begin configuring a virtual network on a node, you must disassociate the 1 GbE interfaces from the br0-up port. This disassociation occurs when you modify the default virtual switch (vs0) and create new virtual switches. Nutanix recommends that you aggregate only the 10 GbE or faster interfaces on br0-up and use the 1 GbE interfaces on a separate OVS bridge deployed in a separate virtual switch.
>
> For information on virtual switch management, see Virtual Switch Management on page 69.

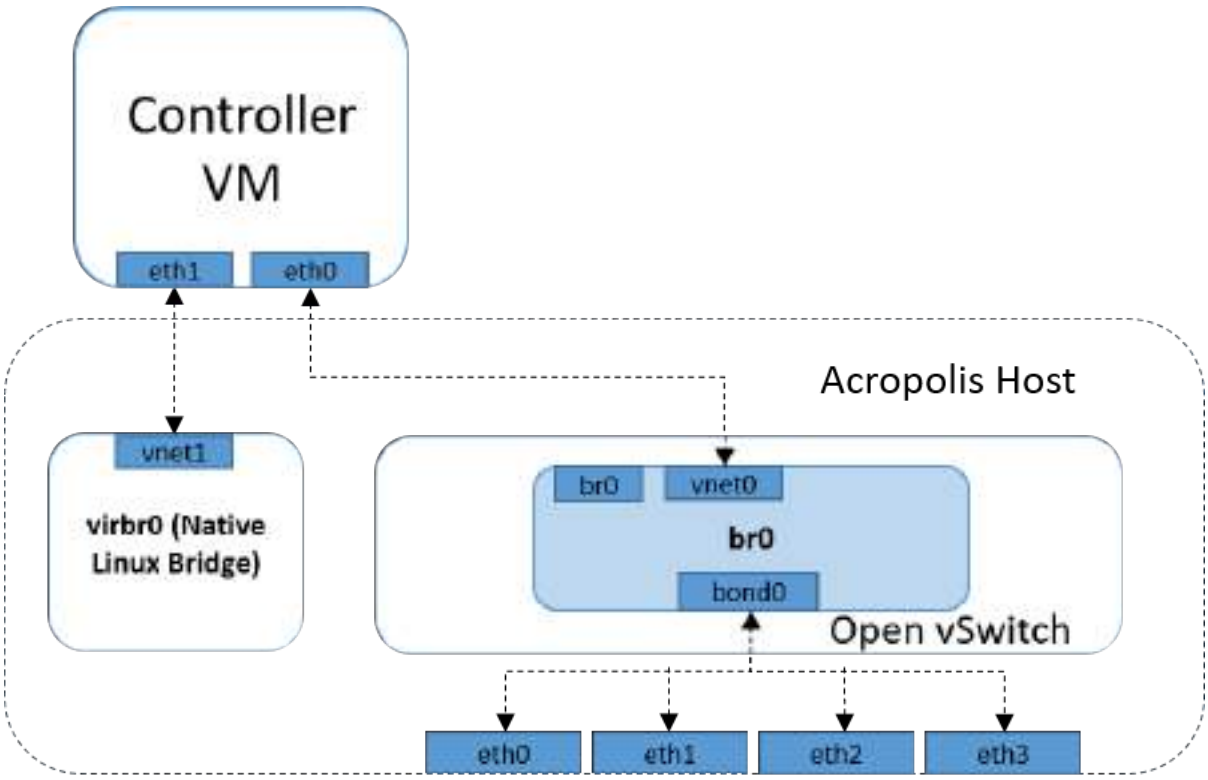


Figure 15: Default factory configuration of Open vSwitch in AHV

The Controller VM has two network interfaces by default. One network interface connects to bridge br0. The other network interface connects to a port on virbr0. The Controller VM uses this bridge to communicate with the hypervisor host.

Virtual Switch Requirements

The requirements to deploy virtual switches are as follows:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1362

- Virtual switches are supported on AOS 5.19 or later with AHV 20201105.12 or later. Therefore you must install or upgrade to AOS 5.19 or later, with AHV 20201105.12 or later, to use virtual switches in your deployments.
- Virtual bridges used for a VS on all the nodes must have the same specification such as name, MTU and uplink bond type. For example, if vs1 is mapped to br1 (virtual or OVS bridge 1) on a node, it must be mapped to br1 on all the other nodes of the same cluster.

Virtual Switch Migration Requirements

The AOS upgrade process initiates the virtual switch migration. The virtual switch migration is successful only when you meet the following requirements:

- Before migrating to Virtual Switch,
  - All bridge br0 bond interfaces should have the same bond type on all hosts in the cluster. For example, all hosts should use the *Active-backup* bond type or *balance-tcp*. If some hosts use *Active-backup* and other hosts use *balance-tcp*, virtual switch migration fails.
  - If using LACP, confirm that the LACP speed on the physical switch is set to fast or 1 second. Also ensure that the switch ports are ready to fallback to individual mode if LACP negotiation fails due to a configuration such as `no lacp suspend-individual`.
  - Confirm that the upstream physical switch is set to spanning-tree portfast or spanning-tree port type edge trunk. Failure to do so might lead to a 30-second network timeout and the virtual switch migration might fail because it uses 20-second non-modifiable timer.
- Ensure that the pre-checks listed in *LCM Prechecks* section of the Life Cycle Manager Guide and the *Always* and *Host Disruptive Upgrades* types of pre-checks listed KB-4409 pass for Virtual Switch deployments.
- For the default virtual switch vs0,
  - All configured uplink ports must be available for connecting the network. In Active-Backup bond type, the active port is selected from any configured uplink port that is linked. Therefore, the virtual switch vs0 can use all the linked ports for communication with other CVMs/hosts.
  - All the host IP addresses in the virtual switch vs0 must be resolvable to the configured gateway using ARP.

Virtual Switch Limitations

Virtual Switch Operations During Upgrade

Do not create, update or delete any virtual switch when the AOS or AHV upgrade process is running.

MTU Restriction

The Nutanix Controller VM uses the standard Ethernet MTU (maximum transmission unit) of 1,500 bytes for all the network interfaces by default. The standard 1,500-byte MTU delivers excellent performance and stability. Nutanix does not support configuring higher values of MTU on the network interfaces of a Controller VM.

You can enable jumbo frames (MTU of 9,000 bytes) on the physical network interfaces of AHV, ESXi, or Hyper-V hosts and guest VMs if the applications on your guest VMs require such higher MTU values. If you choose to use jumbo frames on the hypervisor hosts, enable the jumbo frames end to end in the specified network, considering both the physical and virtual network infrastructure impacted by the change.

If you try to configure, on the default virtual switch vs0, an MTU value that does not fall within the range of 1500 ~ 9000 bytes, Prism displays an error and fails to apply the configuration.

Single node and Two-node cluster configuration.

Virtual switch cannot be deployed is your single-node or two-node cluster has any instantiated user VMs. The virtual switch creation or update process involves a rolling restart, which checks for maintenance mode and

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1363

whether you can migrate the VMs. On a single-node or two-node cluster, any instantiated user VMs cannot be migrated and the virtual switch operation fails.

Therefore, power down all user VMs for virtual switch operations in a single-node or two-node cluster.

Including a storage-only node in a VS is not necessary.

Virtual switch is compatible with Storage-only (SO) nodes but you need not manually include an SO node in any virtual switch, including the default virtual switch.

Mixed-mode Clusters with AHV Storage-only Nodes

Consider that you have deployed a mixed-node cluster where the compute-only nodes are ESXi or Hyper-V nodes and the storage-only nodes are AHV nodes. In such a case, the default virtual switch deployment includes the storage-only nodes in the default virtual switch.

Virtual Switch Management

Virtual Switch can be viewed, created, updated or deleted from both Prism Web Console as well as Prism Central.

Virtual Switch Views and Visualization

For information on the virtual switch network visualization in Prism Element Web Console, see the Network Visualization topic in the *Prism Web Console Guide*.

Virtual Switch Create, Update and Delete Operations

For information on the procedures to create, update and delete a virtual switch in Prism Element Web Console, see the Configuring a Virtual Network for Guest VM Interfaces information in the *Prism Element Web Console Guide*.

For information on the procedures to create, update and delete a virtual switch in Prism Central, see the Network Connections information in the *Prism Central Infrastructure Guide*.

> **Note:**
>
> Do not create, update or delete any virtual switch when the AOS or AHV upgrade process is running.

Uplinks for Virtual Private Cloud Traffic

Starting with a minimum AOS version 6.1.1 with Prism Central version pc.2022.4 and Flow networking controller version 2.1.1, you can use virtual switches to separate traffic of the guest VMs that are networked using Flow Networking Virtual Private Cloud (VPC) configurations.

AHV uses the default virtual switch for the management and other Controller VM traffic (unless if you have configured network segmentation to route the Controller VM traffic on another virtual switch). When you enable Flow networking in a cluster, Prism Central with the Flow networking controller and network gateway allows you to deploy Virtual Private Clouds (VPCs) that network guest VMs on hosts within the cluster and on other clusters. By default, AHV uses the default virtual switch vs0 for the VPC (Flow networking) traffic as well.

You can configure AHV to route the VPC (Flow networking) traffic on a different virtual switch, other than the default virtual switch.

Conditions for VPC Uplinks

Certain conditions apply to the use of virtual switches to separate the Controller VM traffic and traffic of the guest VMs that are networked using Virtual Private Cloud (VPC) configurations.

Host IP Addresses in Virtual Switch

The virtual switch selected for Flow networking VPC traffic must have IP addresses configured on the hosts. If the selected virtual switch does not have IP addresses configured on the hosts, then the following error is displayed:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1364

Bridge interface IP address is not configured for host: <host-UUID> on virtual_switch <name-of-selected-virtual-switch>

Configure IP addresses from this subnet on the hosts in the virtual switch.

> **Note:**
>
> Do not create, update or delete any virtual switch when the AOS or AHV upgrade process is running.

Requirements

Ensure that the default virtual switch vs0 is enabled.

The following conditions apply to the IP addresses that you configure:

- Ensure that the host IP addresses in the subnet do not overlap with the primary IP addresses of the host configured during installation or the IP addresses used in any other configured virtual switches.
- Ensure that the host IP addresses in the subnet do not overlap with the IP addresses configured for the backplane operations (using network segmentation).
- Ensure that the host IP addresses configured on the hosts in the virtual switch is not a network IP address. For example, in a subnet 10.10.10.0/24, the network IP address of the subnet is 10.10.10.0. Ensure that this IP address (10.10.10.0) is not configured as a host IP address in the virtual switch. Failure message is as follows:

  ```
  Host IP address cannot be assigned equal to the subnet.
  ```

- Ensure that the host IP addresses configured on the hosts in the virtual switch is not the broadcast IP address of the subnet. For example, in a subnet 10.10.10.0/24, the broadcast IP address of the subnet is 10.10.10.255. Ensure that this IP address (10.10.10.255) is not configured as a host IP address in the virtual switch. Failure message is as follows:

  ```
  Host IP address cannot be assigned equal to the subnet broadcast address.
  ```

- Ensure that the subnet configured in the virtual switch has a prefix of /30 or less. For example, you can configure a subnet with a prefix of /30 such as 10.10.10.0/30, but not a subnet with prefix of /31 or /32 such as 10.10.10.0/31 or 10.10.10.0/32. Any subnet that you configure in a virtual switch must have not less than 2 usable IP addresses. Failure message is as follows:

  ```
  Prefix length cannot be greater than 30.
  ```

- Ensure that the host IP addresses configured in a virtual switch belongs to the same subnet. In other words, you cannot configure host IP addresses from two or more different subnets. For example, one host IP address is 10.10.10.10 from the subnet 10.10.10.0/24 and another host IP address is 10.100.10.10 from the subnet 10.100.10.0/24. This configuration fails. Both the hosts must have IP addresses from the 10.10.10.0/24 subnet (or both IP addresses must be from 10.100.10.0/24 subnet). Failure message is as follows:

  ```
  Different host IP address subnets found.
  ```

- Ensure that the gateway IP address for the host IP addresses configured in a virtual switch belongs to the same subnet as host IP addresses. In other words, you cannot configure host IP addresses from one subnet while the gateway IP address of any of those host IP address is in a different subnet. Failure message is as follows:

  ```
  Gateway IP address is not in the same subnet.
  ```

Network Traffic Types

The network traffic is classified into the following types:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1365

- *East/West (Intra-VPC) traffic* - Network traffic that is sent and received on the AHV host internal port br0 by default. The intra-VPC traffic is Geneve encapsulated and stays within the VPC. The intra-VPC traffic is also called East/West traffic because it is sent between nodes within the compute clusters.
- *North/South (ingress/egress) traffic*: Network traffic that enters or exits the VPC. The external network determines the virtual switch and VLAN for this traffic type.

The instructions specified in the Configuring Virtual Switch for VPC Traffic Types on page 71 section can isolate the network traffic to another virtual switch and VLAN if traffic separation from the default AHV and CVM VLAN is desired.

Configuring Virtual Switch for VPC Traffic Types

Configure a new or existing non-default virtual switch for VPC traffic.

About this task

> **Important:** Perform this task only if you require physical network separation of VPC East/West (intra-VPC) or North/South (ingress/egress) traffic. If your site already meets this criteria, then do not perform the configuration mentioned in this section.

The default configuration places all VPC East/West traffic in the AHV VLAN, and all North/South traffic in the external network VLAN. For more information on network traffic types, see Network Traffic Types on page 70.

After you create a new virtual switch, the system automatically creates a new interface on all AHV hosts in the new virtual switch. Allocate one new IP address per AHV host to assign to the new interface.

> **Note:** The assumption is to allocate the IP addresses (IP address that is allocated per AHV host to assign to the new interface) from the default VLAN available in the uplinks of the specific non-default bridge (br1). If you want to allocate the IP addresses from a different VLAN, then tag the required VLAN to the specific non-default bridge (br1).
>
> Log on to the AHV host using the `root` account with SSH, and run the following command to tag the VLAN to the non-default bridge (br1):
>
> ```
> root@ahv# nmcli -g ovs-port.tag con show ovs-port-<bridge-name>
> root@ahv# nmcli con modify ovs-port-<bridge-name> ovs-port.tag <new-vlan-tag>
> ```
>
> Replace <*new_vlan_tag*> with the VLAN tag for the host.
>
> Replace <*bridge-name*> with the non-default bridge br1.
>
> For more information, see Assigning an AHV Host to a VLAN on page 85.

When network segmentation is enabled for virtual switch vs1, the AHV internal interface terminates the Geneve encapsulated East/West traffic on internal port br1.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1366

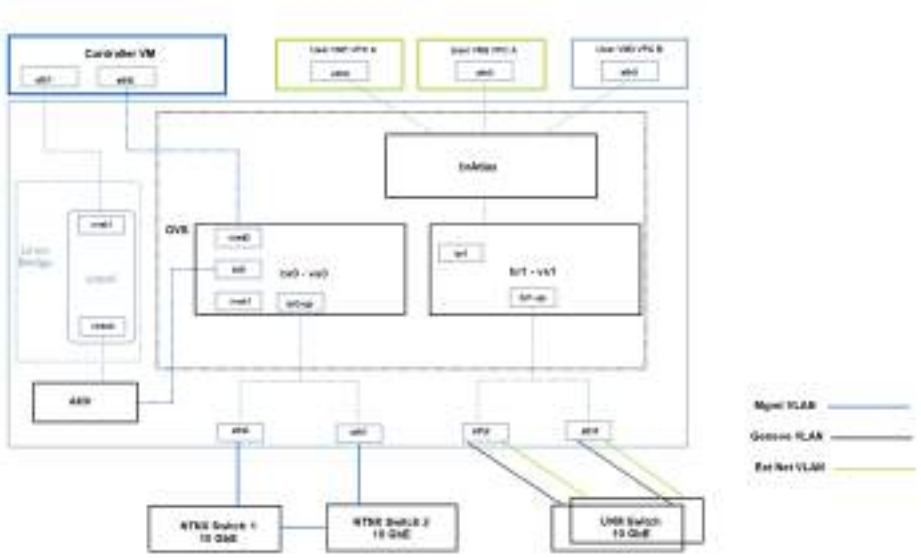


Figure 16: VPC Network Segmentation

Before you begin

You need a virtual switch, other than the default virtual switch vs0, that can be used to route the VPC traffic to achieve optional physical traffic separation. Create a separate virtual switch that you can use to route the VPC traffic.

For information on the procedures to create or update a virtual switch in Prism Element web console, see the Configuring a Virtual Network for Guest VMs section in the *Prism Element Web Console Guide*.

For information on the procedures to create or update a virtual switch in Prism Central, see Network Connections in the *Prism Central Infrastructure Guide*.

> **Note:** Do not create, update or delete any virtual switch when the AOS or AHV upgrade process is running.

Procedure

To configure the uplinks for guest VMs networked by Flow networking VPCs, perform the following steps:

1. Create the virtual switch you want to use for VPC traffic. For example, create `vs1` as a virtual switch for the VPC traffic.

   For more information, see Creating or Updating a Virtual Switch section in the *Prism Element Web Console Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1367

2. Using `acli`, run the following command to configure the IP addresses for the hosts that you have included in the virtual switch and a gateway IP address for the network:

```
nutanix@cvm$ acli net.update_virtual_switch virtual-switch-name
 host_ip_addr_config='{host-uuid1:host_ip_address/prefix;host-uuid2:host_ip_address/
prefix;host-uuid3:host_ip_address/prefix}' gateway_ip_address=IP_address
```

For example, to update the host IP addresses and gateway IP address for virtual switch vs1, the sample command is as follows:

```
nutanix@cvm$ acli net.update_virtual_switch vs1 host_ip_addr_config='{ebeae8d8-47cb-40d0-87f9-
d03a762ffad7:10.XX.XX.15/24;731e24e0-d7a7-11ed-afa1-0242ac120002:10.XX.XX.16/24;88b1746a-d7a7-11ed-
afa1-0242ac120002:10.XX.XX.17/24}' gateway_ip_address=10.XX.XX.1
```

The options are:

- host_ip_addr_config=: Provide the host UUID and associated IP address with prefix as follows:

  ```
  host_ip_addr_config='{host-uuid1:host_ip_address/prefix}'
  ```

  > **Note:** To retrieve the host UUID, run the following command from any CVM:
  >
  > ```
  > nutanix@cvm$ acli host.list
  > ```

  When there are more than one host on the virtual switch, use a semicolon separated list as follows:

  ```
  host_ip_addr_config='{host-uuid1:host_ip_address/prefix;host-
  uuid2:host_ip_address/prefix;host-uuid3:host_ip_address/prefix}'
  ```

- gateway_ip_address=: Provide the gateway IP address as follows:

  ```
  gateway_ip_address=IP_address
  ```

  > **Note:** You can get the gateway IP from the network team at your site. The gateway IP is the same for all the nodes in the cluster.

3. Set the virtual switch for use with Flow Virtual Networking VPCs using the following command:

```
nutanix@cvm$ acli net.set_vpc_east_west_traffic_config virtual_switch=virtual-switch-
name
```

> **Note:** When you run this command, if the virtual switch does not have IP addresses configured for the hosts, the command fails with an error message. For more information, see Conditions for VPC Uplinks on page 69.

For example, to set `vs1` as the virtual switch for VPC traffic, the sample command is as follows:

```
nutanix@cvm$ acli net.set_vpc_east_west_traffic_config virtual_switch=vs1
```

> **Note:** You can set the value for the `permit_all_traffic=` option in the net.set_vpc_east_west_traffic_config command to `true`, if you want to allow this virtual switch to pass traffic other than VPC traffic to the secondary IP of AHV host. For example, ssh and snmp are allowed through the selected virtual switch. The default value for this option is `false` which allows only GENEVE and ICMP traffic to pass through the selected virtual switch and blocks all traffic to the secondary IPs of the AHV Host.
>
> Leave the default `permit_all_traffic=false` option if you only want to use the virtual switch for VPC traffic. Configure the `permit_all_traffic=` option with the value `true` only when you want to

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1368

allow traffic to the secondary IPs of the AHV host. For example, ssh and snmp are allowed through the selected virtual switch.

To update the virtual switch after it is already set, run the following command:

```
nutanix@cvm$ acli net.update_vpc_east_west_traffic_config virtual_switch=vs1
```

Configure the `permit_all_traffic=` option with the value `true` only when you want to allow all traffic types, including the non-VPC traffic, through the selected virtual switch. The value `false` blocks all traffic to the secondary IPs of the AHV host and allows only GENEVE and ICMP pings. To update the `permit_all_traffic=` option with the value `true`, run the following command:

```
nutanix@cvm$ acli net.update_vpc_east_west_traffic_config permit_all_traffic=true
```

4. Update the subnet to use the new virtual switch for the external traffic (or North/South traffic), on the Prism Central VM, using the following command:

```
nutanix@pcvm$ atlas_cli subnet.update external_subnet_name
 virtual_switch_uuid=virtual_switch_uuid
```

What to do next

- To verify if the settings are made as required, run the atlas_config.get command and check the output:

```
nutanix@cvm$ acli atlas_config.get
```

```
config {
  anc_domain_name_server_list: "10.xxx.xxx.xxx"
  dvs_physnet_mapping_list {
    dvs_uuid: "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
    physnet: "physnet1"
  }
  enable_atlas_networking: True
  logical_timestamp: 54
  minimum_ahv_version: "20201105.2016"
  ovn_cacert_path: "/home/certs/OvnController/ca.pem"
  ovn_certificate_path: "/home/certs/OvnController/OvnController.crt"
  ovn_privkey_path: "/home/certs/OvnController/OvnController.key"
  ovn_remote_address: "ssl:anc-ovn-external.default.xxxx.nutanix.com:6652"
  vpc_east_west_traffic_config {
    dvs_uuid: "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
    permit_all_traffic: True
  }
}
```

Where:

  - `dvs_physnet_mapping_list` provides details of the virtual switch.
  - `vpc_east_west_traffic_config` provides the configuration for traffic with `permit_all_traffic` being `true`. It also provides the UUID of the virtual switch being used for traffic as `dvs_uuid: "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"`.

- To verify the UUIDs of all virtual switches, run the following command:

```
nutanix@cvm$ acli net.get_virtual_switch *
```

Observe the following log information to check the uuids of the virtual switches:

```
default: True
description: "Default Virtual Switch"
lacp_config {
lacp: True
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1369

```
lacp_fallback: True
lacp_timeout: "kFast"
}
mtu: 9000
name: "vs0"
nic_team_policy: "kBalanceTcp"
partially_done: False
update_in_progress: False
vswitch_uuid: "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
```

For more information on commands related to managed networks, see Command Reference.

- Perform VLAN tagging. For more information, see VLAN Configuration on page 84.

Clearing and Deleting the Virtual Switch

You can clear and delete a non-default virtual switch used for Flow networking VPC traffic.

About this task

Before you begin

Before you delete a virtual switch that allows Flow networking VPC traffic, you must clear the virtual switch configuration that assigns the VPC traffic to that virtual switch. Use the net.clear_vpc_east_west-traffic_config command.

> **Note:**
>
> Do not create, update or delete any virtual switch when the AOS or AHV upgrade process is running.

About this task

To clear or delete a virtual switch configured to manage Flow networking VPC traffic, do the following:

> **Note:** After you clear the virtual switch settings using step1 on page 75, you can delete the virtual switch in Prism Central.

Procedure

1. Use the `net.clear_vpc_east_west_traffic_config` command to clear the settings on the virtual switch or switches (vs1 per example) configured for Flow networking VPC traffic.
2. Use the `net.delete_virtual_switch virtual_switch=virtual-switch-name` option to delete the virtual switch.

   Replace *`virtual-switch-name`* with the target virtual switch name.

Re-Configuring Bonds Across Hosts Manually

If you are upgrading AOS to 5.20, 6.0, or later versions, you need to migrate the existing bridges to virtual switches. If there are inconsistent bond configurations across hosts before the migration of the bridges, then after the migration of bridges, the virtual switches might not be properly deployed. To resolve such issues, you must manually configure the bonds to make them consistent.

Before you begin

Ensure that you meet the following prerequisites before you reconfigure the bonds:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1370

- Place the affected AHV host where you want to reconfigure the bonds into maintenance mode.

  Log on to any CVM using SSH, and run the following command:

  ```
  nutanix@cvm$ acli host.enter_maintenance_mode hypervisor-IP-address [wait="{ true | false }" ] [non_migratable_vm_action="{ acpi_shutdown | block }" ]
  ```

  Replace *hypervisor-IP-address* with either the IP address or host name of the AHV host you want to shut down.

  The following are optional parameters for running the `acli host.enter_maintenance_mode` command:

  - **wait**: Set the **wait** parameter to **true** to wait for the host evacuation attempt to finish.
  - **non_migratable_vm_action**: By default the **non_migratable_vm_action** parameter is set to **block**, which means the non-migratable VMs are shut down when you put a node into maintenance mode. For more information on non-migratable VMs, see Non-Migratable VMs.

    Note: VMs with host affinity policies are also not migrated to other hosts in the cluster, if any of the following condition is met:

    - The hosts that are configured as part of VM-Host affinity policy are not available.
    - The hosts that are part of VM-Host affinity policy does not have the sufficient resources to run the VM.

    If you want to automatically shut down such VMs, set the **non_migratable_vm_action** parameter to **acpi_shutdown**.

  For more information, see Putting a Node into Maintenance Mode using CLI on page 30.

- Check the **Cluster Resiliency / Fault Tolerance Status** widget in the Prism Element web console dashboard to ensure that the cluster is healthy and resilient to any brief interruptions to network connectivity during uplink changes. For more information, see Home Dashboard in the *Prism Web Console Guide*.

About this task

Important:

- Perform the bond changes only on one host at a time. Ensure that you get the completed host out of maintenance mode before you proceed to work on any other affected hosts.
- Use this procedure only when you need to modify the inconsistent bonds in a migrated bridge across hosts in a cluster, that is preventing Acropolis (AOS) from deploying the virtual switch for the migrated bridge.

  Do not use **nmcli** commands to make the bridge level changes. Use the **manage_ovs** commands, instead.

  The manage_ovs command allows you to update the cluster configuration. The changes are applied and retained across host restarts. The nmcli command allows you to update the live running host configuration but does not update the AOS cluster configuration and the changes are lost at host restart. This behavior of nmcli introduces connectivity issues during maintenance, such as upgrades or hardware replacements.

  nmcli is typically used in cases where a host might be isolated on the network and requires a workaround to gain connectivity before the cluster configuration can actually be updated using manage_ovs.

Note: Disable the virtual switch before you attempt to change the bonds or bridge.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1371

If you face an issue where the virtual switch is automatically re-created after it is disabled (with AOS versions 5.20.0 or 5.20.1), follow steps 1 and 2 below to disable such an automatically re-created virtual switch again before migrating the bridges. For more information, see KB-3263.

Be cautious when using the disable_virtual_switch command because it deletes all the configurations from the IDF, not only for the default virtual switch vs0, but also any virtual switches that you may have created (such as vs1 or vs2). Therefore, before you use the disable_virtual_switch command, ensure that you check a list of existing virtual switches, that you can get using the acli net.get_virtual_switch command.

Complete this procedure on each host Controller VM that is sharing the bridge that needs to be migrated to a virtual switch.

Procedure

1. To list the virtual switch, use the following command.

   ```
   nutanix@cvm$ acli net.list_virtual_switch
   ```

2. Disable all the virtual switches.

   ```
   nutanix@cvm$ acli net.disable_virtual_switch
   ```

   All the virtual switches in the cluster are disabled.

3. Change the bond type to align with the same bond type on all the hosts for the specified virtual switch

   ```
   nutanix@cvm$ manage_ovs --bridge_name bridge-name --bond_name bond_name --
   bond_mode bond-type update_uplinks
   ```

   Where:

   - *bridge-name*: Provide the name of the bridge, such as **br0** for the virtual switch on which you want to set the uplink bond mode.
   - *bond-name*: Provide the name of the uplink port such as **br0-up** for which you want to set the bond mode.
   - *bond-type*: Provide the bond mode that you require to be used uniformly across the hosts on the named bridge.

   Use the `manage_ovs --help` command for help on this command.

   Note: To disable LACP, change the bond type from LACP Active-Active (balance-tcp) to Active-Backup/Active-Active with MAC pinning (balance-slb) by setting the *bond_mode* using this command as active-backup or balance-slb.

   Ensure that you turn off LACP on the connected ToR switch port as well. To avoid blocking of the bond uplinks during the bond type change on the host, ensure that you follow the ToR switch best practices to enable LACP fallback or passive mode.

   To enable LACP, configure *bond-type* as balance-tcp (Active-Active) with additional variables `--lacp_mode fast` and `--lacp_fallback true`.

4. Exit the host from maintenance mode, using the following command:

   ```
   nutanix@cvm$ acli host.exit_maintenance_mode hypervisor-IP-address
   ```

   Replace *hypervisor-IP-address* with the IP address of the AHV host.

   This command migrates (live migration) all the VMs that were previously running on the host back to the host. For more information, see Exiting a Node from the Maintenance Mode Using CLI on page 32.

5. Repeat the above steps for each host for which you intend to reconfigure bonds.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1372

6. (If migrating to AOS version earlier than 5.20.2) Check if the issue in the note and disable the virtual switch.

What to do next

After making the bonds consistent across all the hosts configured in the bridge, migrate the bridge or enable the virtual switch. For more information, see:

- Configuring a Virtual Network for Guest VM Interfaces in the *Prism Element Web Console Guide*.
- Network Configuration in the *Prism Central Infrastructure Guide*.

To check whether LACP is enabled or disabled, use the following command.

```
nutanix@cvm$ manage_ovs show_uplinks
```

Change Interface Ring Buffer Sizes

This section describes the procedure to change the ring buffer sizes of interfaces on AHV hosts.

This feature introduces a safe method to change the RX and TX ring buffer sizes for interfaces on virtual switches in AHV without triggering out-of-memory (OOM) or kernel panic issues when the cluster experiences heavy loads.

> **Note:** Do not disable and re-enable a NIC. Nutanix does not support toggling the NIC status (disable and enable toggling or cycle) because it might cause an out-of-memory (OOM) error leading to a Controller VM failure and loss of connectivity to the AHV host.

Requirements and Support for Ring Buffer Size Changes

This section describes the requirements for changing ring buffer sizes of interfaces on an AHV host

- This feature requires a minimum AOS version of 7.0 with AHV version of 10.0 or later.
- This feature involves an update command that triggers the rolling reboot process for the AHV host or hosts to which on which you are increasing the ring buffer sizes.

  When you run the command to change the ring buffer size, the Controller VM displays a message stating that the AHV host rebooted because of the kernel memory reservation. The message also asks if you want to proceed. The ring buffer size change is implemented only if you type **yes** on the console.

  Increasing the ring buffer size involves reserving additional kernel memory on the AHV host.
- This feature is supported on HCI and compute-only nodes.
- This feature is supported for changing a single host NIC in a single command run, provided that host NIC is not participating in an uplink bond. In other words, the host NIC must be an independent host NIC that is not attached to any uplink bonds configured on the host.

  If you attempt to change the ring buffer size on a single NIC that is configured in an uplink bond, the command interface displays an error that ring buffer sizes of all the interfaces in the same bond must be changed together.
- This feature supports changing the ring buffer sizes on multiple host NICs in a single CLI command run, subject to the following conditions:

  - You can configure multiple host NICs in a single command run, only if all the host NICs belong to the same uplink bond. Configuring multiple host NICs from different uplink bonds in a single command run is not supported.

    > **Note:** The ring buffer sizes of all the host NICs in an uplink bond must be identical. Do not change the ring buffer sizes only on some host NICs in an uplink bond.

  - When the MTU of any NIC changes, the ring buffer size might also change. When the ring buffer size changes due to MTU changes on any NIC in an uplink bond, an alert is raised. Check the ring buffer sizes of all the

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1373

NICs in the uplink bond and ensure that they are the same size by updating the ring buffer size of all NICs in one uplink bond.

- You cannot configure a mixed set of host NICs in a single command run. A mixed set of host NICs has some independent host NICs that do not belong to any uplink bonds and other bonded host NICs belong to one or more uplink bonds.

  In other words, you can configure in a single command, either a single independent host NIC or a set of all bonded host NICs belonging to a single uplink bond. Mixed sets of NICs are not supported.

- You must configure the comma-separated list of interfaces correctly in the `net.update_host_nic` command to change the ring buffer sizes of the listed interfaces. The output of the `net.list_host_nic <host_ip>` command provides the list of interfaces. Use this list to create the comma-separated list of interfaces correctly.

  For more information, see Changing the Interface Ring Buffer Sizes on page 80.

- This feature requires that the ring buffer size change be valid and comply with the following restrictions.

  - The minimum ring buffer size must be 128 bytes.
  - The maximum ring buffer size cannot exceed the maximum size permitted by the NIC driver.
  - The incremental change to the ring buffer size must be multiple of 2 bytes except the maximum value which must be the actual value. Therefore, the examples of valid values are 128, 256, 512, and 1024.
  - The default ring buffer size for RX and TX is determined by the type of NIC.

    If the ring buffer sizes are never changed, the sizes displayed in the output of the `net.list_host_nic <host_ip>` command are the default sizes. If you change the ring buffer sizes of the NICs to 0 using the `net.update_host_nic` command, the ring buffer sizes are reset to the default sizes. In that case, the output of the `net.list_host_nic <host_ip>` command displays the default ring buffer sizes of the NICs.

Limitations For Ring Buffer Size Changes

This section describes the limitations for changing ring buffer sizes of interfaces on an AHV host

- This feature is not supported on a storage-only node since, on a Storage-only node, most of the resources are allocated to the Controller VM (CVM).
- This feature utilizes additional memory on the host. It reserves additional memory with the AHV scheduler. Increasing the ring buffer size reduces the overall available capacity of the host. The ring buffer size changes made using the workflow succeed only if the necessary resources are available on the host. The workflow for the ring buffer size change triggered by the `net.update_host_nic` command checks how much additional memory is necessary and tries to reserve the same with the AHV scheduler. If the reservation is successful, the ring buffer size change task is reported as successful. If the reservation fails, the task aborts and is reported as a failure.

  Therefore, ensure that the host has sufficient resources before you change the ring buffer sizes.
- This feature does not support running multiple ring size update tasks in parallel. You can run only one ring size update task at a time through a single CLI command run at a time. This restriction exists because the feature requires restarting the AHV host and Nutanix supports only one rolling reboot task at a time in a cluster.

  Wait until the ongoing task and the rolling reboot is completed successfully, before running the CLI command again for another change in the ring buffer sizes. If a ring buffer size change is ongoing when you run the `net.update_host_nic` command for another change, the output of the command displays an error message such as the following:

  ```
  Invalid: There is already a rolling restart task in progress. Please wait for that
   task to finish before updating host NIC configuration.
  ```

- When a physical NIC is replaced, the ring buffer size is reset to the default ring buffer sizes. The required ring buffer size must be set on the new NIC using the procedure provided in Changing the Interface Ring Buffer Sizes on page 80.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1374

Changing the Interface Ring Buffer Sizes

This section provides the procedure to change the ring buffer sizes of a NIC or NICs.

About this task

Changing the ring buffer size involves identifying the IP address of the AHV host and NIC or NICs for which you plan to change the ring buffer sizes.

> **Note:** Do not disable and re-enable a NIC. Nutanix does not support toggling the NIC status (disable and enable toggling or cycle) because it might cause an out-of-memory (OOM) error leading to a Controller VM failure and loss of connectivity to the AHV host.

Procedure

1. Log in to the cluster using the admin account with SSH.
2. Access the Acropolis CLI (`<acropolis>`) by entering `acli` at the prompt.

```
admin@cvm$ acli
<acropolis>
```

3. Identify the virtual switch that the NIC is configured on.

```
<acropolis>net.list_virtual_switch
```

From the table of virtual switches, note the virtual switch name.

The following sample output of the command displays the default virtual switch.

```
<acropolis>net.list_virtual_switch
VS Name  VS UUID                              MTU   Bond Type      Bridge  IGMP
 Snooping  VS OWNER
vs0      9178a66a-b485-47fc-92b0-bf944d521b35  1500  kActiveBackup  br0     Disabled
      kPE
```

4. Identify the host that the Virtual Switch has the NIC or NICs configured.

```
<acropolis>net.get_virtual_switch <virtual-switch-name>
```

From the virtual switch details, note the UUID of the AHV host that hosts the NIC(s).

The following sample output displays the attributes of the default switch, vs0.

```
<acropolis> net.get_virtual_switch vs0
config {
  cluster_configuration_list {
    cluster_uuid: "00062174-1015-b922-0000-000000024dc4"
    config_failed: False
    default_uplink_grouping: "kMixed"
    host_configuration_list {
      config_failed: False
      host_uuid: "4de7492f-5836-4828-91f6-85f3be5e3562"
      internal_bridge: "br0"
      route_table: 1000
      uplink_list: "eth0"
      uplink_list: "eth1"
      uplink_list: "eth2"
      uplink_list: "eth3"
    }
  }
  default: True
  description: "Default Virtual Switch"
  lacp_config {
    lacp: False
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1375

```
  }
  logical_timestamp: 1
  mtu: 1500
  name: "vs0"
  nic_team_policy: "kActiveBackup"
  owner_type: "kPE"
  partially_done: False
  vswitch_uuid: "9178a66a-b485-47fc-92b0-bf944d521b35"
}
```

5. Identify the IP address of the AHV host that the NIC belongs to.

```
<acropolis>host.list
```

From the table of hosts, note the IP address of the AHV host identified by the host UUID noted in the previous step.

The following sample output of the command displays the host that has its NICs configured in the default virtual switch.

```
<acropolis> host.list
Hypervisor IP  Hypervisor DNS Name  Host UUID                              Node state
      Connected  Node type       Schedulable  Hypervisor Name  CVM IP
10.19.225.53   10.19.225.53         4de7492f-5836-4828-91f6-85f3be5e3562
 AcropolisNormal  True       Hyperconverged  True         AHV
 10.19.225.57
```

6. List the NIC or NICs on the AHV host.

```
<acropolis>net.list_host_nic <host-IP-address>
```

From the table of NICs, note the <port-name> of the NIC that you plan to change the ring buffer size for. The table of NICs also lists the respective TX and RX ring buffer sizes.

The following sample output displays the host NICs on the sample host identified by the sample IP address, 10.19.xxx.53.

```
<acropolis> net.list_host_nic 10.19.225.53
Port Name  MAC Address        Link Capacity (Mbps)  Link Status  RX Ring Size  TX
 Ring Size
eth0       ac:1f:6b:6f:20:94  1000                  Down         1024          1024
eth1       ac:1f:6b:6f:20:95  1000                  Down         1024          1024
eth2       00:e0:ed:92:ec:38  10000                 Up           1024          1024
eth3       00:e0:ed:92:ec:39  10000                 Up           1024          1024
```

7. Update the ring buffer sizes of the identified NIC.

You can change the RX and TX values separately or together. You can change only the RX ring buffer size, only the TX ring buffer size, or both RX and TX ring buffer sizes in a command run.

```
<acropolis>net.update_host_nic <host-IP-address> <nic-port-name> | <nic-port-names-
comma-separated-list> rx_ring_size=<rx_size> tx_ring_size=<tx_size>
```

For example, if the sample host IP address is 10.19.xxx.53, the sample NIC port name is eth0, and the sample ring buffer size to be updated is 1024, then the sample command would be:

```
<acropolis>net.update_host_nic 10.19.xxx.53 eth0 rx_ring_size=1024 tx_ring_size=1024
```

The output displays a message warning you that the AHV host reboots and changing the ring buffer size reserves additional kernel memory on the AHV host. It asks you to type **yes** to proceed or **no** to cancel the change.

If you choose to proceed and type **yes**, the output displays a message that the rolling reboot task with task UUID is launched to apply the host NIC update. Note the task UUID.

```
<acropolis>net.update_host_nic 10.19.xxx.53 eth0 rx_ring_size=1024 tx_ring_size=1024
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1376

```
This operation will reboot the AHV host. Also, changing of ring buffer size(s) may
 result in the reservation of additional kernel memory on the AHV host.
Do you really want to proceed? (yes/no) yes
"Rolling reboot task 40e93734-064c-xxxx-xxxx-8ddc9bf9xxxx is launched to apply
 the host NIC update. Please monitor this task's progress for the final execution
 result."
<acropolis>
```

The reboot process disconnects the SSH connection to the host.

8. Verify if the host NIC update task was successful after the reboot is complete:

   a. Log in to the cluster using the admin account with SSH.

   b. Get the task details using the task uuid to check the status.

      ```
      admin@cvm$ ecli task.get <task-uuid>
      ```

      Where, `<task-uuid>` is the UUID of the rolling reboot task. It is displayed in the output of the `net.update_host_nic` command.

      The output displays the details of the task run. These details include the `display-name`, `message`, `state` and `status` parameters. The `state` and `status` parameters display `kSucceeded` if the task completed successfully.

   c. Verify the changes:

      ```
      <acropolis> net.list_host_nic <host-ip-address>
      ```

      The output displays the host NIC table with the changed ring buffer sizes for the NICs that were included in the NIC list in the command.

Enabling LACP and LAG (AHV Only)

This section describes the procedure to enable LAG and LACP in AHV nodes and the Top-of-Rack (ToR) switch or any switch that is directly connected to the Nutanix node.

Procedure

To enable LACP and LAG, perform the following steps:

1. Login to the Prism Element web console and go to **Settings** > **Network Configuration** > **Virtual Switch**.

   You can also login to Prism Central, select the **Infrastructure** application from Application Switcher Function, and go to **Network & Security** > **Subnets** > **Network Configuration** > **Virtual Switch** from the navigation bar.

   The system displays the **Virtual Switch** tab.

2. Click the Edit icon ( ) for the target virtual switch on which you want to configure LACP and LAG.

   The system displays the **Edit Virtual Switch** window.

3. In the **General** tab, choose **Standard (Recommended)** option in the **Select Configuration Method** field, and click **Next**.

   Important: When you select the **Standard** method, only the hosts that have been updated are restarted.

   The **Standard** configuration method puts each updated node in maintenance mode before applying the updated settings. After applying the updated settings, the node exits from maintenance mode. For more information, see Virtual Switch Workflow.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1377

4. In the **Uplink** Configuration tab, select `Active-Active` in the **Bond Type** field, and click **Save**.

   > **Note:** The `Active-Active` bond type configures all AHV hosts with the fast setting for LACP speed, causing the AHV host to request LACP control packets at the rate of one per second from the physical switch. In addition, the `Active-Active` bond type configuration sets LACP fallback to `Active-Backup` on all AHV hosts. You cannot modify these default settings after you have configured them in Prism, even by using the CLI.

   This completes the LAG and LACP configuration on the cluster. At this stage, cluster starts the Rolling Reboot operation for all the AHV hosts. Wait for the reboot operation to complete before you put the node and CVM in maintenance mode and change the switch ports.

   For more information about how to manually perform the rolling reboot operation for an AHV host, see Rebooting an AHV Node in a Nutanix Cluster.

Perform the following steps on each node, one at a time:

5. Put the node and the Controller VM into maintenance mode.

   > **Note:** Before you put a node in maintenance mode, see Verifying the Cluster Health and carry out the necessary checks.

   The Step 6 in Putting a Node into Maintenance Mode using Web Console section puts the Controller VM in maintenance mode.

6. Change the settings for the interface on the switch that is directly connected to the Nutanix node to match the LACP and LAG settings made in the Edit Virtual Switch window above.

   For more information about how to change the LACP settings of the switch that is directly connected to the node, refer to the vendor-specific documentation of the deployed switch.

   Nutanix recommends you perform the following configurations for LACP settings on the switch:

Table 8: Nutanix Recommendations for LACP Settings

Nutanix Recommendations	Description
Enable LACP fallback	Nutanix recommends you enable LACP fallback to set up a workaround for the port, using which the port establishes a link before the switch receives the LACP Bridge Protocol Data Units (BPDUs). The LACP fallback helps avoid link failures if either AHV host or switch that is connected to the AHV node does not negotiate LACP. LACP fallback provides seamless discovery of new nodes in an active or passive capacity setup and reduces the impact on the node operation. When LACP fallback is enabled, you can have a minimal business impact as VMs and applications remain healthy in case of an LACP status mismatch between the AHV host and the ToR switch port. As LACP fallback ensures connectivity during initial deployment, so it is crucial when you do not have LACP in discoveryOS. **Caution:** When LACP fallback occurs, the port runs in fallback mode, and this might lead to an unbalanced utilization of ports and lack of redundancy in your site deployment. Based on your internal networking policies, you can decide whether LACP fallback is helpful for you, and enable or disable it.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1378

Nutanix Recommendations	Description
Consider the LACP time options *(slow and fast)*	If the switch has a fast configuration, Nutanix recommends you set the LACP time to fast on AHV host. Nutanix recommends the LACP time to match on both; switch and AHV host, for L2 failure detection at the same time on the switch and AHV host. If the switch has a fast configuration, set the LACP time to fast on AHV host. When the LACP time setting matches on AHV host and switch, the detachment of a failed interface occurs at the same time, and both switch and the AHV host do not use the failed interface. When the LACP time is set to: • *fast* - Failure detection occurs faster within 3 seconds • *slow* - Failure detection occurs slowly and takes up to 90 seconds The matching LACP time helps to prevent the outage.

7. Verify that LACP negotiation status is `Negotiated`.

   Perform the SSH to the CVM as a nutanix user, and run the following commands:

   ```
   nutanix@CVM$ ssh root@[AHV host IP] "ovs-appctl bond/show bond-name"
   ```

   ```
   nutanix@CVM$ ssh root@[AHV host IP] "ovs-appctl lacp/show bond-name”
   ```

   - Replace the following attributes in the above commands:
     - `bond-name` with the actual name of the uplink port such as br0-up in the above commands.
     - `[AHV host IP]` with the actual AHV host IP at your site.
   - Search for the string `negotiated` in the status lines.

8. Remove the node and Controller VM from maintenance mode. For more information, see Exiting a Node from the Maintenance Mode using Web Console.

   The Controller VM exits maintenance mode during the same process.

What to do next

Do the following after completing the procedure to enable LAG and LACP in all the AHV nodes the connected ToR switches:

- Verify that the status of all services on all the CVMs are Up. Run the following command and check if the status of the services is displayed as **Up** in the output:

  ```
  nutanix@cvm$ cluster status
  ```

- Log in to the Prism Element web console of the node and ensure that the **Cluster Resiliency / Fault Tolerance Status** widget displays **OK**.

VLAN Configuration

You can set up a VLAN-based segmented virtual network on an AHV node by assigning the ports on virtual bridges managed by virtual switches to different VLANs. VLAN port assignments are configured from the Controller VM that runs on each node.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1379

For best practices associated with VLAN assignments, see AHV Networking Recommendations on page 48. For information on assigning guest VMs to a virtual switch and VLAN, see Network Connections in the *Prism Central Infrastructure Guide*.

Assigning an AHV Host to a VLAN

About this task

> **Note:** Perform the following procedure during a scheduled maintenance window. Before you begin, stop the cluster. Once the process begins, hosts and CVMs partially lose network access to each other and VM data or storage containers become unavailable until the process completes.

To assign an AHV host to a VLAN, do the following on every AHV host in the cluster:

Procedure

1. Log on to the AHV host using `root` account with SSH.
2. Put the AHV host and the CVM in maintenance mode.
   For more information, see Putting a Node into Maintenance Mode using CLI on page 30.
3. Assign port br0 (the internal port on the default OVS bridge, br0 on default virtual switch vs0) to the VLAN that you want the host be on.

   ```
   root@ahv# nmcli con modify ovs-port-br0 ovs-port.tag <new-vlan-tag>
   ```

   Replace `<new-vlan-tag>` with the VLAN tag for the host.
4. Bring up the connection to apply the new VLAN configuration for the AHV host.

   ```
   root@ahv# nmcli con up ovs-port-br0
   ```

5. Confirm VLAN tagging on port br0.

   ```
   root@ahv# nmcli -g ovs-port.tag con show ovs-port-br0
   ```

6. Check the value of the tag parameter that is shown.
7. Verify connectivity to the IP address of the AHV host by performing a ping test.
8. Exit the AHV host and the CVM from the maintenance mode.
   For more information, see Exiting a Node from the Maintenance Mode Using CLI on page 32.

What to do next

Remove the VLAN configuration for AHV Host. For more information, see Removing VLAN Configuration for CVM and AHV Host on page 87.

Assigning the Controller VM to a VLAN

By default, the public interface of a Controller VM is assigned to VLAN 0. To assign the Controller VM to a different VLAN, change the VLAN ID of its public interface. After the change, you can access the public interface from a device that is on the new VLAN.

About this task

> **Note:** Perform the following procedure during a scheduled maintenance window. Before you begin, stop the cluster. Once the process begins, hosts and CVMs partially lose network access to each other and VM data or storage containers become unavailable until the process completes.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1380

> **Note:** To avoid losing connectivity to the Controller VM, do not change the VLAN ID when you are logged on to the Controller VM through its public interface. To change the VLAN ID, log on to the internal interface that has IP address 192.168.5.254.

Perform these steps on every Controller VM in the cluster. To assign the Controller VM to a VLAN, do the following:

Procedure

1. Log on to the AHV host with SSH.
2. Put the AHV host and the Controller VM in maintenance mode.

   For more information, see Putting a Node into Maintenance Mode using CLI on page 30.
3. Check the Controller VM status on the host.

   ```
   root@host# virsh list
   ```

   An output similar to the following is displayed:

   ```
   root@host# virsh list
    Id    Name                           State
   ----------------------------------------------------
    1     NTNX-CLUSTER_NAME-3-CVM            running
    3     3197bf4a-5e9c-4d87-915e-59d4aff3096a running
    4     c624da77-945e-41fd-a6be-80abf06527b9 running

   root@host# logout
   ```
4. Log on to the Controller VM (CVM).

   ```
   root@host# ssh nutanix@192.168.5.254
   ```

   Accept the host authenticity warning if prompted, and enter the CVM nutanix password.
5. Assign the public interface of the Controller VM to a VLAN.

   ```
   nutanix@cvm$ change_cvm_vlan vlan_id
   ```

   Replace *vlan_id* with the ID of the VLAN to which you want to assign the Controller VM.

   For example, add the Controller VM to VLAN 201.

   ```
   nutanix@cvm$ change_cvm_vlan 201
   ```
6. Confirm VLAN tagging on the Controller VM.

   ```
   root@host# virsh dumpxml cvm_name
   ```

   Replace *cvm_name* with the CVM name or CVM ID to view the VLAN tagging information.

   > **Note:** Refer to step 3 for Controller VM name and Controller VM ID.

   An output similar to the following is displayed:

   ```
   root@host# virsh dumpxml 1 | grep "tag id" -C10 --color
         <target dev='vnet2'/>
         <model type='virtio'/>
         <driver name='vhost' queues='4'/>
         <alias name='net2'/>
         <address type='pci' domain='0x0000' bus='0x00' slot='0x05' function='0x0'/>
       </interface>
       <interface type='bridge'>
         <mac address='50:6b:8d:b9:0a:18'/>
         <source bridge='br0'/>
   ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1381

```
      <vlan>
           <tag id='201'/>
      </vlan>
      <virtualport type='openvswitch'>
        <parameters interfaceid='c46374e4-c5b3-4e6b-86c6-bfd6408178b5'/>
      </virtualport>
      <target dev='vnet0'/>
      <model type='virtio'/>
      <driver name='vhost' queues='4'/>
      <alias name='net3'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x03' function='0x0'/>
    </interface>
root@host#
```

7. Check the value of the tag parameter that is shown.
8. Restart the network service.

```
nutanix@cvm$ sudo service network restart
```

9. Verify connectivity to the Controller VMs external IP address by performing a ping test from the same subnet. For example, perform a ping from another Controller VM or directly from the host itself.
10. Exit the AHV host and the Controller VM from the maintenance mode.

    For more information, see Exiting a Node from the Maintenance Mode Using CLI on page 32.

What to do next

Remove the VLAN configuration for CVM. For more information, see Removing VLAN Configuration for CVM and AHV Host on page 87.

Removing VLAN Configuration for CVM and AHV Host

This section describes how to remove the VLAN tags from AHV host and CVM, and revert to the default untagged configuration.

About this task

Perform the following procedure during a scheduled maintenance window. Before you begin, stop the cluster. Once the process begins, hosts and CVMs partially lose network access to each other and VM data or storage containers become unavailable until the process completes.

> **Note:** To avoid losing connectivity to the Controller VM, do not remove the VLAN ID when you are logged on to the Controller VM through its public interface. To change the VLAN ID, log on to the internal interface that has IP address 192.168.5.254.

> **Important:** Ensure that you have access to the out of band management interface (IPMI, ILO, iDRAC, etc.) for the hosts which helps you to recover the hosts more easily in case of any misconfiguration.

Procedure

To remove the VLAN tagging from CVM and AHV host, perform the following steps:

1. Put the AHV host and the CVM in maintenance mode.

   For more information, see Putting a Node into Maintenance Mode using CLI on page 30.
2. Log on to the Controller VM using SSH.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1382

3. Run the following command to remove the VLAN configuration for the Controller VM.

```
nutanix@cvm$ change_cvm_vlan --remove
```

4. Log on to the AHV host using `root` account with SSH.

5. Run the following command to remove the VLAN configuration for the AHV host.

```
root@ahv# nmcli con modify ovs-port-br0 ovs-port.tag 0
```

6. Bring up the connection to apply the new VLAN configuration for the AHV host.

```
root@ahv# nmcli con up ovs-port-br0
```

7. Exit the AHV host and the CVM from the maintenance mode.

   For more information, see Exiting a Node from the Maintenance Mode Using CLI on page 32.

IGMP Snooping

On an AHV host, when multicast traffic flows to a virtual switch the host floods the Mcast traffic to all the VMs on the specific VLAN. This mechanism is inefficient when many of the VMs on the VLAN do not need that multicast traffic. IGMP snooping allows the host to track which VMs on the VLAN need the multicast traffic and send the multicast traffic to only those VMs. For example, assume there are 50 VMs on VLAN 100 on virtual switch vs1 and only 25 VMs need to receive (hence, receiver VMs) the multicast traffic. Turn on IGMP snooping to help the AHV host track the 25 receiver VMs and deliver the multicast traffic to only the 25 receiver VMs instead of pushing the multicast traffic to all 50 VMs.

When IGMP snooping is enabled in a virtual switch on a VLAN, the ToR switch or router queries the VMs about the Mcast traffic that the VMs are interested in. When the switch receives a join request from a VM in response to the query, it adds the VM to the multicast list for that source entry as a receiver VM. When the switch sends a query, only the VMs that require the multicast traffic respond to the switch. The VMs that do not need the traffic do not respond at all. So, the switch does not add a VM to a multicast group or list unless it receives a response from that VM for the query.

Typically, in a multicast scenario, there is a source entity that casts the multicast traffic. This source may be another VM in this target cluster (that contains the target VMs that need to receive the multicast traffic) or another cluster connected to the target cluster. The host in the target cluster acts as the multicast router. Enable IGMP snooping in the virtual switch that hosts the VLAN connecting the VMs. You must also enable either the native Acropolis IGMP querier on the host or a separate third party querier must exist in the network. Check the documentation of your network vendor to enable an IGMP querier in the appropriate networks. The native Acropolis IGMP querier sends IGMP v2 query packets to the VMs.

The IGMP Querier sends out queries periodically to keep the multicast groups or lists updated. The periodicity of the query is determined by the IGMP snooping timeout value that you must specify when you enable IGMP snooping. For example, if you have configured the IGMP snooping timeout as 30 seconds then the IGMP Querier sends out a query every 15 seconds.

When you enable IGMP snooping and are using the native Acropolis IGMP querier, you must configure the IGMP VLAN list. The IGMP VLAN list is a list of VLANs that the native IGMP Querier must send the query out to. This list value is a comma-separated list of the VLAN IDs that the query needs to be sent to. If you do not provide a list of VLANs, then the native IGMP Querier sends the query to all the VLANs in the switch.

When a VM needs to receive the multicast traffic from specific multicast source, configure the multicast application on the VM to listen to the queries received by the VM from the IGMP Querier. Also, configure The multicast application on the VM to respond to the relevant query, that is, the query for the specific multicast source. The response that the application sends is logged by the virtual switch which then sends the multicast traffic to that VM instead of flooding it to all the VMs on the VLAN.

A multicast source always sends multicast traffic to a multicast group or list that is indicated by a multicast group IP address.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1383

Enabling or Disabling IGMP Snooping

IGMP snooping helps you manage multicast traffic to specific VMs configured on a VLAN.

About this task

You can only enable IGMP snooping using aCLI.

Procedure

- Run the following command:

```
net.update_virtual_switch virtual-switch-name enable_igmp_snooping=true
 enable_igmp_querier=[true | false] igmp_query_vlan_list=VLAN IDs
 igmp_snooping_timeout=timeout
```

  Provide:

  - *virtual-switch-name*—The name of the virtual switch in which the VLANs are configured. For example, the name of the default virtual switch is *vs0*. Provide the name of the virtual switch exactly as it is configured.
  - enable_igmp_snooping=[*true | false*]—*true* to enable IGMP snooping. Provide *false* to disable IGMP snooping. The default setting is *false*.
  - enable_igmp_querier=[*true | false*]—*true* to enable the native IGMP querier. Provide *false* to disable the native IGMP querier. The default setting is *false*.
  - igmp_query_vlan_list=*VLAN IDs*—List of VLAN IDs mapped to the virtual switch for which IGMP querier is enabled. When it's not set or set as an empty list, querier is enabled for all VLANs of the virtual switch.
  - igmp_snooping_timeout=*timeout*—An integer indicating time in seconds. For example, you can provide *30* to indicate IGMP snooping timeout of 30 seconds.

    The default timeout is *300* seconds.

    You can set the timeout in the range of *15* - *3600* seconds.

What to do next

You can verify whether IGMP snooping is enabled or disabled by running the following command:

```
net.get_virtual_switch virtual-switch-name
```

The output of this command includes the following sample configuration:

```
igmp_config {
  enable_querier: True
  enable_snooping: True
 }
```

The above sample shows that IGMP snooping and the native acropolis IGMP querier are enabled.

Traffic Redirection and Inspection

This section describes traffic redirection and inspection tools that Nutanix provides.

Tools that perform network traffic redirection or traffic inspection request promiscuous mode configuration on the VM vNIC to receive traffic that is not originally directed to that VM. Instead of promiscuous mode, Nutanix AHV provides other traffic redirection tools, based on the use case or the required outcome.

A VM in an AHV host receives only the traffic that is specifically directed to the MAC address of that VM. The VM does not receive any other traffic unless the traffic is redirected to it by one of these traffic redirection tools. These tools are described in the following sections.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1384

Policy-based Routing for Redirection

This section describes policy-based routing deployed using Flow Virtual Networking Network Controller for traffic redirection and inspection.

For traffic already flowing between separate subnets inside Flow Virtual Networking VPCs, use policy-based routing (PBR) to redirect the traffic to a separate, routed Layer 3 endpoint device such as a firewall VM.

A single firewall VM or a pair of active and standby VMs in the VPC act as reroute destination(s) for all the VMs networked in the VPC. The reroute action is performed on the virtual router and the original packet is forwarded to the active destination VM which receives the traffic, and then evaluates whether to forward or drop the traffic.

Firewalls and VPN appliances inside a VPC are examples of devices that might use PBR. For more information on Policies that can be created for routing (or policy-based routing), see Creating a Policy in the *Flow Virtual Networking Guide*.

Traffic Mirroring for Traffic Redirection and Inspection

This section describes Traffic Mirroring for traffic redirection and inspection.

For traffic that does not cross a routed boundary, or for traffic that must be duplicated instead of forwarded for processing, use Traffic Mirroring sessions to forward a copy of the traffic from a VM or physical interface to a single destination VM.

The single destination VM is provisioned on any host in the cluster. The original packet is not modified when the traffic is copied to the destination or target VM.

Packet capture devices, traffic inspection devices, or troubleshooting tools that use on-premises AHV VLANs or VPCs, are examples that might use traffic mirroring. Use Traffic Mirroring when a physical switch Traffic Mirroring port is connected to a Nutanix AHV server. Traffic Mirroring forwards this switch port to a destination or target VM. For more information on Traffic Mirroring, see Traffic Mirroring on AHV Hosts on page 90 and Traffic Mirroring in the *Prism Central Infrastructure Guide*.

Service Chain

This section describes Service Chaining for traffic redirection and inspection.

For traffic in Basic VLANs for VMs on on-premises AHV hosts, service chaining transparently redirects the traffic through, or copies to, service VMs running locally on the same host. Create one service VM for every AHV host in the cluster. AHV hosts direct the traffic through a service chain for individual VMs, entire AHV networks, or using Flow Network Security rules. However, you must first create the service chain.

You can create and manage service chains as a part of a solution packaged by a Nutanix Partner. These solutions integrate with AHV, allowing you to create and manage the service chains, and redirect the traffic as required for the service VM to function.

Firewalls, intrusion detection, or other packet-capture and analysis systems services are examples that might effectively use service chaining.

For more information about service chains, see KB-12833.

Traffic Mirroring on AHV Hosts

Traffic Mirroring enables you to mirror traffic from the interfaces of the AHV hosts to the virtual NIC (vNIC) of guest VMs. Traffic Mirroring mirrors the packets from a set of source ports to a set of destination ports. You can mirror inbound, outbound, or bidirectional traffic flowing on a set of source ports. You can then use the mirrored traffic for security analysis and to gain visibility of traffic flowing through the set of source ports. Traffic Mirroring is a useful tool for troubleshooting packets and necessary for compliance.

> **Important:** Configuring the Traffic Mirroring session on an AHV host using aCLI is disabled if the cluster is registered to Prism Central. Nutanix recommends that you create the Traffic Mirroring session on Prism Central. For more information, see Creating a Traffic Mirroring Session section in *Prism Central Infrastructure Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1385

VLAN Subnets (VLAN constructs on the Network Controller stack for Flow Virtual Networking on Prism Central) support Traffic Mirroring. For information on VLAN Subnets, see Network Types in the *Flow Virtual Networking Guide*.

AHV supports the following types of source ports in a Traffic Mirroring session:

- A bond port that is already mapped to a virtual switch (VS) such as vs0, vs1, or any other VS you have created.
- A non-bond port that is already mapped to a VS such as vs0, vs1, or any other VS you have created.
- An uplink port that is not assigned to any VS or bridge on the host.
- A virtual port attached to a VM.

Important Considerations

Consider the following before you configure Traffic Mirroring on AHV hosts:

- AHV supports mirroring of traffic from physical and virtual interfaces. Therefore, a source port could be physical or virtual interfaces.
- AHV supports Traffic Mirroring to destination guest VMs running on the same AHV host (to which the source ports belong) or on a remote AHV host.
- The Traffic Mirroring sessions and traffic forwarding are independent of the security policies configured on the Traffic Mirroring source and destination VMs.
- AHV supports different types of source ports in one session. For example, you can create a session with br0-up (bond port) and eth5 (single uplink port) on the same host as two different source ports in the same session. You can even have two different bond ports in the same session.
- AHV does not support Traffic Mirroring from a member of a bond port. For example, if you have a bond with eth0 and eth1in virtual switch vs0, you cannot create a Traffic Mirroring session with either eth0 or eth1 as the source port.
- You cannot create a Traffic Mirroring session on an AHV host that is in the maintenance mode.
- Delete the Traffic Mirroring session before you delete the Traffic Mirroring destination VM or vNIC. Otherwise, the state of the Traffic Mirroring session is displayed as an error.
- If you move the uplink interface to another virtual switch, the Traffic Mirroring session fails. The system does not generate an alert in this situation.
- TCP Segmentation Offload can coalesce multiple packets belonging to the same TCP stream into a single one before being delivered to the Traffic Mirroring destination VM. With TCP Segmentation Offload enabled, there can be a difference between the number of packets received on the uplink interface and packets forwarded to the Traffic Mirroring destination VM (session packet count <= uplink interface packet count). However, the byte count at the Traffic Mirroring destination VM is closer to the number at the uplink interface.
- All the source and destination entities must run on the same AHV host. If you migrate a destination VM, delete a vNIC, or a physical port is down, the Traffic Mirroring session displays an error status.
- If all vNICs are migrated to the same host, the Traffic Mirroring session displays active status. However, if the session has physical NICs (pNICs), the Traffic Mirroring session displays an error status.
- You cannot enable or disable the Traffic Mirror sessions using aCLI.
- You cannot configure the direction of the traffic if the ports are not managed by Open vSwitch (OVS).
- Traffic mirroring is disabled if a cluster is connected to AWS and Azure.
- You can select source VM vNIC for a single Traffic Mirroring session.
- You can select destination VM vNIC for a single Traffic Mirroring session.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1386

Traffic Mirroring Session Scale

Traffic Mirroring session supports the following scale:

Table 9: Traffic Mirroring Session Scale

Entities	Scale
Source ports or entities	4 entities per Traffic Mirroring session
Destination ports or entities	2 entities per Traffic Mirroring session
Maximum number of Traffic Mirror sessions	2,000 per cluster
Maximum number of Active Sessions	2 per host

Nutanix Recommendations for Traffic Mirroring

The following table provides the Nutanix recommendations for a successful Traffic Mirroring session based on the Traffic Mirroring setup criteria:

Table 10: Nutanix Recommendations - Traffic Mirroring

Traffic Mirroring Setup Criteria	Applicable AOS Release	Condition for successful Traffic Mirroring session	Nutanix Recommendations
Source: Host NICs and bonds *Destination*: VM (Traffic Mirroring Destination VM/ Monitoring VM)	AOS 6.0 and later	The Traffic Mirroring destination VM (monitoring VM) must run on the same AHV host where the source ports are located.	Create or modify the Traffic Mirroring destination VM as an agent VM so that it is not migrated from the host. For information on how to create or modify a VM as an agent VM, see Creating a VM (AHV) on page 112or Managing a VM (AHV) on page 117.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1387

Traffic Mirroring Setup Criteria	Applicable AOS Release	Condition for successful Traffic Mirroring session	Nutanix Recommendations
Source: VM (Source VMs / Guest VMs) *Destination*: VM (Traffic Mirroring Destination VM/ Monitoring VM) **Note:** • VM, Host NICs, and bonds can co-exist as sources, however the system supports up to a maximum of 4 sources and 2 Traffic Mirroring destination VMs in a Traffic Mirroring session. • VM with only *kHostNic* and *kVmNic* types are supported and VM with *kDirectNIC* type is not supported.	AOS 6.5.2 and later	The Traffic Mirroring destination VM (monitoring VM) must run on the same AHV host where the source VMs are located.	Set the VM-Host affinity policy for both source VMs (guest VMs) and Traffic Mirroring destination VM with the same host. For information on affinity policies, see VM-Host Affinity Policies on page 160. For information on how to create a VM-Host affinity policy, see Creating a VM (AHV) on page 112or Managing a VM (AHV) on page 117. This helps you to have both guest VMs and Traffic Mirroring destination VM always reside on the same host when any of the following VM migration scenario occurs: • VM migration to another host due to an HA event. • VM migration to another host due to Nutanix admin-initiated change in host in VM-Host affinity policies for both source and Traffic Mirroring destination VM. After both source VMs and destination VMs migrate to the same host, the system restores the Traffic Mirroring session.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1388

Traffic Mirroring Setup Criteria	Applicable AOS Release	Condition for successful Traffic Mirroring session	Nutanix Recommendations
Source: VM (Source VMs / Guest VMs) *Destination*: VM (Traffic Mirroring Destination VM/ Monitoring VM) **Note:** • VM, Host NICs, and bonds can co-exist as sources, however the system supports up to a maximum of 4 sources and 2 Traffic Mirroring destination VMs in a Traffic Mirroring session. • VM with only *kHostNic* and *kVmNic* types are supported and VM with *kDirectNIC* type is not supported.	AOS 6.8 and later	The Traffic Mirroring destination VM (monitoring VM) might run on the same or different AHV hosts, from the AHV host(s) that the source VMs are located. If the list of sources includes Host NICs and bonds, then only the destination VMs that are located on the same AHV host where the source host NICs/bonds are located, receive the mirrored traffic.	None

Configuring Traffic Mirroring on an AHV Host

To configure Traffic Mirroring on an AHV host, create a Traffic Mirroring destination vNIC where you assign that vNIC to a guest VM (Traffic Mirroring destination VM). After you create the vNIC, create a Traffic Mirroring session specifying the source and destination ports between which you want to run the Traffic Mirroring session.

Before you begin

Ensure that the following prerequisites are met before you configure Traffic Mirroring on AHV host:

- Configuring the Traffic Mirroring session on an AHV host using aCLI is disabled if the cluster is registered to Prism Central. Nutanix recommends that you create the Traffic Mirroring session on Prism Central. For more information, see Creating a Traffic Mirroring Session section in *Prism Central Infrastructure Guide*.
- The guest VM that you want to configure as the Traffic Mirroring destination VM (monitoring VM) is created.
- The Nutanix recommendations described in Nutanix Recommendations for Traffic Mirroring on page 92 are followed.

Procedure

To configure Traffic Mirroring on an AHV host, perform the following steps:

1. Log on to a Controller VM in the cluster with SSH.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1389

2. Determine the name and UUID of the guest VM that you want to configure as the Traffic Mirroring destination VM.

```
nutanix@cvm$ acli vm.list
```

Example:

```
nutanix@cvm$ acli vm.list
VM name                 VM UUID
traffic-mirror-dest-VM  85abfdd5-7419-4f7c-bffa-8f961660e516
```

In this example, **traffic-mirror-dest-VM** is the name and **85abfdd5-7419-4f7c-bffa-8f961660e516** is the UUID of the guest VM.

> **Note:** If you delete the Traffic Mirroring destination VM without deleting the Traffic Mirroring session that you created with this Traffic Mirroring destination VM, the Traffic Mirroring session State displays **kError**.

3. Create a Traffic Mirroring destination vNIC for the guest VM.

```
nutanix@cvm$ acli vm.nic_create vm-name type=kSpanDestinationNic
```

Replace *vm-name* with the name of the guest VM on which you want to configure Traffic Mirroring session.

> **Note:** Do not include any other parameter when you are creating a Traffic Mirroring destination vNIC.

Example:

```
nutanix@cvm$ acli vm.nic_create traffic-mirror-dest-VM type=kSpanDestinationNic
NicCreate: complete
```

> **Note:** If you delete the Traffic Mirroring destination vNIC without deleting the Traffic Mirroring session that you created with this Traffic Mirroring destination vNIC, the Traffic Mirroring session State displays **kError**.

4. Determine the MAC address of the vNIC.

```
nutanix@cvm$ acli vm.nic_get vm-name
```

Replace *vm-name* with the name of the guest VM to which you assigned the vNIC.

Example:

```
nutanix@cvm$ acli vm.nic_get traffic-mirror-VM
50:6b:8d:de:c6:44 {
  connected: True
  mac_addr: "50:6b:8d:de:c6:44"
  network_type: "kNativeNetwork"
  type: "kSpanDestinationNic"
  uuid: "75e1582f-cb33-4b69-bd00-c0657cbc716a"
}
50:6b:8d:8b:2c:94 {
  connected: True
  mac_addr: "50:6b:8d:8b:2c:94"
  network_name: "vlan.124"
  network_type: "kNativeNetwork"
  network_uuid: "5128e6bf-3253-4db7-ab3b-c197a1b881eb"
  type: "kNormalNic"
  uuid: "ac752ec9-be79-4774-8ea9-a9ea7ea5e956"
  vlan_mode: "kAccess"
}
```

Note that the MAC address (value of **mac_addr**) of the vNIC for which **type** is set to **kSpanDestinationNic**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1390

5. Determine the UUID of the host whose traffic you want to monitor by using Traffic Mirroring.

```
nutanix@cvm$ acli host.list
```

6. Create a Traffic Mirroring session based on the following Traffic Mirroring setup criteria:

> **Note:** VM, host NICs, and bonds can co-exist as sources, however the system supports a maximum of 4 sources and 2 Traffic Mirroring destination VMs in a Traffic Mirroring session.

Table 11: Traffic Mirroring Session Creation

Traffic Mirroring Setup Criteria	Traffic Mirroring Session Creation Command

Source: Host NICs and bonds
Destination: VM (Traffic Mirroring Destination VM/ Monitoring VM)
	Run the following command:
	`nutanix@cvm$ acli net.create_traffic_mirror traffic-mirror-session-name description="description-text" source_list=\{uuid=host-uuid,type=kHostNic,identifier=source-port-name,direction=traffic-type} dest_list=\{uuid=vm-uuid,type=kVmNic,identifier=vnic-mac-address}`
	For example,
	`nutanix@cvm$ acli net.create_traffic_mirror traffic-mirror-1 description="traffic mirror session 1" source_list=\{uuid=492a2bda-ffc0-486a-8bc0-8ae929471714,type=kHostNic,identifier=br0-up,direction=kBiDir} dest_list=\{uuid=85abfdd5-7419-4f7c-bffa-8f961660e516,type=kVmNic,identifier=50:6b:8d:de:c6:44}`

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1391

Traffic Mirroring Setup Criteria	Traffic Mirroring Session Creation Command

Source: VM (Source VMs / Guest VMs)
Destination: VM (Traffic Mirroring Destination VM/ Monitoring VM)
	Run the following command:
	`nutanix@cvm$ acli net.create_traffic_mirror traffic-mirror-session-name description="description-text" source_list=\{uuid=source-vm-uuid,type=kVmNic,identifier=source-vnic-mac-address,direction=traffic-type} dest_list=\{uuid=vm-uuid,type=kVmNic,identifier=vnic-mac-address}`
	For example,
	`nutanix@cvm$ acli net.create_traffic_mirror traffic-mirror-1 description="traffic mirror session 1" source_list=\{uuid= dc2aef46-c326-4bdd-a9da-9f87e972ea3d,type= kVmNic,identifier= 50:6b:8d:d1:93:ba,direction=kBiDir} dest_list=\{uuid=85abfdd5-7419-4f7c-bffa-8f961660e516,type=kVmNic,identifier=50:6b:8d:de:c6:44}`

Replace the variables mentioned in the command for the following parameters with their appropriate values:

- **traffic-mirror-session-name**: Replace *`traffic-mirror-session-name`* with a name for the session.
- **description** (Optional): Replace *`description-text`* with a description for the session.

  Note:

  All *`source_list`* and *`dest_list`* parameters are mandatory inputs. These parameters do not have default values. Provide an appropriate value for each parameter.

Source list parameters:

- **uuid**:
  - Replace *`host-uuid`* with the UUID of the host whose traffic you want to monitor by using Traffic Mirroring. (determined in *step 5*).
  - Replace *`source-vm-uuid`* with the UUID of the VM whose traffic you want to monitor by using Traffic Mirroring. You can use the same command as indicated in *Step 2* using the source VM name.
- **type**:
  - Specify *kHostNic* as the type if the source is Host NIC or bond.
  - Specify *kVmNic* as the type if source is a VM
- **identifier**:
  - Replace *`source-port-name`* with name of the source port whose traffic you want to mirror. For example, br0-up, eth0, or eth1.
  - Replace *`source-vnic-mac-address`* with the MAC address of the source VM for which you want to mirror the traffic. You can use the same command as described in step 4 using the source VM name.
- **direction**: Replace *`traffic-type`* with **kIngress** if you want to mirror inbound traffic, **kEgress** for outbound traffic, or **kBiDir** for bidirectional traffic.

Destination list parameters:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1392

- **uuid**: Replace *vm-uuid* with the UUID of the guest VM that you want to configure as the Traffic Mirroring destination VM. (determined in *step 2*).
- **type**: Specify *kVmNic* as the type. Only the *kVmNic* type is supported in this release.
- **identifier**: Replace *vnic-mac-address* with the MAC address of the destination port where you want to mirror the traffic (determined in step 4).

  Note: The syntax for **source_list** and **dest_list** is as follows:

  source_list/dest_list=[{key1=value1,key2=value2,..}]

  Each pair of curly brackets includes the details of one source or destination port with a comma-separated list of the key-value pairs. There must not be any space between two key-value pairs and commas in-between the two key-value pairs.

  One Traffic Mirroring session supports up to 2 source and 2 destination ports. If you want to include an extra port, separate the curly brackets with a semicolon (no space) and list the key-value pairs of the second port in the other curly bracket.

7. Display the list of all Traffic Mirroring sessions running on a host.

```
nutanix@cvm$ acli net.list_traffic_mirror
```

   Example:

```
nutanix@cvm$ acli net.list_traffic_mirror
Name              UUID                                  State
traffic-mirror-1  69252eb5-8047-4e3a-8adc-91664a7104af  kActive
```

   Possible values for State are:

   - *kActive*: Denotes that the Traffic Mirroring session is active.
   - *kError*: denotes that there is an error and the configuration is not working. For example, if there are two sources and one source is down, the State of the session is displayed as *kError*.

8. Display the details of a Traffic Mirroring session.

```
nutanix@cvm$ acli net.get_traffic_mirror traffic-mirroring-session-name
```

   Replace traffic-mirroring-session-name with the name of the Traffic Mirroring session whose details you want to view.

   See the following example where source NIC is a physical interface (`source_list` has `nic_type` listed as `"kHostNic"`):

```
nutanix@cvm$ acli net.get_traffic_mirror traffic-mirror-1
traffic-mirror-1 {
  config {
    datapath_name: "s6925"
    description: "traffic mirror session 1"
    destination_list {
      nic_type: "kVmNic"
      port_identifier: "50:6b:8d:de:c6:44"
      uuid: "85abfdd5-7419-4f7c-bffa-8f961660e516"
    }
    name: "traffic-mirror-1"
    session_uuid: "69252eb5-8047-4e3a-8adc-91664a7104af"
    source_list {
      direction: "kBiDir"
      nic_type: "kHostNic"
      port_identifier: "br0-up"
      uuid: "492a2bda-ffc0-486a-8bc0-8ae929471714"
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1393

```
    }
  }
  stats {
    name: "traffic-mirror-1"
    session_uuid: "69252eb5-8047-4e3a-8adc-91664a7104af"
    state: "kActive"
    stats_list {
      tx_byte_cnt: 67498
      tx_pkt_cnt: 436
    }
  }
}
```

See the following example where source NIC is a virtual interface (`source_list` has `nic_type` listed as `"kVmNic"`):

```
nutanix@cvm$ acli net.get_traffic_mirror traffic-brAtlas
traffic-session-name {
 config {
  datapath_name: "s5812"
  destination_list {
   nic_type: "kVmNic"
   port_identifier: "50:6b:8d:95:11:00"
   uuid: "c6234cbf-c6e8-4a9c-1234-b8ade24f"
  }
  name: "traffic-brAtlas"
  session_uuid: "58122427-0302-4e61-8185-13abaad2a8d8"
  source_list {
   direction: "kBiDir"
   inactive: False
   nic_type: "kVmNic"
   port_identifier: "50:6b:8d:ab:cd:21"
   uuid: "1a70d859-253b-43d6-ac17-de78d854d925"
  }
 }
 stats {
  name: "traffic-brAtlas"
  session_uuid: "58122427-0302-4e61-8185-13abaad2a8d8"
  state: "kActive"
  state_message: ""
  stats_list {
   tx_byte_cnt: 0
   tx_pkt_cnt: 0
  }
 }
}
```

> **Note:** The value of the **datapath_name** field in the Traffic Mirroring session configuration is a unique key that identifies the Traffic Mirroring session. You need the unique key to correctly identify the Traffic Mirroring session for troubleshooting reasons.

Updating a Traffic Mirroring Session

You can update any of the details of a Traffic Mirroring session.

About this task

When you are updating a Traffic Mirroring session:

- Specify the values of the parameters you want to update.
- Add the remaining parameters again as specified originally when you created the Traffic Mirroring session.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1394

For example, if you want to change only the name and description, specify the updated name and description and then add the `source_list` and `dest_list` parameters exactly as they were before updating.

> **Important:** Updating the Traffic Mirroring session on an AHV host through aCLI is disabled if the cluster is registered to Prism Central. Nutanix recommends creating Traffic Mirroring sessions from Prism Central user interface or v4 API.

Perform the following procedure to update a Traffic Mirroring session:

Procedure

1. Log on to a Controller VM in the cluster with SSH.
2. Update the Traffic Mirroring session.

```
nutanix@cvm$ acli net.update_traffic_mirror traffic-mirroring-
session-name description="description-text" source_list=\{uuid=host-
uuid,type=kHostNic,identifier=source-port-name,direction=traffic-type} dest_list=
\{uuid=vm-UUID,type=kVmNic,identifier=vNIC-mac-address}
```

The update command includes the same parameters as the create command. See Configuring Traffic Mirroring on an AHV Host on page 94 for more information.

Example:

```
nutanix@cvm$ acli net.update_traffic_mirror traffic-mirror-1
 name=traffic-mirror_br0_to_traffic-mirror_dest description="traffic
 mirror from br0-up to traffic-mirror-dest VM" source_list=
\{uuid=492a2bda-ffc0-486a-8bc0-8ae929471714,type=kHostNic,identifier=br0-
up,direction=kBiDir} dest_list=\{uuid=85abfdd5-7419-4f7c-
bffa-8f961660e516,type=kVmNic,identifier=50:6b:8d:de:c6:44}
SpanUpdate: complete

nutanix@cvm$ acli net.list_traffic_mirror
Name                                        UUID
 State
traffic-mirror_br0_to_traffic-mirror_dest  69252eb5-8047-4e3a-8adc-91664a7104af
 kActive

nutanix@cvm$ acli net.get_traffic_mirror traffic_mirror_br0_to_traffic_mirror_dest
traffic-mirror_br0_to_traffic-mirror_dest {
  config {
    datapath_name: "s6925"
    description: "traffic mirror from br0-up to traffic-mirror-dest VM"
    destination_list {
      nic_type: "kVmNic"
      port_identifier: "50:6b:8d:de:c6:44"
      uuid: "85abfdd5-7419-4f7c-bffa-8f961660e516"
    }
    name: "traffic-mirror_br0_to_traffic-mirror_dest"
    session_uuid: "69252eb5-8047-4e3a-8adc-91664a7104af"
    source_list {
      direction: "kBiDir"
      nic_type: "kHostNic"
      port_identifier: "br0-up"
      uuid: "492a2bda-ffc0-486a-8bc0-8ae929471714"
    }
  }
  stats {
    name: "traffic-mirror_br0_to_traffic-mirror_dest"
    session_uuid: "69252eb5-8047-4e3a-8adc-91664a7104af"
    state: "kActive"
    stats_list {
      tx_byte_cnt: 805705
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1395

```
      tx_pkt_cnt: 4792
    }
  }
}
```

In this example, only the name and description are updated. However, complete details of the source and destination ports are included in the command exactly as they were before the update.

If you want to change the name of a Traffic Mirroring session, specify the existing name first, and then include the new name by using the “name=” parameter as shown in this example.

Deleting a Traffic Mirroring Session

Delete the Traffic Mirroring session if you want to disable Traffic Mirroring on an AHV host. Nutanix recommends that you delete the Traffic Mirroring session associated with a Traffic Mirroring destination VM or Traffic Mirroring destination VNIC.

About this task

> **Important:** Deleting the Traffic Mirroring session on an AHV host through aCLI is disabled if the cluster is registered to Prism Central. Nutanix recommends creating Traffic Mirroring sessions from Prism Central user interface or v4 API.

To delete a Traffic Mirroring session, do the following:

Procedure

1. Log on to a Controller VM in the cluster with SSH.
2. Delete the Traffic Mirroring session.

   ```
   nutanix@cvm$ acli net.delete_traffic_mirror traffic-mirror-session-name
   ```

   Replace *traffic-mirror-session-name* with the name of the Traffic Mirroring session you want to delete.

Traffic Mirroring Session Alerts

Prism Element web console generates the Traffic Mirroring session alerts for the following inconsistent state scenarios:

> **Note:** For more information about the Alerts generated in Prism Element web console, see Prism Web Console Alerts and Events Reference Guide .

Table 12: Traffic Mirror Session Alerts List

Alert Title	Possible Cause
Inconsistent SPAN Session State Detected	This alert occurs when a VM NIC is removed from the destination VM.
Inconsistent SPAN Session State Detected	This alert occurs when a destination VM is migrated to another host.
Inconsistent SPAN Session State Detected	This alert occurs when a destination VM is powered off.

Virtual Switch Security with MAC Addresses

This section describes how the Virtual Switch treats MAC addresses of VMs in different configurations.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1396

Forged MAC Transmits and MAC Address Changes

This section describes the forged MAC transmits and MAC address changes for Virtual Switch security.

A forged MAC is when a VM sends traffic from a MAC address that is not assigned on the virtual NIC. This configuration is commonly used for load balancers and other highly available VMs that might share a single MAC between several VMs and move the MAC to pass service to another VM.

A MAC address change is when a VM starts using a new MAC address than the one it was using previously.

VLANs

In the default AHV-based Basic VLANs, or VLAN Basic Subnets, and network-controller backed VLAN Subnets, VMs are allowed to send traffic from any MAC address, even to those MAC addresses that are not assigned to a VM NIC. In VLANs, VMs can use any MAC address required, and change MAC addresses.

Flow Virtual Networking VPC

In the Flow Virtual Networking VPC, VMs are not allowed to send traffic from any MAC address other than the one they are assigned on the virtual NIC. This can cause issues with VMs, such as load balancer VMs, that attempt to send traffic from MAC addresses that are not assigned to them. For such use cases, consider alternate load balancing mechanisms other than MAC address sharing, or contact Nutanix Support for options.

MAC Address Prefix

You can avoid duplicate IP addresses in a single-cluster or multi-cluster environment by implementing one of two possible configurations:

- Nutanix recommends that you assign a set of unique VLANs for guest VMs on each AHV cluster. Ensure these VLANs do not overlap with the VLANs on other AHV clusters. Assigning unique VLAN ranges for each cluster reduces the risk of MAC address conflicts. Such an assignment also ensures compliance with the general best practice of maintaining small Layer 2 broadcast domains with limited numbers of endpoints.
- If multiple AHV clusters need to share the same VLAN, or when guest VM MAC addresses need be globally unique among multiple AHV clusters, configure a predefined MAC address prefix for each AHV cluster.

Nutanix does not guarantee unique MAC address assignment by default between Nutanix clusters with VLAN networks.

Sample Design Scenario with Multiple Sites and Clusters

Using locally administered MAC addresses, you can ensure unique MAC addresses for VMs in an environment made up of multiple sites and clusters.

A MAC address is usually a 6-octet hexadecimal address block. The notation for a MAC address is `XX:XX:XX:XX:XX:XX`. In this 6-octet address, the first 3 octets are the organizationally unique identifier (OUI) octets or the MAC address prefix OUI. The second bit of the 1st octet (the first hexadecimal number `XX`) is set to 1 to make the MAC address a locally administered MAC address. The next 3 octets are NIC specific octets, `XX:XX:XX`, represents the useable hexadecimal range for endpoints within each AHV cluster.

> **Note:** Nutanix AHV clusters use the MAC address prefix OUI `50:6B:8D` by default.
>
> By default, Acropolis leader generates MAC address for a VM on AHV. The first 24 bits of the MAC address (OUI) is set to `50-6b-8d` (0101 0000 0110 1101 1000 1101) and are reserved by Nutanix, the 25th bit is set to 1 (reserved by Acropolis leader), the 26th bit to 48th bits are auto generated random numbers.

Consider this sample design of a deployment with three sites and five clusters in each site. Define a unique MAC address prefix for Site1-Cluster1 such as 02:01:01, where:

- 02—Defines the MAC address as a unicast address that is locally administered. This value could be a hexadecimal number defined by X2, X3, X6, X7, XA, XB, or XE series, where X is any valid hexadecimal value such that the

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1397

second binary bit (binary bits being counted from right to left, right most is the first bit) of the binary equivalent of this hexadecimal number `XX` is set to 1 to make the MAC address a locally administered MAC address.

- 01—Used to identify, for example, the site number. This value could be any valid hexadecimal value.
- 01—Used to identify, for example, the AHV cluster within the site. This value could be any valid hexadecimal value

The NIC specific octets, `XX:XX:XX`, are auto-assigned to the VM NICs or the endpoints within each AHV cluster. Thus, for Site1, the clusters would have the following prefixes:

- Site1-Cluster1: 02:01:01
- Site1-Cluster2: 02:01:02
- Site1-Cluster3: 02:01:03
- Site1-Cluster4: 02:01:04
- Site1-Cluster5: 02:01:05

  ... and so on for the other clusters at Site1.

Similarly for Site2, if you define, for example 02:02:01 as the MAC address prefix for the first cluster - Cluster1, you get the series of predefined MAC address prefixes for the clusters and VMs or endpoints in Site2, Cluster1.

- Site2-Cluster1-VM1: 02:02:01:00:00:01
- Site2-Cluster1-VM2: 02:02:01:00:00:02
- ...
- Site2-Cluster1-VM10: 02:02:01:00:00:0A

  ... and so on for the other clusters at Site2.

Adding a MAC Address Prefix

Before you begin

Ensure that you meet the following requirements before you add a MAC address prefix:

- Guest VMs in the cluster do not have any NICs that have MAC addresses with the default prefix.
- Check the #unique_106/unique_106_Connect_42_section_ktr_3mw_1dc.

About this task

Use aCLI to configure the MAC address prefix for a cluster.

Procedure

1. Log on to a Controller VM in your cluster with SSH.
2. Access Acropolis CLI using the `acli` command.

   ```
   nutanix@cvm$ acli
   ```

   The prompt changes to `<acropolis>`.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1398

3. Add the MAC address prefix for the cluster using the following command.

```
<acropolis> net.set_mac_prefix XX:XX:XX
```

> **Note:** Ensure that the VMs in the cluster do not have any NICs that have MAC addresses with the default prefix.

> **Warning:**
>
> Ensure that you do not set the MAC address prefix to `52:6b:8d` as this might lead to a conflict due to one of the guest VMs acquiring `52:6b:8d:00:00:00` IP, which AHV uses internally for packet probing purposes.

Replace *XX:XX:XX* by the MAC address prefix for the cluster.

Using the example discussed in MAC Address Prefix on page 102, the following sample command adds the `02:01:01` as the MAC address prefix for Site1-Cluster1

```
<acropolis> net.set_mac_prefix 02:01:01
```

What to do next

Verify if the MAC address prefix is configured using the `net.get_mac_prefix` command.

The output displays the hexadecimal prefix that you configured.

Using the configuration example, the output would show `"02:01:01"` as follows:

```
<acropolis> net.get_mac_prefix
"02:01:01"
<acropolis>
```

Repeat this procedure to add MAC address prefixes to other clusters that share the same VLAN (defining the common broadcast domain) that you want to avoid duplicate MAC addresses in.

Removing the MAC Address Prefix

You can remove the MAC address prefix. The cluster then uses the default MAC prefix, `"50:6b:8d"`.

Before you begin

Remove the MAC addresses with the configured prefix from the VM NICs in the cluster.

About this task

Use aCLI commands to remove the MAC address prefix for a cluster.

Procedure

1. Log on to a Controller VM in your cluster with SSH.
2. Access Acropolis CLI using the `acli` command.

   ```
   nutanix@cvm$ acli
   ```

   The prompt changes to `<acropolis>`.
3. Remove the MAC address prefix for the cluster using the following command.

   ```
   <acropolis> net.clear_mac_prefix
   ```

   > **Note:** Ensure that the VMs in the cluster do not have any NICs that have MAC addresses with the configured prefix.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1399

What to do next

Verify that the MAC address prefix is removed. When you use the `net.get_mac_prefix` command, the output displays the default MAC address prefix, `"50:6b:8d"`.

```
<acropolis> net.get_mac_prefix
"50:6b:8d"
<acropolis>
```

Enabling RSS Virtio-Net Multi-Queue by increasing the Number of VNIC Queues

Multi-Queue in VirtIO-net enables you to improve network performance for network I/O-intensive guest VMs or applications running on AHV hosts.

About this task

You can enable VirtIO-net multi-queue by increasing the number of VNIC queues. If an application uses many distinct streams of traffic, Receive Side Scaling (RSS) can distribute the streams across multiple VNIC DMA rings. This increases the amount of RX buffer space by the number of VNIC queues (N). Also, most guest operating systems pin each ring to a particular vCPU, handling the interrupts and ring-walking on that vCPU, by that means achieving N-way parallelism in RX processing. However, if you increase the number of queues beyond the number of vCPUs, you cannot achieve extra parallelism.

Following workloads have the greatest performance benefit of VirtIO-net multi-queue:

- VMs where traffic packets are relatively large
- VMs with many concurrent connections
- VMs with network traffic moving:
  - Among VMs on the same host
  - Among VMs across hosts
  - From VMs to the hosts
  - From VMs to an external system
- VMs with high VNIC RX packet drop rate if CPU contention is not the cause

You can increase the number of queues of the AHV VM VNIC to allow the guest OS to use multi-queue VirtIO-net on guest VMs with intensive network I/O. Multi-Queue VirtIO-net scales the network performance by transferring packets through more than one Tx/Rx queue pair at a time as the number of vCPUs increases.

Nutanix recommends that you be conservative when increasing the number of queues. Do not set the number of queues larger than the total number of vCPUs assigned to a VM. Packet reordering and TCP retransmissions increase if the number of queues is larger than the number vCPUs assigned to a VM. For this reason, start by increasing the queue size to 2. The default queue size is 1. After making this change, monitor the guest VM and network performance. Before you increase the queue size further, verify that the vCPU usage has not dramatically or unreasonably increased.

Perform the following steps to make more VNIC queues available to a guest VM. See your guest OS documentation to verify if you must perform extra steps on the guest OS to apply the additional VNIC queues.

> **Note:** You must shut down the guest VM to change the number of VNIC queues. Therefore, make this change during a planned maintenance window. The VNIC status might change from Up->Down->Up or a restart of the guest OS might be required to finalize the settings depending on the guest OS implementation requirements.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1400

Before you begin

(Optional) Nutanix recommends that you perform the following checks before you enable RSS Virtio-Net Multi-Queue by increasing the number of VNIC queues:

- AHV and AOS are running the latest version.
- AHV guest VMs are running the latest version of the Nutanix VirtIO driver package.

  For RSS support, ensure you are running Nutanix VirtIO 1.1.6 or later. For more information on Nutanix VirtIO , see Nutanix VirtIO for Windows on page 140.

Procedure

To set up a multi-queue virtio-net connection, perform the following steps:

1. Determine the exact name of the guest VM for which you want to change the number of VNIC queues using the following command:

   ```
   nutanix@cvm$ acli vm.list
   ```

   An output similar to the following is displayed:

   ```
   nutanix@cvm$ acli vm.list
   VM name          VM UUID
   ExampleVM1       a91a683a-4440-45d9-8dbe-xxxxxxxxxxxx
   ExampleVM2       fda89db5-4695-4055-a3d4-xxxxxxxxxxxx
   ...
   ```

2. Determine the MAC address of the VNIC and confirm the current number of VNIC queues using the following command:

   ```
   nutanix@cvm$ acli vm.nic_get VM-name
   ```

   Replace *VM-name* with the name of the VM.

   An output similar to the following is displayed:

   ```
   nutanix@cvm$ acli vm.nic_get VM-name
   ...
   mac_addr: "50:6b:8d:2f:zz:zz"
   ...
   (queues: 2)    <- If there is no output of 'queues', the setting is default (1
    queue).
   ```

   Note: AOS defines queues as the maximum number of Tx/Rx queue pairs (default is 1).

3. Determine the total count of vCPUs assigned to the VM using the following command:

   ```
   nutanix@cvm$ acli vm.get VM-name | grep num.*vcpu
   ```

   Replace *VM-name* with the name of the VM.

   An output similar to the following is displayed:

   ```
   num_cores_per_vcpu: 4
       num_vcpus: 1
   ```

   The total count of vCPUs assigned to the VM is calculated as - *num_vcpus* * *num_cores_per_vcpu*. In the above output, the total count of vCPUs assigned to the VM is 1 * 4 = 4.

4. Shut down the guest VM using the following command:

   ```
   nutanix@cvm$ acli vm.shutdown VM-name
   ```

   Replace *VM-name* with the name of the VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1401

5. Increase the number of VNIC queues.

```
nutanix@cvm$acli vm.nic_update VM-name vNIC-MAC-address queues=N
```

Replace *VM-name* with the name of the guest VM, *vNIC-MAC-address* with the MAC address of the VNIC, and *N* with the number of queues.

> **Note:** *N* must be less than or equal to the total count of vCPUs assigned to the guest VM.

6. Start the guest VM using the following command:

```
nutanix@cvm$ acli vm.on VM-name
```

Replace *VM-name* with the name of the VM.

7. Confirm in the guest OS documentation if any additional steps are required to enable multi-queue in VirtIO-net.

> **Note:** Microsoft Windows has RSS enabled by default.

For example, for RHEL and CentOS VMs, perform the following steps:

a. Log on to the guest VM.

b. Confirm if irqbalance.service is active or not using the following command:

```
uservm# systemctl status irqbalance.service
```

An output similar to the following is displayed:

```
irqbalance.service - irqbalance daemon
   Loaded: loaded (/usr/lib/systemd/system/irqbalance.service; enabled; vendor
 preset: enabled)
   Active: active (running) since Tue 2020-04-07 10:28:29 AEST; Ns ago
```

c. Start irqbalance.service if it is not active using the following command:

> **Note:** It is active by default on CentOS VMs. You might have to start it on RHEL VMs.

```
uservm# systemctl start irqbalance.service
```

d. Run the following command:

```
uservm# ethtool -L ethX combined M
```

Replace:

- *M* with the number of VNIC queues.
- *ethX* with the required ethernet interface. For example, eth1.

Note the following caveat from the RHEL 7 *Virtualization Tuning and Optimization Guide: 5.4. NETWORK TUNING TECHNIQUES* document:

Currently, setting up a multi-queue virtio-net connection can have a negative effect on the performance of outgoing traffic. Specifically, this might occur while sending packets under 1,500 bytes over the Transmission Control Protocol (TCP) stream.

8. Monitor the VM performance to make sure that the expected network performance increase is observed and that the guest VM vCPU usage is not dramatically increased to impact the application on the guest VM.

For assistance with the steps described in this document, or if these steps do not resolve your guest VM network performance issues, contact Nutanix Support.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1402

Changing the IP Address, Network Mask, or Gateway of an AHV Host

Use this procedure to change the IP address, network mask, or gateway of an AHV host.

Before you begin

Ensure that all Controller VMs and hypervisor hosts are on the same subnet.

About this task

To change the IP address, netmask, or gateway of an AHV host, follow these steps:

Procedure

1. Set up the environment. For more information, see Setting up the Environment to change the IP Address, Network Mask, or Gateway of an AHV Host on page 110.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1403

2. Edit the settings of port br0, which is the internal port on the default bridge br0.

   a. Log on to the host console as `root` through IPMI.

   b. Update entries for host IP address, netmask, and gateway using network manager command line interface (nmCLI):

   ```
   root@ahv# nmcli con modify ovs-port-<bridge-name> ipv4.addresses <new-ip-address>/
   <prefix-length> ipv4.gateway <new-gateway-ip>
   ```

   - Replace `<bridge-name>` with the OVS bridge port. For example, br0.
   - Replace `<new-ip-address>/<prefix-length>` with the IP address of the hypervisor host and subnet size. For example, for host IP address 10.10.128.10 and subnet mask 255.255.255.0, the `<new-ip-address>/<prefix-length>` is 10.10.128.10/24.
   - Replace `<new-gateway-ip>` with the gateway address for host IP address.

   For example,

   ```
   root@ahv# nmcli con modify ovs-port-br0 ipv4.addresses 10.46.144.132/21
    ipv4.gateway 10.46.144.1
   ```

   c. Start the new connection.

   ```
   root@ahv# nmcli con up ovs-port-<bridge-name>
   ```

   Replace `<bridge-name>` with the OVS bridge port, for example, br0.

   d. Assign the impacted host to a VLAN and confirm VLAN tagging on port br0.

   ```
   root@ahv# nmcli con modify ovs-port-<bridge-name> ovs-port.tag <new-vlan-tag>
   ```

   ```
   root@ahv# nmcli -g ovs-port.tag con show ovs-port-<bridge-name>
   ```

   Replace `<new-vlan-tag>` with the VLAN tag for the host.

   Replace `<bridge-name>` with the default bridge br0.

   e. Start the new connection.

   ```
   root@ahv# nmcli con up ovs-port-<bridge-name>
   ```

   Replace `<bridge-name>` with the OVS bridge port. For example, br0.

   f. Log on to the host console as root.

   You can access the hypervisor host console either through IPMI or by attaching a keyboard and monitor to the node.

   g. Verify network connectivity by pinging the gateway, other CVMs, and AHV hosts.

   > **Note:** Repeat the earlier steps for every host for which you want to change the IP address.

3. Log on to the Controller VM that is running on the AHV host whose IP address you changed and restart Genesis.

   ```
   nutanix@cvm$ genesis restart
   ```

   If the restart is successful, output similar to the following is displayed:

   ```
   Stopping Genesis pids [1933, 30217, 30218, 30219, 30241]
   Genesis started on pids [30378, 30379, 30380, 30381, 30403]
   ```

   For information on how to log on to a Controller VM, see Controller VM Access on page 15.

   Genesis takes a few minutes to restart.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1404

4. From any CVM in the cluster, restart the Acropolis service.

```
nutanix@cvm$ cluster start
```

5. Obtain the updated IP address of the node (AHV host).

```
nutanix@cvm$ acli host.list
```

6. Exit the node from the maintenance mode:

```
nutanix@cvm$ acli host.exit_maintenance_mode <Host_IP>
```

Replace `<Host_IP>` with either the updated IP address or host name of the AHV host to be removed from maintenance mode.

7. Verify if the host is exited from maintenance mode:

```
nutanix@cvm$ acli host.get <Host_IP>
```

Replace `<Host_IP>` with either the IP address or hostname of the AHV host for which you are verifying the maintenance mode exit status.

In the output that is displayed, ensure that node_state equals kAcropolisNormal or AcropolisNormal and schedulable equals True.

8. Verify if the IP address of the hypervisor host has changed by running the following nCLI command from any CVM other than the one in the maintenance mode.

```
nutanix@cvm$ ncli host list
```

An output similar to the following is displayed:

```
nutanix@cvm$ ncli host list
    Id                        : aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee::1234
    Uuid                      : ffffffff-gggg-hhhh-iiii-jjjjjjjjjjj
    Name                      : XXXXXXXXXX-X
    IPMI Address              : X.X.Z.3
    Controller VM Address     : X.X.X.1
    Hypervisor Address        : X.X.Y.4 <- New IP Address
...
```

9. Start the guest VMs from the Prism Element web console.

Setting up the Environment to change the IP Address, Network Mask, or Gateway of an AHV Host

About this task

Use this procedure to set up the environment to change the IP Address, network mask, or gateway of an AHV host.

Procedure

Perform the following actions to set up the environment:

> **Caution:** You must perform these actions in the exact order indicated in this document.

1. Verify the cluster health by following the instructions in Verifying the Cluster Health.

> **Note:** Do not proceed if the cluster cannot tolerate failure of at least one node.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1405

2. Shut down all guest VMs in the cluster from within the guest OS or from the Prism Element web console.
   For more information, see Managing a VM (AHV) on page 117.

3. Put the node into the maintenance mode:

   > **Note:** You can change the IP address of multiple AHV hosts at once. For this, you must put all the target nodes in maintenance mode

   a. Use SSH to log on to a Controller VM in the cluster.

   b. Determine the IP address of the node to be put into maintenance mode:

      ```
      nutanix@cvm$ acli host.list
      ```

      Note the value of Hypervisor IP (Host IP) for the node you want to put in the maintenance mode.

   c. Put the node in maintenance mode:

      ```
      nutanix@cvm$ acli host.enter_maintenance_mode <Host_IP>
      ```

      Replace `<Host_IP>` with either the IP address or hostname of the AHV host you want to shut down.

   d. Verify that the host is in maintenance mode:

      ```
      nutanix@cvm$ acli host.get <Host_IP>
      ```

      Replace `<Host_IP>` with either the IP address or hostname of the AHV host for which you want to verify the maintenance mode exit status.

      In the output that is displayed, ensure that node_state equals EnteredMaintenanceMode and schedulable equals False

4. Stop the Acropolis service on all the CVMs in the cluster.

   ```
   nutanix@cvm$ allssh genesis stop acropolis
   ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1406

VIRTUAL MACHINE MANAGEMENT

The following topics describe various aspects of virtual machine management in an AHV cluster.

Supported Guest VM Types for AHV

The compatibility matrix available on the Nutanix Support portal includes the latest supported AHV guest VM OSes.

AHV Configuration Maximums

The Nutanix configuration maximums available on the Nutanix support portal includes all the latest configuration limits applicable to AHV. Select the appropriate AHV version to view version specific information.

Creating a VM (AHV)

In AHV clusters, you can create a new virtual machine (VM) through the Prism Element web console.

About this task

> **Note:** Use Prism Central to create a VM with the memory overcommit feature enabled. Prism Element web console does not allow you to enable memory overcommit while creating a VM. If you create a VM using the Prism Element web console and want to enable memory overcommit for it, update the VM using Prism Central and enable memory overcommit in the **Update VM** page in Prism Central. For more information, see Updating a VM through Prism Central information in *Prism Central Infrastructure Guide*.

When creating a VM, you can configure all of its components, such as number of vCPUs and memory, but you cannot attach a volume group to the VM. Attaching a volume group is possible only when you are modifying a VM.

To create a VM, do the following:

Procedure

1. Log in to Prism Element web console.
2. In the VM dashboard, click the **Create VM** button.

   > **Note:** This option does not appear in clusters that do not support this feature.

   The **Create VM** dialog box appears.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1407

3. Do the following in the indicated fields:

   a. **Name**: Enter a name for the VM.

   b. **Description** (optional): Enter a description for the VM.

   c. **Timezone**: Select the timezone that you want the VM to use. If you are creating a Linux VM, select **(UTC) UTC**.

      Note:

      The RTC of Linux VMs must be in UTC, so select the UTC timezone if you are creating a Linux VM.

      Windows VMs preserve the RTC in the local timezone, so set up the Windows VM with the hardware clock pointing to the desired timezone.

   d. **Use this VM as an agent VM**: Select this option to make this VM as an agent VM.

      You can use this option for the VMs that must be powered on before the rest of the VMs (for example, to provide network functions before the rest of the VMs are powered on the host) and must be powered off after the rest of the VMs are powered off (for example, during maintenance mode operations). Agent VMs are never migrated to any other host in the cluster. If an HA event occurs or the host is put in maintenance mode, agent VMs are powered off and are powered on the same host once that host comes back to a normal state.

      If an agent VM is powered off, you can manually start that agent VM on another host and the agent VM now permanently resides on the new host. The agent VM is never migrated back to the original host. Note that you cannot migrate an agent VM to another host while the agent VM is powered on.

   e. **vCPU(s)**: Enter the number of virtual CPUs to allocate to this VM.

   f. **Number of Cores per vCPU**: Enter the number of cores assigned to each virtual CPU.

   g. **Memory**: Enter the amount of memory (in GiB) to allocate to this VM.

4. (For GPU-enabled AHV clusters only) To configure GPU access, click **Add GPU** in the **Graphics** section, and then do the following in the **Add GPU** dialog box:

   For more information, see GPU and vGPU Support on page 205.

   a. To configure GPU pass-through, in **GPU Mode**, click **Passthrough**, select the GPU that you want to allocate, and then click **Add**.

      If you want to allocate additional GPUs to the VM, repeat the procedure as many times as you need to. Make sure that all the allocated pass-through GPUs are on the same host. If all specified GPUs of the type that you

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1408

want to allocate are in use, you can proceed to allocate the GPU to the VM, but you cannot power on the VM until a VM that is using the specified GPU type is powered off.

For more information, see GPU and vGPU Support on page 205.

b. To configure virtual GPU (vGPU) access, in **GPU Mode**, click **virtual GPU**, select a GRID license, and then select a virtual GPU (vGPU) profile from the list.

> **Note:** This option is available only if you have installed the GRID host driver on the GPU hosts in the cluster.
>
> For more information about the NVIDIA GRID host driver installation instructions, see the NVIDIA Grid Host Driver for Nutanix AHV Installation Guide.

You can assign multiple virtual GPU (vGPU) to a VM. A vGPU is assigned to the VM only if a vGPU is available when the VM is starting up.

Before you add multiple vGPUs to the VM, see Multiple Virtual GPU Support on page 209 and Restrictions for Multiple vGPU Support on page 210.

> **Note:** Multiple vGPUs are supported on the same VM only if you select the highest vGPU profile type.

After you add the first vGPU, to add multiple vGPUs, see Adding Multiple vGPUs to the Same VM on page 213.

5. Select one of the following firmware to boot the VM.

» **Legacy BIOS**: Select legacy BIOS to boot the VM with legacy BIOS firmware.

» **UEFI**: Select UEFI to boot the VM with UEFI firmware. UEFI firmware supports larger hard drives, faster boot time, and provides more security features. For more information about UEFI firmware, see UEFI Support for VM on page 187.

If you select UEFI, you can enable the following features:

- **Secure Boot**: Select this option to enable UEFI secure boot policies for your guest VMs. For more information about Secure Boot, see Secure Boot Support for VMs on page 194.
- **Windows Defender Credential Guard**: Select this option to enable the Windows Defender Credential Guard feature of Microsoft Windows operating systems that allows you to securely isolate user credentials from the rest of the operating system. Follow the detailed instructions described in Windows Defender Credential Guard Support in AHV on page 153 to enable this feature.

> **Note:** For information on how to add the virtual TPM, see Securing AHV VMs with Virtual Trusted Platform Module.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1409

6. To attach a disk to the VM, click the **Add New Disk** button.

   The **Add Disk** dialog box appears. Do the following in the indicated fields:

   a. **Type**: Select the type of storage device, **DISK** or **CD-ROM**, from the drop-down list.

      The following fields and options vary depending on whether you choose **DISK** or **CD-ROM**.

   b. **Operation**: Specify the device contents from the drop-down list.

      - Select **Clone from ADSF file** to copy any file from the cluster that can be used as an image onto the disk.
      - Select **Empty CD-ROM** to create a blank CD-ROM device. (This option appears only when **CD-ROM** is selected in the previous field.) A CD-ROM device is needed when you intend to provide a system image from CD-ROM.
      - Select **Allocate on Storage Container** to allocate space without specifying an image. (This option appears only when **DISK** is selected in the previous field.) Selecting this option means you are allocating space only. You have to provide a system image later from a CD-ROM or other source.
      - Select **Clone from Image Service** to copy an image that you have imported by using image service feature onto the disk. For more information about the Image Service feature, see Configuring Images and Image Management in the *Prism Self Service Administration Guide*.

   c. **Bus Type**: Select the bus type from the dropdown list.

      The options displayed in the **Bus Type** dropdown list varies based on the storage device **Type** selected in Step a.

      - For device **Disk**, select from **SCSI**, **SATA**, **PCI**, or **IDE** bus type.
      - For device **CD-ROM**, you can select either **IDE** or **SATA** bus type.

      Note:

      - SCSI bus is the preferred bus type and it is used in most cases. Ensure you have installed the VirtIO drivers in the guest OS. For more information about VirtIO drivers, see Nutanix VirtIO for Windows in *AHV Administration Guide*.
      - For AHV 5.16 and later, you cannot use an IDE device if **Secured Boot** is enabled for **UEFI Mode** boot configuration.

      Caution: Use SATA, PCI, IDE for compatibility purpose when the guest OS does not have VirtIO drivers to support SCSI devices. This may have performance implications. For more information about VirtIO drivers, see Nutanix VirtIO for Windows in *AHV Administration Guide*.

   d. **ADSF Path**: Enter the path to the desired system image.

      This field appears only when **Clone from ADSF file** is selected. It specifies the image to copy. Enter the path name as `/storage_container_name/iso_name.iso`. For example to clone an image from myos.iso in a storage container named crt1, enter /crt1/myos.iso. When a user types the storage container

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1410

name (/*storage_container_name*/), a list appears of the ISO files in that storage container (assuming one or more ISO files had previously been copied to that storage container).

e. **Image**: Select the image that you have created by using the image service feature.
   This field appears only when **Clone from Image Service** is selected. It specifies the image to copy.

f. **Storage Container**: Select the storage container to use from the drop-down list.
   This field appears only when **Allocate on Storage Container** is selected. The list includes all storage containers created for this cluster.

g. **Logical Size (GiB)**: Enter the disk size in GiB.

h. **Index**: Displays **Next Available** by default.

i. When all the field entries are correct, click the **Add** button to attach the disk to the VM and return to the **Create VM** dialog box.

j. Repeat this step to attach additional devices to the VM.

7. To create a network interface for the VM, click the **Add New NIC** button.
   Prism console displays the **Create NIC** dialog box.

   Note: To create or update a Traffic Mirroring destination type VM or vNIC, use command line interface. For more information, see Traffic Mirroring on AHV Hosts on page 90.

   Do the following in the indicated fields:

   a. **Subnet Name**: Select the target virtual LAN from the drop-down list.
      The list includes all defined networks.

      Note: Selecting IPAM enabled subnet from the drop-down list displays the **Private IP Assignment** information that provides information about the number of free IP addresses available in the subnet and in the IP pool.

   b. **Network Connection State**: Select the state for the network that you want it to operate in after VM creation. The options are *Connected* or *Disconnected*.

   c. **Private IP Assignment**: This is a read-only field and displays the following:

      - **Network Address/Prefix**: The network IP address and prefix.
      - **Free IPs (Subnet)**: The number of free IP addresses in the subnet.
      - **Free IPs (Pool)**: The number of free IP addresses available in the IP pools for the subnet.

   d. **Assignment Type**: This is for IPAM enabled network. Select **Assign with DHCP** to assign IP address automatically to the VM using DHCP. For more information, see IP Address Management on page 55 .

   e. When all the field entries are correct, click the **Add** button to create a network interface for the VM and return to the **Create VM** dialog box.

   f. Repeat this step to create additional network interfaces for the VM.

      Note:

      - Nutanix does not recommend configuring multiple clusters to use the same broadcast domain (the same VLAN network), but if you do, configure MAC address prefixes for each cluster to avoid

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1411

duplicate MAC addresses. For information on configuring or removing pre-defined prefix of MAC addresses for each cluster, see MAC Address Prefix on page 102

- Nutanix AHV clusters use the MAC address prefix OUI `50:6B:8D` by default.

8. To configure affinity policy for this VM, click **Set Affinity**.
   The **Set VM Host Affinity** dialog box appears.
   a. Select the host or hosts on which you want configure the affinity for this VM.
   b. Click **Save**.
      The selected host or hosts are listed. This configuration is permanent. The VM will not be moved from this host or hosts even in case of HA event and will take effect once the VM starts.
9. To customize the VM by using Cloud-init (for Linux VMs) or Sysprep (for Windows VMs), select the **Custom Script** check box.
   Fields required for configuring Cloud-init and Sysprep, such as options for specifying a configuration script or answer file and text boxes for specifying paths to required files, appear below the check box.
10. To specify a user data file (Linux VMs) or answer file (Windows VMs) for unattended provisioning, do one of the following:
    » If you uploaded the file to a storage container on the cluster, click **ADSF path**, and then enter the path to the file.
      Enter the ADSF prefix (adsf:///) followed by the absolute path to the file. For example, if the user data is in /home/my_dir/cloud.cfg, enter adsf:///home/my_dir/cloud.cfg. Note the use of three slashes.
    » If the file is available on your local computer, click **Upload a file**, click **Choose File**, and then upload the file.
    » If you want to create or paste the contents of the file, click **Type or paste script**, and then use the text box that is provided.
11. To copy one or more files to a location on the VM (Linux VMs) or to a location in the ISO file (Windows VMs) during initialization, do the following:
    a. In **Source File ADSF Path**, enter the absolute path to the file.
    b. In **Destination Path in VM**, enter the absolute path to the target directory and the file name.
      For example, if the source file entry is /home/my_dir/myfile.txt then the entry for the **Destination Path in VM** should be /<directory_name>/copy_destination> i.e. /mnt/myfile.txt.
    c. To add another file or directory, click the button beside the destination path field. In the new row that appears, specify the source and target details.
12. When all the field entries are correct, click the **Save** button to create the VM and close the **Create VM** dialog box.
    The new VM appears in the VM table view.

Managing a VM (AHV)

You can use the web console to manage virtual machines (VMs) in AHV managed clusters.

About this task

Note: Use Prism Central to update a VM if you want to enable memory overcommit for it. Prism Element web console does not allow you to enable memory overcommit while updating a VM. You can enable memory overcommit in

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1412

the **Update VM** page in Prism Central. For more information, see Updating a VM through Prism Central information in *Prism Central Infrastructure Guide*.

After creating a VM, you can use the web console to start or shut down the VM, launch a console window, update the VM configuration, take a snapshot, attach a volume group, migrate the VM, clone the VM, or delete the VM.

Note: Your available options depend on the VM status, type, and permissions. Unavailable options are grayed out.

To accomplish one or more of these tasks, do the following:

Procedure

1. Log in to Prism Element web console.
2. In the VM dashboard, click the **Table** view.
3. Select the target VM in the table (top section of screen).

   The Summary line (middle of screen) displays the VM name with a set of relevant action links on the right. You can also right-click on a VM to select a relevant action.

   The possible actions are **Manage Guest Tools**, **Launch Console**, **Power on** (or **Power off**), **Take Snapshot**, **Migrate**, **Clone**, **Update**, and **Delete**.

   Note: VM pause and resume feature is not supported on AHV.

   The following steps describe how to perform each action.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1413

4. To manage guest tools as follows, click **Manage Guest Tools**.

   You can also enable NGT applications (self-service restore, Volume Snapshot Service and application-consistent snapshots) also as part of manage guest tools.

   a. Select the **Enable Nutanix Guest Tools** checkbox to enable NGT on the selected VM.

   b. Select the **Mount Nutanix Guest Tools** checkbox to mount NGT on the selected VM.

      Ensure that VM must have at least one empty IDE CD-ROM slot to attach the ISO.

      The VM is registered with the NGT service. NGT is enabled and mounted on the selected virtual machine. A CD with volume label NUTANIX_TOOLS gets attached to the VM.

   c. To enable self-service restore feature for Windows VMs, select the **Self Service Restore (SSR)** checkbox.

      The Self-Service Restore feature is enabled on the VM. The guest VM administrator can restore the desired file or files from the VM. For more information about self-service restore feature, see Self-Service Restore in the *Data Protection and Recovery with Prism Element* guide.

   d. After you select the **Enable Nutanix Guest Tools** checkbox the VSS snapshot feature is enabled by default.

      After this feature is enabled, Nutanix native in-guest VmQuiesced Snapshot Service (VSS) agent takes snapshots for VMs that support VSS.

      > **Note:** The AHV VM snapshots are not application consistent. The AHV snapshots are taken from the **VM** entity menu by selecting a VM and clicking **Take Snapshot**.
      >
      > The application consistent snapshots feature is available with Protection Domain based snapshots and Recovery Points in Prism Central. For more information, see Conditions for Application-consistent Snapshots in the *Data Protection and Recovery with Prism Element* guide.

   e. Click **Submit**.

      The VM is registered with the NGT service. NGT is enabled and mounted on the selected virtual machine. A CD with volume label NUTANIX_TOOLS gets attached to the VM.

      > **Note:**
      >
      > - If you clone a VM, by default NGT is not enabled on the cloned VM. If the cloned VM is powered off, enable NGT from the UI and power on the VM. If cloned VM is powered on, enable NGT from the UI and restart the nutanix guest agent service.
      > - You can enable NGT on multiple VMs simultaneously. For more information, see Enabling NGT and Mounting the NGT Installer Simultaneously on Multiple Cloned VMs.

      If you eject the CD, you can mount the CD back again by logging into the Controller VM and running the following nCLI command.

      ```
      nutanix@cvm$ ncli ngt mount vm-id=virtual_machine_id
      ```

      For example, to mount the NGT on the VM with VM_ID=00051a34-066f-72ed-0000-000000005400::38dc7bf2-a345-4e52-9af6-c1601e759987, type the following command.

      ```
      nutanix@cvm$ ncli ngt mount vm-id=00051a34-066f-72ed-0000-000000005400::38dc7bf2-
      a345-4e52-9af6-
      c1601e759987
      ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1414

5. To launch a console window, click the **Launch Console** action link.

   This opens a Virtual Network Computing (VNC) client and displays the console in a new tab or window. This option is available only when the VM is powered on. The console window includes the following menu options (top right):

   - Clicking the **Mount ISO** button displays a window that allows you to mount an ISO image to the VM. To mount an image, select the desired image and CD-ROM drive from the drop-down lists and then click the **Mount** button.

     > **Note:** For information on how to select CD-ROM as the storage device when you intent to provide a system image from CD-ROM, see *Add New Disk* in Creating a VM (AHV) on page 112.

   - Clicking the **Unmount ISO** button unmounts the ISO from the console.
   - Clicking the **C-A-D** icon button sends a **CtrlAltDel** command to the VM.
   - Clicking the camera icon button takes a screenshot of the console window.
   - Clicking the power icon button allows you to power on/off the VM. These are the same options that you can access from the **Power On Actions** or **Power Off Actions** action link below the VM table (see next step).

6. To start or shut down the VM, click the **Power on** (or **Power off**) action link.

   Power on begins immediately. If you want to power off the VMs, you are prompted to select one of the following options:

   - **Power Off**: Hypervisor performs a hard power off action on the VM.
   - **Power Cycle**: Hypervisor performs a hard restart action on the VM.
   - **Reset**: Hypervisor performs an ACPI reset action through the BIOS on the VM.
   - **Guest Shutdown**: Operating system of the VM performs a graceful shutdown.
   - **Guest Reboot**: Operating system of the VM performs a graceful restart.

   Select the option you want and click **Submit**.

   > **Note:** If you perform power operations such as Guest Reboot or Guest Shutdown by using the Prism Element web console or API on Windows VMs, these operations might silently fail without any error messages if at that time a screen saver is running in the Windows VM. Perform the same power operations again immediately, so that they succeed.

7. To make a snapshot of the VM, click the **Take Snapshot** action link.

   For more information, see Virtual Machine Snapshots on page 139.

8. To migrate the VM to another host, click the **Migrate** action link.

   This displays the **Migrate VM** dialog box. Select the target host from the drop-down list (or select the **System will automatically select a host** option to let the system choose the host) and then click the **Migrate** button to start the migration.

   > **Note:** Nutanix recommends to live migrate VMs when they are under light load. If they are migrated while heavily utilized, migration may fail because of limited bandwidth.

9. To clone the VM, click the **Clone** action link.

   This displays the **Clone VM** dialog box, which includes the same fields as the **Create VM** dialog box. A cloned VM inherits the most the configurations (except the name) of the source VM. Enter a name for the clone and

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1415

then click the **Save** button to create the clone. You can optionally override some of the configurations before clicking the **Save** button. For example, you can override the number of vCPUs, memory size, boot priority, NICs, or the guest customization.

> **Note:**
>
> - You can clone up to 250 VMs at a time.
> - You cannot override the secure boot setting while cloning a VM, unless the source VM already had secure boot setting enabled.

10. To modify the VM configuration, click the **Update** action link.

    The **Update VM** dialog box appears, which includes the same fields as the **Create VM** dialog box. Modify the configuration as needed, and then save the configuration. In addition to modifying the configuration, you can attach a volume group to the VM and enable flash mode on the VM. If you attach a volume group to a VM that is part of a protection domain, the VM is not protected automatically. Add the VM to the same Consistency Group manually.

    (For GPU-enabled AHV clusters only) You can add pass-through GPUs if a VM is already using GPU pass-through. You can also change the GPU configuration from pass-through to vGPU or vGPU to pass-through, change the vGPU profile, add more vGPUs, and change the specified vGPU license. However, you need to power off the VM before you perform these operations.

    - Before you add multiple vGPUs to the VM, see Multiple Virtual GPU Support and Restrictions for Multiple vGPU Support in the *AHV Administration Guide*.
    - Multiple vGPUs are supported on the same VM only if you select the highest vGPU profile type.
    - For more information on vGPU profile selection, see:
      - *Virtual GPU Types for Supported GPUs* in the *NVIDIA Virtual GPU Software User Guide* in the NVIDIA's *Virtual GPU Software Documentation* web-page, and
      - GPU and vGPU Support in the *AHV Administration Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1416

- After you add the first vGPU, to add multiple vGPUs, see Adding Multiple vGPUs to the Same VM in the *AHV Administration Guide*.

You can add new network adapters or NICs using the **Add New NIC** option. For more information, see Step 7 in Creating a VM (AHV) on page 112.

You can also modify the network used by an existing NIC. Before you modify the NIC network observe the limitations in Limitation for vNIC Hot-Unplugging in the *AHV Administration Guide*.

> **Note:**
>
> - To create or update a Traffic Mirroring destination type VM or vNIC, use command line interface. For more information, see Traffic Mirroring on AHV Hosts on page 90.
> - If you delete a vDisk attached to a VM and snapshots associated with this VM exist, space associated with that vDisk is not reclaimed unless you also delete the VM snapshots.

To increase the memory allocation and the number of vCPUs on your VMs while the VMs are powered on (hot-pluggable), do the following:

a. In the **vCPUs** field, you can increase the number of vCPUs on your VMs while the VMs are powered on.

b. In the **Number of Cores Per vCPU** field, you can change the number of cores per vCPU only if the VMs are powered off.

> **Note:** This is not a hot-pluggable feature.

c. In the **Memory** field, you can increase the memory allocation on your VMs while the VMs are powered on.

For more information about hot-pluggable vCPUs and memory, see Virtual Machine Memory and CPU Hot-Plug Configurations.

To attach a volume group to the VM, do the following:

a. In the **Volume Groups** section, click **Add volume group**, and then do one of the following:

   » From the **Available Volume Groups** list, select the volume group that you want to attach to the VM.

   » Click **Create new volume group**, and then, in the **Create Volume Group** dialog box, create a volume group. After you create a volume group, select it from the **Available Volume Groups** list.

   Repeat these steps until you have added all the volume groups that you want to attach to the VM.

b. Click **Add**.

11. To enable flash mode on the VM, click the **Enable Flash Mode** check box.

» After you enable this feature on the VM, the status is updated in the VM table view. To view the status of individual virtual disks (disks that are flashed to the SSD), click the update disk icon in the **Disks** pane in the **Update VM** window.

» You can disable the flash mode feature for individual virtual disks. To update the flash mode for individual virtual disks, click the update disk icon in the **Disks** pane and deselect the **Enable Flash Mode** check box.

12. To delete the VM, click the **Delete** action link. A window prompt appears; click the **OK** button to delete the VM.
The deleted VM disappears from the list of VMs in the table.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1417

Limitation for vNIC Hot-Unplugging

If you detach (hot-unplug) the vNIC for the VM with guest OS installed on it, the AOS displays the detach result as successful, but the actual detach success depends on the status of the ACPI mechanism in guest OS.

The following table describes the vNIC detach observations and workaround applicable based on guest OS response to ACPI request:

Table 13: vNIC Detach - Observations and Workaround

Detach Procedure Followed	Guest OS responds to ACPI request (Yes/No)	AOS Behavior	Actual Detach Result	Workaround
vNIC Detach (hot-unplug) • *Using Prism Central:* For more information, see Managing a VM (AHV) topic in *Prism Central Infrastructure Guide*. • Using Prism Element web console: For more information, see Managing a VM (AHV) on page 117. • *Using acli:* Log on to the CVM with SSH and run the following command: nutanix@cvm$ acli vm.nic_delete <vm_name> <nic mac address> or, nutanix@cvm$ acli vm.nic_update <vm_name> <nic mac address> connected=false Replace the following attributes in the above commands: • *<vm_name>* with the name of the guest VM for which the vNIC is to be detached. • *<nic mac address>* with the vNIC MAC address that needs to be detached.	Yes	vNIC detach is Successful.	vNIC detach is successful.	*No action needed*
	No	Observe the following logs: `Device detached successfully`	vNIC detach is not successful.	Power cycle the VM for successful vNIC detach.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1418

Note: In most cases, it is observed that the ACPI mechanism failure occurs when no guest OS is installed on the VM.

Shutting Down VMs using aCLI

You might need to shut down VMs in an AHV cluster to perform a maintenance activity or tasks such as relocating the hardware.

Before you begin

Ensure that you meet the following prerequisites before you shut down the VMs:

- The NCC is upgraded to the most recent version and passes a complete NCC health check.
- Shut down the services or VMs associated with AOS features or Nutanix products. For example, shut down all the Nutanix file server VMs (FSVMs). For more information, see the features or product documentation.

About this task

You can shut down all the guest VMs in the cluster in one of the following ways:

- Shut down a single guest VMs.
- Shut down all the guest VMs in the AHV cluster.

Procedure

1. Log on to a CVM in the cluster with SSH.
2. To force shut down through AHV, run the following command:

   ```
   nutanix@cvm$ acli vm.shutdown vm-name
   ```

   Replace *vm-name* with the name of the VM you want to shut down.
3. Verify if all the guest VMs are shut down.

   ```
   nutanix@CVM$ acli vm.list power_state=on
   ```

4. If any of the VMs are still on, consider powering off the VMs from within the guest OS. To force shut down all the VMs through AHV, run the following command.

   ```
   nutanix@cvm$ for i in $(acli vm.list power_state=on | grep -v NTNX | awk 'NR!=1
    {print $NF}');do acli vm.shutdown $i ; done
   ```

5. Complete the maintenance activity or any other tasks.

Starting Up VMs using aCLI

You might need to restart VMs in an AHV cluster after a maintenance activity or tasks such as relocating the hardware is performed.

Before you begin

Ensure that you meet the following prerequisites before you shut down the all the VMs in the cluster:

- Node is powered on using the power button on the front of the block for each node.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1419

- IPMI password is accessible and logged on to the IPMI web console of each node, as it is required to verify if the node is powered on. On the **System** tab check the **Power Control** status.

  > **Note:** The navigation path, tabs, and UI layout in IPMI web console can vary based on the hardware used at your site.

- Wait for approximately 5 minutes after you start the last node to allow the cluster services to start. All CVMs start automatically after you start all the nodes.

About this task

You can start up all the guest VMs in the cluster in one of the following ways:

- Start up a single guest VM.
- Start up all the guest VMs in the AHV cluster.

Procedure

1. Start the cluster and verify its status:

   a. Log on to any CVM in the cluster with SSH.

   b. Start the cluster.

   ```
   nutanix@cvm$ cluster start
   ```

   c. Verify that all the cluster services are in the UP state.

   ```
   nutanix@cvm$ cluster status
   ```

2. To force start the VMs through AHV, run the following command:

   ```
   nutanix@cvm$ acli vm.on vm-name
   ```

   Replace *vm-name* with the name of the VM you want to start up.

3. Verify if all the guest VMs are powered on.

   ```
   nutanix@CVM$ acli vm.list power_state=on
   ```

4. If any of VMs are still off, consider powering on the VMs from within the guest OS. To force power on all the VMs through AHV, run the following command.

   ```
   nutanix@cvm$ for i in $(acli vm.list power_state=off | grep -v NTNX | awk 'NR!=1
    {print $NF}');do acli vm.on $i ; done
   ```

5. Start the services or VMs associated with AOS features or Nutanix products. For example, start all the FSVMs. See the documentation of those features or products for more information.

   > **Note:** You can also verify if all guest VMs are powered on by using the Prism Element web console.

VM Migration Specifications

VM migration can be performed in the following ways:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1420

- *Live Migration* – This method is used to transfer the VM from one physical host to another host without affecting the normal functions and operations of the VM, and with minimal and often no interruption to the users of the VM.

  Live migration is supported for the following scenarios:

  - Intra-cluster live migration of guest VMs from one host to another host. For more information, see Migrating Within the Cluster in the *Prism Central Infrastructure Guide*.
  - Cross-cluster live migration (CCLM) of guest VMs protected with synchronous replication schedules. For more information, see Cross-Cluster Live Migration in the *Nutanix Disaster Recovery Guide*.
  - On-demand cross-cluster live migration of guest VMs across AHV clusters registered to the same or different Prism Central AZs. For more information, see On-Demand Cross-Cluster Live Migration on page 133.

- *Cold Migration* - This method is used to transfer the VM from one physical host to another host with minimal VM downtime. You can use **Nutanix Move** for Inter-cluster VM migration <Third-Party Hypervisor> to the AHV cluster. For more information, see Move User Guide.

  Note: The <Third-party hypervisors> are Xen (Amazon EC2), Microsoft Hyper-V, and VMware ESXi.

Live Migration Cases

VM live migration is applicable for the following cases:

- Maintenance activity required on the cluster - This scenario is applicable for a planned event (for example, scheduled maintenance of guest VMs) at the primary AZ when you put node into maintenance mode. For information on how to configure a planned failover, see Cross-Cluster Live Migration section in *Nutanix Disaster Recovery Guide*.
- AHV or Firmware Upgrades - When you upgrade the AHV or Firmware, the VMs need to be live migrated to another AHV cluster.
- Load balancing or to isolate specific VMs on hosts.
- Changes in Host affinity policy.
- Acropolis Dynamic Scheduling (ADS)- If ADS detects a resource contention in the cluster, it creates a migration plan to eliminate the hotspots in the cluster by migrating VMs from one host to another. For more information about ADS, see Acropolis Dynamic Scheduling in AHV.
- Defragmentation activity to create resources for VM power-on operation. This activity is performed when the cluster can accommodate resources for VM power-on operation after moving some VMs to another host.

Live Migration Restrictions

This section provides the list of factors that affect VM live migration.

The following conditions affect VM live migration;

- VM is powered off.
- VM is configured as an agent VM.

  You can select or clear the **Use this VM as an agent VM** checkbox to enable or disable this function when you create or update a VM. For more information, see the Creating a VM through Prism Central (AHV) section in the *Prism Central Infrastructure Guide*.

- For guest VMs with Windows Credential Guard enabled, the VM live migration is only supported between the nodes with Skylake or newer Intel CPU generations. While expanding the cluster, if you add a node with CPU generation prior to Skylake, the system generates an alert *VMs became non-migratable due to node addition* after

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1421

cluster expansion. Nutanix recommends that you remove the nodes with older CPU generation, power-off, then power-on affected guest VMs to re-enable VM live migration support. For more information, see KB-15227.

For information about Windows Credential Guard, see the Windows Defender Credential Guard Support .

- For guest VMs with WSL2 enabled, VM live migration is only supported between the nodes with Skylake or newer Intel CPU generations. While expanding the cluster, if you add a node with CPU generation prior to Skylake, the system generates an alert *VMs became non-migratable due to node addition* after cluster expansion. Nutanix recommends that you remove the nodes with older CPU generation, power-off, then power-on affected guest VMs to re-enable VM live migration support. For more information, see KB-15227.

  For information about WSL2, see the Windows Subsystem for Linux (WSL2) Support on AHV on page 158 .

- GPU passthrough is enabled.

  For information on how to verify if GPU passthrough is enabled for the VM, see Checking Live Migration Status of a VM on page 128.

- CPU passthrough is enabled.

- VM-Host affinity is set from the Prism Element web console with one host.

  For information on how to verify the VM-Host affinity policy from the Prism Element web console, see Verifying Affinity Policy Association on page 129.

- VM affinity policies are defined from Prism Central using VM categories and host categories.

  For information on how to verify the affinity policies mapped to a VM from Prism Central, see Checking Affinity Policies of a VM From Prism Central on page 130.

- Defragmentation activity to create resources for VM-power-on is in progress.

Note:

- Starting with AOS 6.8 release, AHV supports the live migration of the guest VMs that have Windows Credential Guard enabled. When you upgrade to AOS 6.8 or later release and enable HA reservation for the cluster, the system reserves the resources to accommodate the HA event. However, if you have the existing VMs in the cluster that have Windows Credential Guard enabled, some guest VMs (both with or without Windows Credential Guard enabled) might fail to start due to the unavailability of sufficient resources in the cluster. Ensure that you have sufficient resources available in the cluster to accommodate the HA reservation.

  For more information on Windows Credential Guard, see the Windows Defender Credential Guard Support in AHV section in the *AHV Administration Guide*.

  For more information on how to enable HA reservation, see the Enabling High Availability for the Cluster section in the *Prism Element Web Console Guide*.

- Starting from AOS 7.0 release, with a minimum required AHV version of 10.0, AHV supports the live migration of the guest VMs that have WSL2 enabled. When you upgrade to AOS 7.0 or later release and enable HA reservation for the cluster, the system reserves the resources to accommodate the HA event. However, if you have the existing VMs in the cluster that have WSL2 enabled, some guest VMs (both with or without WSL2 enabled) might fail to start due to the unavailability of sufficient resources in the cluster. Ensure that you have sufficient resources available in the cluster to accommodate the HA reservation.

  For more information on WSL2, see Windows Subsystem for Linux (WSL2) Support on AHV on page 158 in the *AHV Administration Guide*.

  For information on how to enable HA reservation, see Enabling High Availability for the Cluster section in the *Prism Element Web Console Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1422

Checking Live Migration Status of a VM

This section describes how to check whether the live migration is allowed for the VM.

Procedure

To check if a VM can be live migrated, perform the following steps:

1. Log on to the CVM as a nutanix user using SSH.
2. Run the following command:

   ```
   nutanix@cvm$ acli vm.get <VM_NAME> | grep 'allow_live_migrate
   ```

   Replace `<VM_NAME>` with the actual VM name at your site.

   The following attribute value confirms the live migration is allowed:

   ```
   allow_live_migrate: True
   ```

What to do next

If `allow_live_migrate: False` is returned for the above command, then check the status of the VM properties that restricts live migration.

The following table provides the information about the verification procedure to check the status of VM properties:

VM Properties	Verification Procedure

WSL2	Log on to the CVM as a Nutanix user using SSH, and run the following command:
	`nutanix@cvm$ acli vm.get <VM_NAME> | grep 'hardware_virtualization`
	Replace `<VM_NAME>` with the actual VM name at your site.
	The following attribute value confirms WSL2 is enabled:
	`hardware_virtualization: True`

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1423

VM Properties	Verification Procedure
GPU	1. Log in to Prism Central. 2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information on the **Navigation Bar**, see Application-specific Navigation Bar. The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment. 3. Apply the **GPU TYPE** filter from the **Modify Filter** option. The system displays the VMs based on the selected GPU criteria. **Figure 17: GPU TYPE Filter**

Verifying Affinity Policy Association

This section describes how to verify the VM-Host affinity from Prism Element web console and affinity policies mapped to the VM from Prism Central.

Procedure

To verify affinity policy association for a VM, perform the following checks:

- Checking VM-Host Affinity From Prism Element on page 129.
- Checking Affinity Policies of a VM From Prism Central on page 130.

Checking VM-Host Affinity From Prism Element

About this task

Using Prism Element, you can define the VM-host affinity policy that controls the placement of a VM. You can use this policy to specify that a selected VM can only run on the members of the affinity host list.

Procedure

To verify the VM-Host affinity, perform the following steps:

1. Log in to Prism element web console.
2. Navigate to **VM** > **Table**, and double-click the target VM name. The system displays the **Update VM** window.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1424

3. Under **VM Host Affinity**, check the hosts specified for the VM.

> **Note:**
>
> VMs with Host affinity policies can only be migrated to the hosts specified in the affinity policy during an HA event. If only one host is specified, the VMs cannot be migrated.

Checking Affinity Policies of a VM From Prism Central

About this task

Using Prism Central, you can define the affinity policy based on VM Categories and Host categories.

Procedure

To verify the affinity policy associated with a VM, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.

   The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment.
3. Click the target VM name.
   The system displays the details view of the target VM.
4. Click the **Categories** tab in the target VM's details view.
   The system displays the Categories and Affinity Policy associated with the VM.

Defining Behaviour for Non-migratable VMs (GPU/CPU/PCI/Host Affinity configured VMs)

About this task

When a host is put in maintenance mode, VMs are moved from that host to other hosts in the cluster. After exiting maintenance mode, those VMs are automatically returned to the original host, eliminating the need to manually move them. However, some VMs cannot be migrated to other hosts. For more information, see Non-Migratable VMs on page 171.

When an attempt is made for a host to enter maintenance mode, the VMs with GPU passthrough, CPU passthrough, and PCI passthrough are not migrated to the other hosts in the cluster and therefore may block the attempt to enter maintenance mode.

> **Note:** VMs with host affinity policies are also not migrated to other hosts in the cluster, if any of the following condition is met:
>
> - The hosts that are configured as part of VM-Host affinity policy are not available.
> - The hosts that are part of VM-Host affinity policy does not have the sufficient resources to run the VM.

To overcome this situation, Nutanix recommends you define either of the following behavior for these non-migratable VMs when host enters the maintenance mode:

- Automatically shutdown these non-migratable VMs.
- Set a block migration indication for these non-migratable VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1425

Procedure

To define the above behaviors for non-migratable VMs, perform the following steps:

1. Log on to CVM with SSH.
2. Run the following command to put the host into maintenance mode with default action set for non-migratable VMs:

```
nutanix@cvm$ acli host.enter_maintenance_mode <Hypervisor-IP-address> [wait="{ true | false }" ]
 [non_migratable_vm_action="{ acpi_shutdown | block }"
```

   Replace:

   - `<Hypervisor-IP-address>` - with the actual host name at your site.
   - `wait`: Set the wait parameter to true to wait for the host evacuation attempt to finish.
   - `non_migratable_vm_action`: By default, this parameter is set to *block*, which means the non-migratable VMs are shut down when you put a node into maintenance mode. For more information on non-migratable VMs, see Non-Migratable VMs on page 171.

     If you want to automatically shut down such VMs for the duration of the maintenance mode, set this parameter to *acpi_shutdown*.

Multichannel Support for AHV Live Migration Performance

Multichannel live migration facilitates the creation of multiple channels (or data streams) between the source and the destination host during live migration. For every channel, there is a separate TCP/unix socket and a thread that manages the data processing (sending or receiving the data) on that socket. The live migration feature then uses multiple send and receive threads to completely use the higher network bandwidths.

Live migration with multiple send and receive threads provides the following benefits:

- Support for the usage of multiple NICs available in uplinks to transfer the data during live migration.

  Note: If you have NICs configured in Active-Standby mode and only one NIC is used at a time, Nutanix recommends you perform link aggregation using LACP to use the combined network bandwidth of all the NICs. For more information about how to enable LACP, see Enabling LACP and LAG (AHV Only).

- Live migration with an optimum number of channels or data streams and utilization of the maximum network bandwidth between source and destination host.

For example, for a four-node cluster with an available bandwidth of 25 Gbps per node, a single live migration with multiple channels utilizes the complete network and improves the migration speed. The following table provides a brief comparison of the measurement attributes between live migration with multiple channels and live migration without multiple channels:

Table 14: Measurement Attributes - Multichannel Live Migration

Measurement Attributes	Live migration with Multiple Channels	Live Migration without Multiple Channels
Bandwidth Utilization at the source and destination host.	Utilizes more than 50 to 55 % bandwidth and offers approximately 55.54 Gbps bandwidth at both source and destination hosts.	Utilizes only 10 to 11 % bandwidth and offers approximately 10.57 to 11.1 Gbps bandwidth at both source and destination hosts.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1426

Measurement Attributes	Live migration with Multiple Channels	Live Migration without Multiple Channels
Enter Maintenance Mode (EMM) task time	Significant reduction in EMM task time to approximately six times when compared to the single live migration without multiple channels.	

Note:

- The Multichannel functionality is supported with AHV version 20220304.10055 and AOS version 6.7 or above.
- Multichannel Live migration is only supported for host *Enter Maintenance Mode* and *Restore Locality* migration tasks. These migration tasks run in parallel during host evacuation and restore operations.
- Based on the workloads available, the system allocates the source host bandwidth during *Enter Maintenance Mode* migration task and destination host bandwidth during the *Restore Locality* migration task

During serial live migration, the CPU is unable to use the complete bandwidth if a single migration is in progress on a 10 Gbps or faster network. However, with multichannel support, the system performs the following actions:

- Uses multiple streams.
- Selects the right number of channels for transfer.
- Utilizes the complete network bandwidth, and reduces the host evacuation time during live migration.

Note: For reliability improvements, the system performs the internal serial retry for each migration that fails due to insufficient bandwidth at the source host.

The following table describes the system behavior when the multichannel support for live migration is enabled based on AOS and AHV releases:

Table 15: Multichannel Support - System Behavior

AOS	AHV Version	Is Multichannel Support Enabled?	System Behavior
AOS 6.6 or before.	Bundled AHV version	No	The system performs live migration using a single data stream for host evacuation and restore operations. In this case, a single CPU is not able to use the network bandwidth completely. The system can only use 16 Gbps for host evacuation, which means only two live migrations at a time, as 8 Gbps is available for single live migration.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1427

AOS	AHV Version	Is Multichannel Support Enabled?	System Behavior
AOS 6.7 or later	20220304.10055 or recommended AHV version for later AOS releases.	Yes	The system utilizes the complete network bandwidth using multiple channels or data streams for the following migration tasks: • *Enter Maintenance Mode* task for host evacuation at a source host. • *Restore Locality* task for restore at the destination host. Based on the network workload, the system assigns the maximum required bandwidth to the data streams for live migration.

Adaptive CPU Management during Live Migration

VM live migration involves migrating a VM from one host to another host without any noticeable VM downtime. During this live migration process, the system transfers the VM memory from the source host (where the VM is currently running) to the destination host. Since the VM is still running on the source host, a part or the entire VM's memory might get written again. The rewritten memory is called the dirty memory that needs to be transferred again to the destination host. The dirty memory transfer process goes on for iterations until we have a very small size of dirty memory that can be transferred in a smaller downtime window. The high dirty memory rate impacts the VM migration time and success rate, especially when the network bandwidth is limited for VM Live migration.

AHV provides a seamless mechanism to handle these dirty memory build-ups. AHV intelligently detects the vCPUs that are involved in actively dirtying memory and manages their utilization dynamically without any impact on the vCPUs that are not dirtying the memory. The adaptive CPU management in AHV helps you to automatically optimize the network bandwidth consumption, increase the success rate for VM migrations, and reduce the VM migration time significantly.

On-Demand Cross-Cluster Live Migration

On-demand cross-cluster live migration (OD-CCLM) enables you to migrate guest VMs (and all of their associated metadata like VM categories) across AHV clusters registered to the same or different Prism Central instances spanning availability zones (AZs). To ensure zero downtime of the guest VMs, you can live migrate without the need to protect the guest VMs with synchronous replication schedules or set up Nutanix Disaster Recovery from the Prism Central web console.

> **Note:** AHV Metro Availability also provides cross-cluster live migration (CCLM) capability that is based on the Nutanix Disaster Recovery workflows. With AHV Metro CCLM, you can live migrate only the guest VMs protected with synchronous replication schedules. For more information on AHV Metro CCLM, see Cross-Cluster Live Migration in the *Nutanix Disaster Recovery Guide*.

You can live migrate a VM in the following situations:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1428

- In an overlay subnet in a Prism Central AZ to an overlay subnet in another Prism Central AZ
- In an overlay subnet in a virtual private cloud (VPC) in a Prism Central AZ to an overlay subnet in another VPC in the same Prism Central AZ
- Within the same VPC in a Prism Central AZ
- In a VLAN subnet in a Prism Central AZ to a VLAN subnet in another Prism Central AZ
- In a VLAN subnet in a Prism Central AZ to another VLAN subnet in the same Prism Central AZ

A Layer 2 (L2) network extension creates a tunnel between the source and destination subnets so that the VMs in these subnets can communicate with each other. To ensure that dependent VMs on the source cluster and the destination cluster can communicate with the migrating VM throughout the live migration process, connect the source and the destination subnets using an L2 network extension before you live migrate a VM in the following scenarios:

- From an overlay subnet in a Prism Central AZ to an overlay subnet in another Prism Central AZ
- From an overlay subnet in a VPC in a Prism Central AZ to an overlay subnet in another VPC in the same Prism Central AZ
- From a VLAN subnet in a Prism Central AZ to a VLAN subnet in another Prism Central AZ
- From a VLAN subnet in a Prism Central AZ to another VLAN subnet in the same Prism Central AZ

> **Note:** An L2 network extension is not required between the source and the destination subnets if you live migrate a guest VM within the same VPC subnet.

For successful live migration, Nutanix recommends that the round-trip latency between the clusters must be 40 ms or less. The data copy time during live migration is dependent on the data to be copied between the clusters and the available network bandwidth.

On-Demand Cross-Cluster Live Migration (OD-CCLM) Requirements

This section describes the requirements for live migrating guest VMs.

Table 16: Nutanix Software Requirements

Nutanix Software	Software Version Required
AOS	• 6.7 or later. While upgrading the AOS version from 6.6 to 6.7, ensure that the upgrade is completed before performing on-demand migration of the guest VM. • For OD-CCLM of vTPM-enabled guest VMs, 6.8 or later. Both the source and destination clusters must be running AOS 6.8 and later.
Prism Central	• pc.2023.3 or later. • For OD-CCLM of vTPM-enabled guest VMs pc.2024.1 or later.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1429

Table 17: Prism Central User Requirements

Prism Central User	Permissions
Administrator	Only the administrator (local admin user account in Prism Central) can perform on-demand live migration between the clusters registered to different Prism Central deployments.
Non-administrator	Non-administrators can perform on-demand live migration only between the clusters registered to the Prism Central deployment. The user must have the following permissions: • View_Prism_Central • View_Virtual_Machine • View_Subnet • View_Availability_Zone • Allow_Cross_Cluster_VM_Migration • View_Cluster For more information on user management, see User Management in *Security Guide*.

- Both the source and the destination subnet must have the same IP network prefix.
- If you did not enable the advanced processor compatibility feature for the guest VM, ensure that the destination Nutanix cluster supports all of the CPU feature sets (set of CPU flags) that are supported on the source Nutanix cluster. Otherwise, live migration fails. For more information, see Advanced Processor Compatibility in AHV Administration Guide.

  Live migration can happen even when the CPU types of the source and destination clusters do not match exactly. The destination cluster must support the superset of the CPU features of the source cluster.
- If the VM in the source cluster has NGT enabled, then the VM must have at least one empty IDE or SATA CD-ROM to attach the ISO required for reconfiguration on the destination cluster.
- Both the source and the destination clusters must run on the same AHV version.
- Both the source and the destination clusters must have the same storage container name for the guest VMs.

  A storage container with the same name as the one on the source cluster must exist on the destination cluster. For example, if a *SelfServiceContainer* storage container exists on the source cluster, the destination cluster must also have a *SelfServiceContainer* storage container.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1430

- If the source and the destination cluster (Prism Element) are in different subnets, open the ports listed on Ports and Protocols for communication.

  > **Tip:** If the source and the destination cluster (Prism Element) are in the same subnet, you do not need to open the ports manually.

  - To open the ports for communication from the source cluster to the destination cluster, run the following command on all CVMs of the source cluster:

    ```
    nutanix@cvm$ allssh 'modify_firewall -f -r remote_cvm_ip,remote_virtual_ip -p
     2030,2036,2073,2090 -i eth0'
    ```

    Replace *remote_cvm_ip* with the IP address of the destination cluster CVM. For multiple CVMs, replace *remote_cvm_ip* with the IP addresses of the CVMs separated by comma.

    Replace *remote_virtual_ip* with the virtual IP address of the destination cluster.

  - To open the ports for communication from the destination cluster to the source cluster, run the following command on all CVMs of the destination cluster:

    ```
    nutanix@cvm$ allssh 'modify_firewall -f -r source_cvm_ip,source_virtual_ip -p
     2030,2036,2073,2090 -i eth0'
    ```

    Replace *source_cvm_ip* with the IP address of the source cluster CVM. For multiple CVMs, replace *source_cvm_ip* with the IP addresses of the CVMs separated by comma.

    Replace *source_virtual_ip* with the virtual IP address of the source cluster.

    > **Note:**
    >
    > - Use the *eth0* interface only. *eth0* is the default CVM interface that shows up when you install AOS.
    > - For Nutanix Disaster Recovery on Network Segmentation enabled Nutanix cluster, use the *ntnx0* interface and run the following command:
    >
    >   ```
    >   nutanix@cvm$ allssh 'modify_firewall -f -r remote_cvm_ip,remote_virtual_ip
    >    -p 2030,2036,2073,2090 -i ntnx0'
    >   ```
    >
    >   Replace *remote_cvm_ip* with the IP address of the cluster CVM where you want to migrate the guest VMs. For multiple CVMs, replace *remote_virtual_ip* with the IP addresses of the CVMs separated by comma.

- The destination cluster must have sufficient storage capacity to host the migrating guest VMs.
- The destination cluster must be reachable from the source cluster.
- IP address management must be manually set up on both the source and the destination cluster.
- The guest VM to be live migrated must be powered on.

  The Prism Central web console filters out the guest VMs that are powered off.

On-Demand Cross-Cluster Live Migration (OD-CCLM) Limitations

Consider the following limitations before performing OD-CCLM of your guest VMs:

- Currently, on-demand live migration of guest VMs is not supported when Windows Defender Credential Guard is enabled.
- On-demand live migration to clusters on Nutanix Cloud AZ (DRaaS) is not supported.
- On-demand live migration to Nutanix Cloud Cluster AZ (NC2) is not supported.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1431

- On-demand live migration of up to 60 guest VMs in parallel is supported.

  While no limit exists to the number of parallel migrations, the time required for successful migration depends on the guest VM size.

- On-demand live migration of guest VMs fails in the following scenarios:

  - Guest VMs are part of Flow Network Security policies.
  - Guest VMs are part of consistency groups.
  - You cannot migrate VMs that have volume groups attached to them.
  - Guest VMs have Replication Factor 1 (RF1).
  - GPU passthrough is enabled on guest VMs.

    For information on GPU passthrough verification, see Checking Live Migration Status of a VM.

    For information on GPU passthrough verification using acropolis CLI (acli), see vm in the Command Reference Guide.

  - Guest VMs are vNUMA VMs.
  - Guest VMs are in a paused state or have NVMe disks attached.
  - Memory overcommit is enabled on guest VMs.
  - Guest VMs are connected to a managed VLAN (IPAM-enabled).
  - Guest VMs are connected to Open Virtual Network (OVN) LAN.
  - Guest VMs are upgraded before on-demand live migration starts.

    When on-demand live migration is in progress, do not perform hotplug upgrades to the memory or CPU. Updates to NIC, disk, memory, and CPU are fatal while data is copied during migration.

  - Prism Central upgrade is in progress.
  - AHV upgrade is in progress.

    Similarly, if on-demand live migration is in progress, upgrading AHV fails.

  - LCM upgrade is in progress.

- After migrating a guest VM in an overlay subnet in a virtual private cloud (VPC) to an overlay subnet in another VPC, Prism Central does not retain the floating IP address of the guest VM if the VPCs are attached to different external subnets. Therefore, you must reassign the floating IP address to the migrated guest VM to access the guest VM from the external network.

  If the VPCs share the same external subnets, Prism Central retains the floating IP address of the guest VM.

- After migration to the recovery cluster, VM categories are not preserved if those categories do not exist on the recovery cluster.
- Data over the wire is not encrypted during the live migration.
- Automatic defragmentation on the recovery cluster is not supported.
- Guest VMs running on ESXi are not supported.

On-Demand Cross-Cluster Live Migration (OD-CCLM) Best Practices

Nutanix recommends the following best practices for live migrating your guest VMs (and all of their associated metadata like VM categories):

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1432

- Ensure that you set up the relevant user permissions. For more information, see On-Demand Cross-Cluster Live Migration (OD-CCLM) Requirements on page 134.
- Enable the advanced processor compatibility feature for the guest VM and select the oldest CPU generation to maximize the migration capability of the guest VM. For more information, see Advanced Processor Compatibility in AHV.
- Do not protect the guest VM with a DR protection policy when on-demand live migration is in progress.
- Do not perform Nutanix software upgrades when on-demand live migration is in progress. For more information, see On-Demand Cross-Cluster Live Migration (OD-CCLM) Limitations on page 136.
- Do not perform on-demand live migration when Nutanix software upgrades are in progress. For more information, see On-Demand Cross-Cluster Live Migration (OD-CCLM) Limitations on page 136.
- Do not change the IP addresses or other network configurations of the guest VMs when on-demand live migration is in progress.
- Ensure that a 10G network link is available in the infrastructure setup.
- When an administrator user live migrates the guest VMs created by a non-administrator to a Nutanix cluster registered to a different Prism Central deployment, the administrator user becomes the owner of the guest VM after the VM migration. The ownership remains the same irrespective of who migrated the guest VM when the live migration happens between the Nutanix clusters registered to the same Prism Central deployment.

Performing On-Demand CCLM

If, due to a failure event (for example, scheduled maintenance of guest VMs) at the primary cluster, you must migrate your applications to another AHV cluster without VM downtime, perform an on-demand live migration to the recovery cluster.

Before you begin

See On-Demand Cross-Cluster Live Migration (OD-CCLM) Requirements on page 134, On-Demand Cross-Cluster Live Migration (OD-CCLM) Limitations on page 136, and On-Demand Cross-Cluster Live Migration (OD-CCLM) Best Practices on page 137.

About this task

To live migrate the guest VMs, follow these steps at the primary AZ:

Procedure

1. Log in to the Prism Central web console.
2. From **Application Switcher Function**, select the **Infrastructure** application, and navigate to **Compute** > **VMs** from the **Navigation Bar**.
3. Select the guest VMs to live migrate.

   Warning: To see the guest VM configurations that cannot be migrated, see On-Demand Cross-Cluster Live Migration (OD-CCLM) Limitations on page 136.

4. Click **Migrate Across Clusters** from the **Actions** drop-down menu.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1433

5. Do the following in the **Destination Cluster** tab:
   a. From the dropdown menu, under **Destination Location**, select the AZ to live migrate your guest VMs.
   b. From the dropdown menu, under **Destination Cluster**, select the AHV cluster to live migrate your guest VMs.
   c. Click **Next**.
6. Do the following in the **Network** tab:
   a. From the dropdown menu under **Destination Subnets**, select the network to map the subnet of the migrated guest VMs.
   b. Click **Next**.
7. Do the following in the **Migration Checks** tab:
   a. Review the status of the selected guest VMs after the prechecks run automatically.
      If any precheck fails, resolve the issue that is causing the failure and click **check again**.
   b. When all the **Checks** under the **Selected VMs** show OK, click **Migrate**.

   The selected guest VMs migrate to the recovery cluster with zero VM downtime.

Virtual Machine Snapshots

You can generate snapshots of virtual machines or VMs. You can generate snapshots of VMs manually or automatically. Some of the purposes that VM snapshots serve are as follows:

- Disaster recovery
- Testing - as a safe restoration point in case something went wrong during testing.
- Migrate VMs
- Create multiple instances of a VM.

Snapshot is a point-in-time state of entities such as VM and Volume Groups, and used for restoration and replication of data. You can generate snapshots and store them locally or remotely. Snapshots are mechanism to capture the delta changes that has occurred over time. Snapshots are primarily used for data protection and disaster recovery. Snapshots are not autonomous like backup, in the sense that they depend on the underlying VM infrastructure and other snapshots to restore the VM. Snapshots consume less resources compared to a full autonomous backup. Typically, a VM snapshot captures the following:

- The state including the power state (for example, powered-on, powered-off, suspended) of the VMs.
- The data includes all the files that make up the VM. This data also includes the data from disks, configurations, and devices, such as virtual network interface cards.

VM Snapshots and Snapshots for Disaster Recovery

The **VM** Dashboard only allows you to generate VM snapshots manually. You cannot select VMs and schedule snapshots of the VMs using the VM dashboard. The snapshots generated manually have very limited utility.

> **Note:** These snapshots (stored locally) cannot be replicated to other sites.

You can schedule and generate snapshots as a part of the disaster recovery process using Nutanix DR solutions. AOS generates snapshots when you protect a VM with a protection domain using the **Data Protection** dashboard in Prism Element web console. For more information, see Snapshots in the *Data Protection and Recovery with Prism Element Guide*. Similarly, AOS generates recovery points (snapshots are called recovery points in Prism Central)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1434

when you protect a VM with a protection policy. For more information about protection policies, see Protection Policies View in *Nutanix Disaster Recovery Guide*.

For example, in the **Data Protection** dashboard in Prism Element web console, you can create schedules to generate snapshots using various RPO schemes such as asynchronous replication with frequency intervals of 60 minutes or more, or NearSync replication with frequency intervals of as less as 20 seconds up to 15 minutes. These schemes create snapshots in addition to the ones generated by the schedules, for example, asynchronous replication schedules generate snapshots according to the configured schedule and, in addition, an extra snapshot every 6 hours. Similarly, NearSync generates snapshots according to the configured schedule and also generates one extra snapshot every hour.

Similarly, you can use the options in the Data Protection entity of Prism Central to generate recovery points using the same RPO schemes.

Windows VM Provisioning

This section provides information about the windows OS specifications, installation, and configurations that you can perform on a guest VM.

Nutanix VirtIO for Windows

Nutanix VirtIO is a collection of drivers for para-virtual devices that enhance the stability and performance of virtual machines on AHV.

Nutanix VirtIO is available in two formats:

- *VirtIO ISO file* - Use it when VM does not yet have a Windows OS installed. For more information, see Installing or Upgrading Nutanix VirtIO for Windows on page 141.
- *VirtIO MSI installer file* - Use it to install or upgrade VirtIO when Windows OS is installed and running on a VM or VM already has VirtIO installed.

The VirtIO MSI installer file is also bundled with Nutanix Guest Tools (NGT). Install NGT on a VM to install the Nutanix VirtlO Package on the VM. For information on how to install NGT, see NGT Installation in the *Prism Web Console Guide*.

The following table describes the NGT behavior based on AOS release:

Table 18: NGT Behavior - AOS Release

AOS Release	NGT Behavior
Prior to AOS 6.6	NGT includes the VM Mobility package which is a re-packaging of VirtIO. The repackaging is done with additional changes to enable a built-in driver that is pre-installed in Windows but not enabled by default. This driver is used to enable the SCSI controller required by some Windows editions for seamless mobility between different types of hypervisors. In this case, the VM Mobility package uses the same version numbering as VirtIO.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1435

AOS Release	NGT Behavior
AOS 6.6 and above	NGT contains both a VirtIO and a VM Mobility packages. The Nutanix VirtIO contains all VirtIO drivers, and the VM Mobility package is no longer re-packaged with VirtIO drivers and contains only the change to enable SCSI controller. The NGT release is aligned with the AOS release and the NGT contains the latest VirtIO package available at the time of NGT release. However, there is no back-porting of NGT release alignment with the previous AOS releases. **Caution:** If you install an older version of NGT, the latest VirtIO version, even if installed, is replaced by the older VirtIO version. The VirtIO release is not aligned with the AOS release. To ensure that you have the latest VirtIO drivers, either install the latest NGT version or update the drivers using the latest VirtIO package available on the Nutanix Support portal. For more information, see Installing or Upgrading Nutanix VirtIO for Windows on page 141.

VirtIO Requirements

Requirements for Nutanix VirtIO for Windows.

VirtIO supports the following operating systems:

- Microsoft Windows server version: Windows 2008 R2 or later
- Microsoft Windows client version: Windows 7 or later

Note: On Windows 7 and Windows Server 2008 R2, install Microsoft KB3033929 or update the operating system with the latest Windows Update to enable support for SHA2 certificates.

Caution: The VirtIO installation or upgrade may fail if multiple Windows VSS snapshots are present in the guest VM. The installation or upgrade failure is due to the timeout that occurs during installation of *Nutanix VirtIO SCSI pass-through controller* driver.

It is recommended to clean up the VSS snapshots or temporarily disconnect the drive that contains the snapshots. Ensure that you only delete the snapshots that are no longer needed. For more information about how to observe the VirtIO installation or upgrade failure that occurs due to availability of multiple Windows VSS snapshots, see KB-12374.

Installing or Upgrading Nutanix VirtIO for Windows

Download Nutanix VirtIO and the Nutanix VirtIO Microsoft installer (MSI). The MSI installs and upgrades the Nutanix VirtIO drivers.

Before you begin

Make sure that your system meets the VirtIO requirements described in VirtIO Requirements on page 141.

About this task

If you have already installed Nutanix VirtIO, use the following procedure to upgrade VirtIO to a latest version. If you have not yet installed Nutanix VirtIO, use the following procedure to install Nutanix VirtIO.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1436

Procedure

1. Go to the Downloads page of VirtIO package on Nutanix Support portal.

   Alternatively, you can also click **AHV** in the Downloads page on Nutanix Support portal, and select **VirtIO** from the dropdown list.

2. Select the appropriate VirtIO package.

   » If you are creating a new Windows VM, download the ISO file. The installer is available on the ISO if your VM does not have Internet access.

   » If you are updating drivers in a Windows VM, download the MSI installer file.

Figure 18: Search filter and VirtIO options

3. Run the selected package.

   » For the ISO: Upload the ISO to the cluster, as described in the Configuring Images topic in *Prism Element Web Console Guide*.

   » For the MSI: open the download file to run the MSI.

4. Read and accept the Nutanix VirtIO license agreement. Click **Install**.

Figure 19: Nutanix VirtIO Windows Setup Wizard

The Nutanix VirtIO setup wizard shows a status bar and completes installation.

Manually Installing or Upgrading Nutanix VirtIO
Manually install or upgrade Nutanix VirtIO.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1437

Before you begin

Make sure that your system meets the VirtIO requirements described in VirtIO Requirements on page 141.

About this task

> **Note:** To automatically install Nutanix VirtIO, see Installing or Upgrading Nutanix VirtIO for Windows on page 141.

If you have already installed Nutanix VirtIO, use the following procedure to upgrade VirtIO to a latest version. If you have not yet installed Nutanix VirtIO, use the following procedure to install Nutanix VirtIO.

Procedure

1. Go to the Downloads page of VirtIO package on Nutanix Support portal.

   Alternatively, you can also click **AHV** in the Downloads page on Nutanix Support portal, and select **VirtIO** from the dropdown list.

2. Do one of the following:

   » Extract the VirtIO ISO into the same VM where you load Nutanix VirtIO, for easier installation.

   If you choose this option, proceed directly to step 7.

   » Download the VirtIO ISO for Windows to your local machine.

   If you choose this option, proceed to step 3.

3. Upload the ISO to the cluster, as described in the Configuring Images topic of *Prism Element Web Console Guide*.

4. Locate the VM where you want to install the Nutanix VirtIO ISO and update the VM.

5. Add the Nutanix VirtIO ISO by clicking **Add New Disk** and complete the indicated fields.

   - **TYPE**: **CD-ROM**
   - **OPERATION**: **CLONE FROM IMAGE SERVICE**
   - **BUS TYPE**: **IDE**
   - **IMAGE**: Select the Nutanix VirtIO ISO

6. Click **Add**.

7. Log on to the VM and browse to **Control Panel** > **Device Manager**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1438

8. **Note:** Select the `x86` subdirectory for 32-bit Windows, or the `amd64` for 64-bit Windows.

   Open the devices and select the specific Nutanix drivers for download. For each device, right-click and **Update Driver Software** into the drive containing the VirtIO ISO. For each device, follow the wizard instructions until you receive installation confirmation.

   a. **System Devices** > **Nutanix VirtIO Balloon Drivers**

   b. **Network Adapter** > **Nutanix VirtIO Ethernet Adapter**.

   c. **Processors** > **Storage Controllers** > **Nutanix VirtIO SCSI pass through Controller**
      The Nutanix VirtIO SCSI pass-through controller prompts you to restart your system. Restart at any time to install the controller.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1439

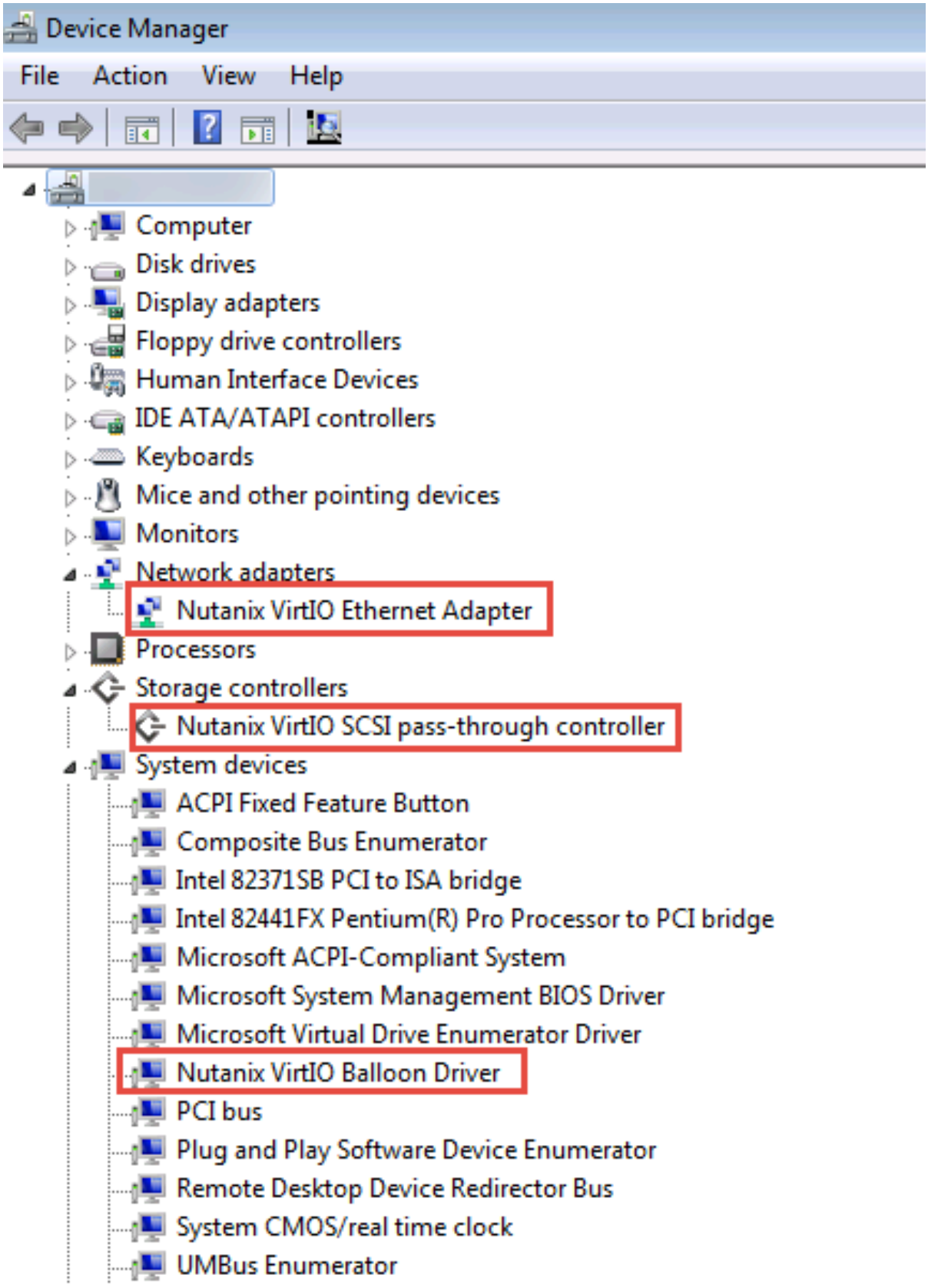


Figure 20: List of Nutanix VirtIO downloads

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1440

Creating a Windows VM on AHV with Nutanix VirtIO

Create a Windows VM in AHV, or migrate a Windows VM from a non-Nutanix source to AHV, with the Nutanix VirtIO drivers.

Before you begin

- Upload the Windows installer ISO to your cluster as described in the Configuring Images topic in *Web Console Guide*.
- Upload the Nutanix VirtIO ISO to your cluster as described in the Configuring Images topic in *Web Console Guide*.

About this task

To install a new or migrated Windows VM with Nutanix VirtIO, complete the following.

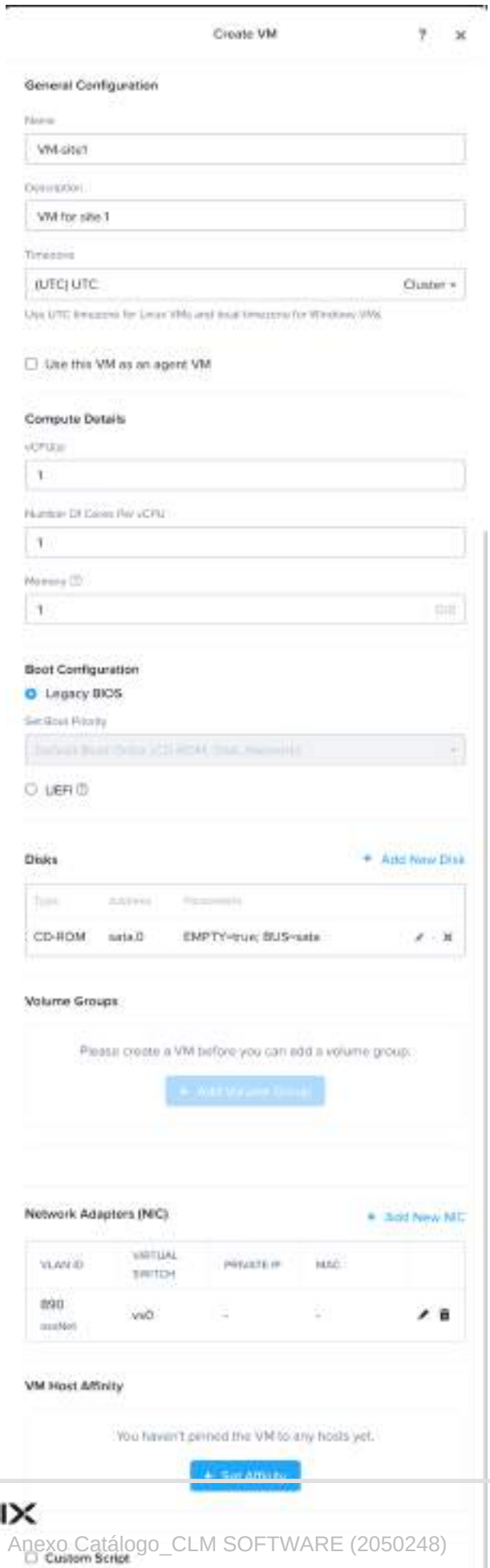
Procedure

1. Log on to the Prism web console using your Nutanix credentials.
2. At the top-left corner, click **Home** > **VM**.
   The **VM page** appears.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1441

3. Click **+ Create VM** in the corner of the page.
   The **Create VM** dialog box appears.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1442


Create VM
General Configuration
VM for site 1
(UTC) UTC
Cluster
Use this VM as an agent VM
Compute Details
1
1
1
Boot Configuration
Legacy BIOS
UEFI
Disks
Add New Disk
CD-ROM
sata.0
EMPTY=true; BUS=sata
Volume Groups
Please create a VM before you can add a volume group.
Network Adapters (NIC)
Add New NIC
VLAN ID
VIRTUAL SWITCH
PRIVATE IP
MAC
vs0
VM Host Affinity
You haven't pinned the VM to any hosts yet.
Custom Script

4. Complete the indicated fields.

   a. **NAME**: Enter a name for the VM.

   b. **Description** (optional): Enter a description for the VM.

   c. **Timezone**: Select the timezone that you want the VM to use. If you are creating a Linux VM, select **(UTC) UTC**.

      > **Note:**
      >
      > The RTC of Linux VMs must be in UTC, so select the UTC timezone if you are creating a Linux VM.
      >
      > Windows VMs preserve the RTC in the local timezone, so set up the Windows VM with the hardware clock pointing to the desired timezone.

   d. **Number of Cores per vCPU**: Enter the number of cores assigned to each virtual CPU.

   e. **MEMORY**: Enter the amount of memory for the VM (in GiB).

5. If you are creating a Windows VM, add a Windows CD-ROM to the VM.

   a. Click the pencil icon next to the CD-ROM that is already present and fill out the indicated fields.

      - **OPERATION**: **CLONE FROM IMAGE SERVICE**
      - **BUS TYPE**: **SATA**

        > **Note:** If **Secured Boot** is enabled for **UEFI** boot configuration, the **IDE** interface is not supported for CD-ROM. You must use **SATA** as the **BUS TYPE** for CD-ROM. For more information, see Secure Boot Support for VMs on page 194.

      - **IMAGE**: Select the Windows OS install ISO.

   b. Click **Update**.
   The current CD-ROM opens in a new window.

6. Add the Nutanix VirtIO ISO.

   a. Click **Add New Disk** and complete the indicated fields.

      - **TYPE**: **CD-ROM**
      - **OPERATION**: **CLONE FROM IMAGE SERVICE**
      - **BUS TYPE**: **SATA**

        > **Note:** If **Secured Boot** is enabled for **UEFI** boot configuration, the **IDE** interface is not supported for Nutanix VirtIO ISO. You must use **SATA** as the **BUS TYPE** for Nutanix VirtIO ISO. For more information, see Secure Boot Support for VMs on page 194.

      - **IMAGE**: Select the Nutanix VirtIO ISO.

   b. Click **Add**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1444

7. Add a new disk for the hard drive.

   a. Click **Add New Disk** and complete the indicated fields.

      - **TYPE**: **DISK**
      - **OPERATION**: **ALLOCATE ON STORAGE CONTAINER**
      - **BUS TYPE**: **SCSI**

        Note: SCSI bus is the preferred bus type and it is used in most cases. For more information, see Compatibility and Interoperability Matrix for AHV Guest OS.

      - **STORAGE CONTAINER**: Select the appropriate storage container.
      - **SIZE**: Enter the number for the size of the hard drive (in GiB).

   b. Click **Add** to add the disk driver.

8. If you are migrating a VM, create a disk from the disk image.

   a. Click **Add New Disk** and complete the indicated fields.

      - **TYPE**: **DISK**
      - **OPERATION**: **CLONE FROM IMAGE**
      - **BUS TYPE**: **SCSI**

        Note: SCSI bus is the preferred bus type and it is used in most cases. For more information, see Compatibility and Interoperability Matrix for AHV Guest OS.

      - **CLONE FROM IMAGE SERVICE**: Click the drop-down menu and choose the image you created previously.

   b. Click **Add** to add the disk driver.

9. Optionally, after you have migrated or created a VM, add a network interface card (NIC).

   a. Click **Add New NIC**.

   b. In the **VLAN ID** field, choose the VLAN ID according to network requirements and enter the IP address, if necessary.

   c. Click **Add**.

10. Click **Save**.

What to do next

Install Windows by following Installing Windows on a VM on page 150.

Installing Windows on a VM

Install a Windows virtual machine.

Before you begin

Create a Windows VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1445

Procedure

1. Log on to the Prism Element web console.
2. Click **Home** > **VM** to open the VM dashboard.
3. Select the Windows VM.
4. In the center of the VM page, click **Power On**.
5. Click **Launch Console**.
   The Windows console opens in a new window.
6. Select the desired language, time and currency format, and keyboard information.
7. Click **Next** > **Install Now**.
   The Windows setup dialog box shows the operating systems to install.
8. Select the Windows OS you want to install.
9. Click **Next** and accept the license terms.
10. Click **Next** > **Custom: Install Windows only (advanced)** > **Load Driver** > **OK** > **Browse**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1446

11. Choose the Nutanix VirtIO driver.

    a. Select the Nutanix VirtIO CD drive.

    b. Expand the Windows OS folder and click **OK**.

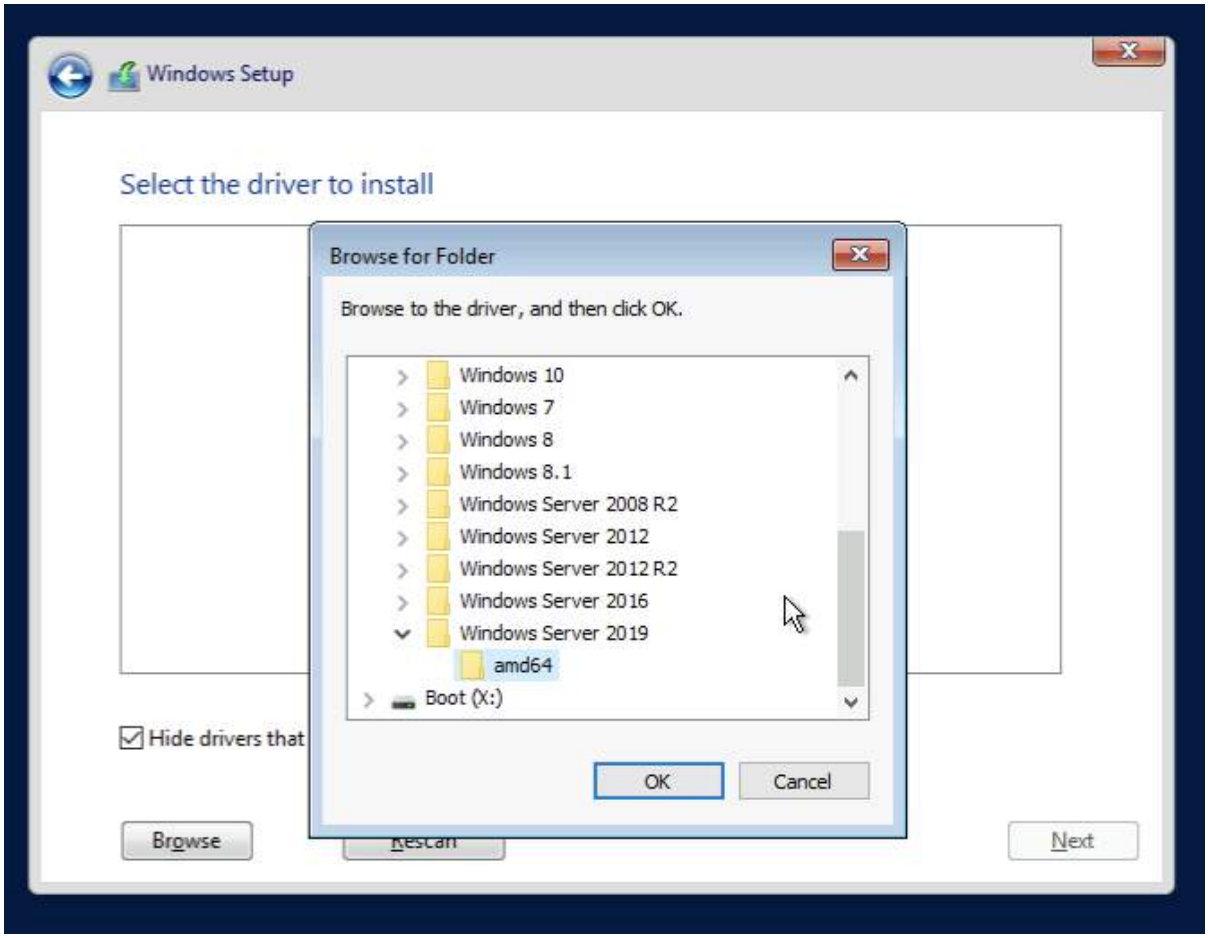


Figure 22: Select the Nutanix VirtIO drivers for your OS

The **Select the driver to install** window appears.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1447

12. Select the VirtIO SCSI driver (vioscsi.inf) and click **Next**.

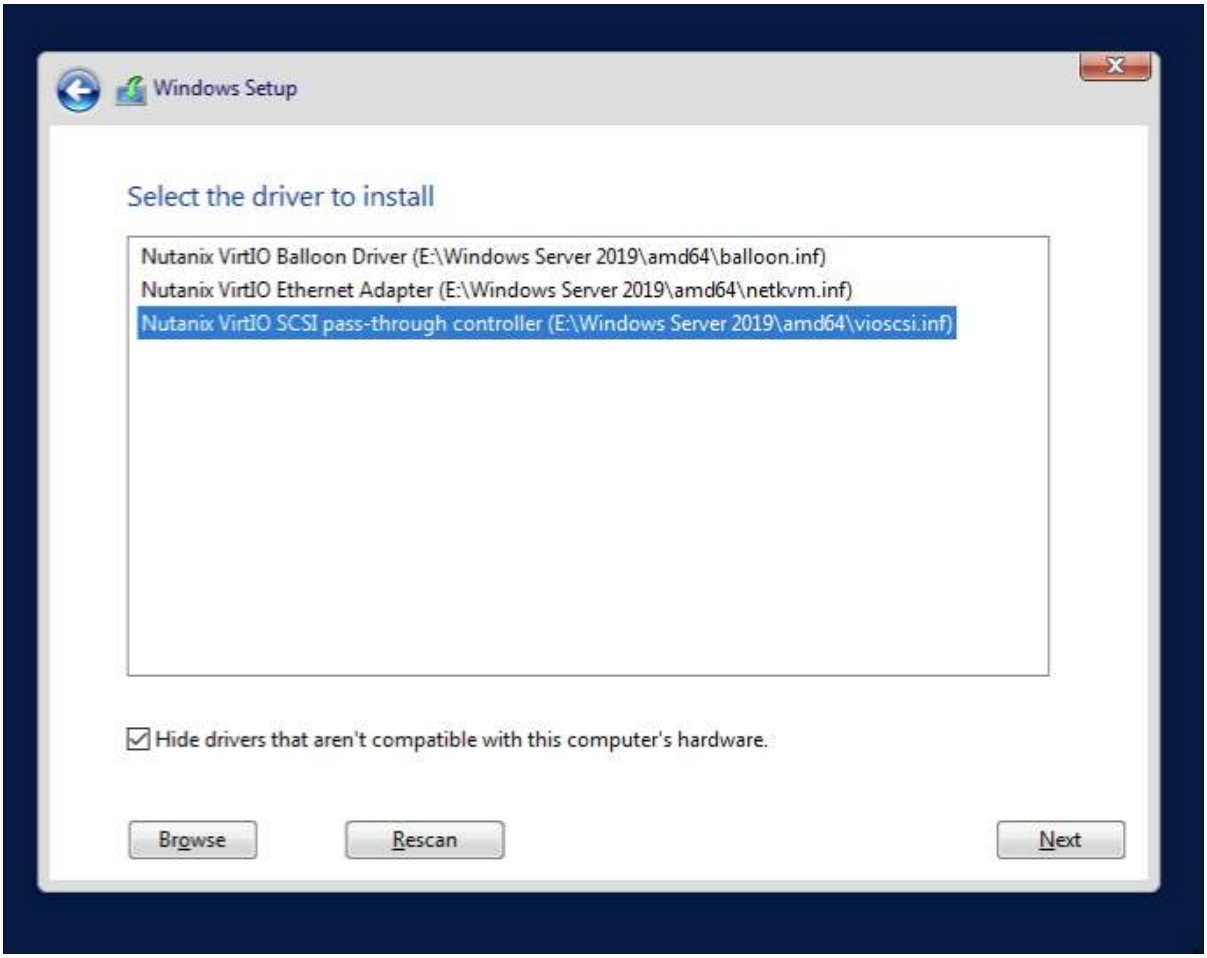


Figure 23: Select the Driver for Installing Windows on a VM

The amd64 folder contains drivers for 64-bit operating systems. The x86 folder contains drivers for 32-bit operating systems.

> **Note:** From Nutanix VirtIO driver version 1.1.5, the driver package contains Windows Hardware Quality Lab (WHQL) certified driver for Windows.

13. Select the allocated disk space for the VM and click **Next**.
    Windows shows the installation progress, which can take several minutes.

14. Enter your user name and password information and click **Finish**.
    Installation can take several minutes.
    Once you complete the login information, Windows setup completes installation.

15. Follow the instructions in Installing or Upgrading Nutanix VirtIO for Windows on page 141 to install other drivers which are part of Nutanix VirtIO package.

Windows Defender Credential Guard Support in AHV

AHV enables you to use the Windows Defender Credential Guard security feature on Windows guest VMs.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1448

Windows Defender Credential Guard feature of Microsoft Windows operating systems allows you to securely isolate user credentials from the rest of the operating system. By that means, you can protect guest VMs from credential theft attacks such as Pass-the-Hash or Pass-The-Ticket.

For more information on the Windows Defender Credential Guard security feature, see the Microsoft documentation.

Windows Defender Credential Guard Architecture in AHV

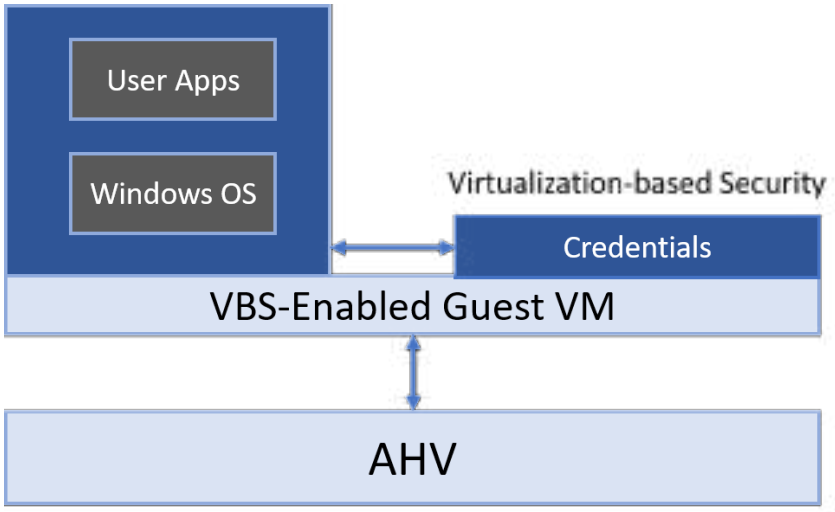


Figure 24: Windows Defender Credential Guard Architecture

Windows Defender Credential Guard uses Microsoft virtualization-based security to isolate user credentials in the virtualization-based security (VBS) module in AHV. When you enable Windows Defender Credential Guard on an AHV guest VM, the guest VM runs on top of AHV running both the Windows OS and VBS. Each Windows OS guest VM, which has Windows Defender Credential Guard enabled, has a VBS to securely store credentials.

Windows Defender Credential Guard Requirements

Ensure the following to enable Windows Defender Credential Guard:

1. AOS, AHV, and Windows Server versions support Windows Defender Credential Guard:
   - AOS version must be 5.19 or later
   - AHV version must be AHV 20201007.1 or later
   - Windows Server version must be Windows server 2016 or later, Windows 10 Enterprise or later and Windows Server 2019 or later
2. UEFI, Secure Boot, and machine type q35 are enabled in the Windows VM from AOS.

   The Prism Element workflow to enable Windows Defender Credential Guard includes the workflow to enable these features.

Windows Defender Credential Guard Limitations

The following limitations apply to the guest VMs with Windows Defender Credential Guard enabled:

- VM Live migration is only supported between the nodes with Skylake or newer Intel CPU generation. While expanding the cluster, if you add a node with CPU generation prior to Skylake, the system generates an alert *VMs became non-migratable due to node addition* after cluster expansion. Nutanix recommends you remove the nodes with older CPU generation, power-off , and then power-on affected guest VMs to re-enable VM live migration support. For more information, see KB-15227.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1449

- Both the Cross Cluster Live Migration (CCLM) and On-Demand CCLM (OD-CCLM) are not supported on guest VMs that have Windows Defender Credential Guard enabled.
- The following optional configurations are not supported:
  - Virtual GPU (vGPU) configurations.
  - Virtual Trusted Platform Modules (vTPM) to store MS policies.

    Note: vTPM is supported with AOS 6.5.1 or later and AHV 20220304.242 or later release versions only.
  - DMA protection (vIOMMU).
  - Cross Hypervisor Disaster Recovery (CHDR).
  - Starting with AOS 6.8 release, AHV supports the live migration of the guest VMs that have Windows Defender Credential Guard enabled. When you upgrade to AOS 6.8 or later release and enable HA reservation for the cluster, the system reserves the resources to accommodate the HA event. However, if you have the existing guest VMs in the cluster that have Windows Defender Credential Guard enabled, some guest VMs (both with or without Windows Defender Credential Guard enabled) might fail to start due to the unavailability of sufficient resources in the cluster. Ensure that you have sufficient resources available in the cluster to accommodate the HA reservation.

    For information on how to enable HA reservation, see Enabling High Availability for the Cluster section in *Prism Web Console Guide*

Caution: If you enable Windows Defender Credential Guard on the guest VMs in an AHV cluster, the VM density drops, which affects the VM performance. This is due to nested virtualization overhead added as a result of enabling Windows Defender Credential Guard. Nutanix recommends that you ascertain the impact on the guest VM performance in a test environment, before you enable Windows Defender Credential Guard in the production environment.

Enabling Windows Defender Credential Guard Support in AHV Guest VMs

You can enable Windows Defender Credential Guard when you are either creating a VM or updating a VM.

Before you begin

Ensure that the following prerequisites are met before you enable Windows Defender Credential Guard for a guest VM:

- Observe the Windows Defender Credential Guard Limitations on page 154.
- Adhere to the Windows Defender Credential Guard Requirements on page 154.
- Enable UEFI, Secure Boot, and machine type q35 in the Windows VM from AOS. For more information, see UEFI Support for VM on page 187.

About this task

Perform the following procedure to enable Windows Defender Credential Guard:

Procedure

1. Enable Windows Defender Credential Guard when you are either creating a VM or updating a VM. Do one of the following:
   - » If you are creating a VM, see step 2.
   - » If you are updating a VM, see step 3.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1450

2. If you are creating a Windows VM, do the following:
   a. Log on to the Prism Element web console.
   b. In the VM dashboard, click **Create VM**.
   c. Fill in the mandatory fields to configure a VM.
   d. Under **Boot Configuration**, select **UEFI**, and then select the **Secure Boot** and **Windows Defender Credential Guard** options.
   e. Proceed to configure other attributes for your Windows VM.
      See Creating a Windows VM on AHV with Nutanix VirtIO on page 146 for more information.
   f. Click **Save**.
   g. Turn on the VM.
3. If you are updating an existing VM, do the following:
   a. Log on to the Prism Element web console.
   b. In the VM dashboard, click the **Table** view, select the VM, and click **Update**.
   c. Under **Boot Configuration**, select **UEFI**, and then select the **Secure Boot** and **Windows Defender Credential Guard** options.

      Note:

      If the VM is configured to use BIOS, install the guest OS again.

      If the VM is already configured to use UEFI, skip the step to select Secure Boot.

      See UEFI Support for VM on page 187 and Secure Boot Support for VMs on page 194 for more information about these features.
   d. Click **Save**.
   e. Turn on the VM.
4. Enable Windows Defender Credential Guard in the Windows VM by using group policy.

   See the *Enable Windows Defender Credential Guard by using the Group Policy* procedure of the *Manage Windows Defender Credential Guard* topic in the Microsoft documentation to enable VBS, Secure Boot, and Windows Defender Credential Guard for the Windows VM.
5. Open command prompt in the Windows VM and apply the **Group Policy** settings:

   ```
   > gpupdate /force
   ```

   If you have not enabled Windows Defender Credential Guard (step 4) and perform this step (step 5), a warning similar to the following is displayed:

   ```
   Updating policy...

   Computer Policy update has completed successfully.

   The following warnings were encountered during computer policy processing:

   Windows failed to apply the {F312195E-3D9D-447A-A3F5-08DFFA24735E} settings.
    {F312195E-3D9D-447A-A3F5-08DFFA24735E} settings might have its own log file. Please
    click on the "More information" link.
   User Policy update has completed successfully.
   ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1451

```
For more detailed information, review the event log or run GPRESULT /H GPReport.html
 from the command line to access information about Group Policy results.
```

Event Viewer displays a warning for the group policy with an error message that indicates Secure Boot is not enabled on the VM.

To view the warning message in Event Viewer, do the following:

- In the Windows VM, open **Event Viewer**.
- Go to **Windows Logs** -> **System** and click the warning with the **Source** as **GroupPolicy (Microsoft-Windows-GroupPolicy)** and **Event ID** as **1085**.

> **Note:** Ensure that you follow the steps in the order that is stated in this document to successfully enable Windows Defender Credential Guard.

6. Restart the VM.
7. Verify if Windows Defender Credential Guard is enabled in your Windows VM.
   a. Start a Windows PowerShell terminal.
   b. Run the following command.

```
PS > Get-CimInstance -ClassName Win32_DeviceGu
ard -Namespace 'root\Microsoft\Windows\DeviceGuard'
```

An output similar to the following is displayed.

```
PS > Get-CimInstance -ClassName Win32_DeviceGuard -Namespace 'root\Microsoft
\Windows\DeviceGuard'
AvailableSecurityProperties               : {1, 2, 3, 5}
CodeIntegrityPolicyEnforcementStatus      : 0
InstanceIdentifier                        : 4ff40742-2649-41b8-bdd1-e80fad1cce80
RequiredSecurityProperties                : {1, 2}
SecurityServicesConfigured                : {1}
SecurityServicesRunning                   : {1}
UsermodeCodeIntegrityPolicyEnforcementStatus : 0
Version                                   : 1.0
VirtualizationBasedSecurityStatus         : 2
PSComputerName
```

Confirm that both **SecurityServicesConfigured** and **SecurityServicesRunning** have the value **{ 1 }**.

Alternatively, you can verify if Windows Defender Credential Guard is enabled by using System Information (msinfo32):

a. In the Windows VM, open **System Information** by typing **msinfo32** in the search field next to the **Start** menu.
b. Verify if the following parameter values are available:
   - Virtualization-based security = Running
   - Virtualization-based security Required Security Properties = Base Virtualization Support, Secure Boot
   - Virtualization-based security Available Security Properties = Base Virtualization Support, Secure Boot, UEFI Code Readonly
   - Virtualization-based security Services Configured = Credential Guard
   - Virtualization-based security Services Running = Credential Guard

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1452

Windows Subsystem for Linux (WSL2) Support on AHV

AHV supports WSL2 that enables you to run a Linux setup on a Windows OS without a dedicated VM and dual-boot environment.

For more information about WSL, see the *What is the Windows Subsystem for Linux?* topic in Microsoft Technical Documentation.

Note:

- Both hardware and software support are required to enable a guest VM to communicate with its nested guest VMs in a WSL2 setup.
- WSL2 requires nested virtualization, which affects guest VM performance. Ensure to validate that the performance of VMs with WSL2 enabled meets your expectations.
- Starting from AOS 7.0 release, with a minimum required AHV version of 10.0, AHV by default supports the live migration of the WSL2-enabled guest VMs.
- To enable live migration support for existing WSL2-enabled VMs, do the following:
  - Upgrade AOS to 7.0 release, with a minimum required AHV version of 10.0.
  - Power off and power on.

WSL2 Limitations

The following table provides the information about the limitations that are applicable for WSL2 based on the AOS and AHV version:

Table 19: WSL2 Limitations

AOS Version	AHV Version	WSL2 Limitations
AOS 6.5.1	AHV 20201105.30411 (default bundled AHV with AOS 6.5.1)	The following optional configurations are not supported: • vTPM (Virtual Trusted Platform Modules) to store MS policies • Hosts with AMD CPUs • Nutanix Live Migration • Cross hypervisor DR of WSL2 VM
AOS 6.5.1 to AOS 6.6.2.8	AHV 20220304.242 to AHV-20220304.10057	The following optional configurations are not supported: • Hosts with AMD CPUs • Nutanix Live Migration • Cross hypervisor DR of WSL2 VM

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1453

AOS Version	AHV Version	WSL2 Limitations
AOS 6.7 and 6.8	AHV-20230302.207 (default bundled AHV with AOS 6.7) or recommended AHV version for later AOS releases. **Note:** From AOS 6.8 release onwards, AOS does not include the AHV installation bundle. Download the AHV installer bundle from the Downloads page on Nutanix portal.	The following optional configurations are not supported: • Nutanix Live Migration • Cross hypervisor DR of WSL2 VM
AOS 7.0 or later	From AHV 10.0 or later	Cross hypervisor DR of WSL2 VM

Enabling WSL2 on AHV

This section provides the information on how to enable the WSL2 on AHV.

Before you begin

Ensure that the following prerequisites are met before you enable WSL2 on AHV:

- Observe the WSL2 Limitations on page 158.
- Deploy AOS 6.5.1 or later along with AHV 20220304.242 or later release version at your site.
- Enable UEFI, Secure Boot, and machine type q35 in the Windows VM from AOS. For more information, see UEFI Support for VM on page 187.

About this task

Note:

In the following procedure, ensure that you replace the <VM_name> with the actual guest VM name.

To configure WSL2 on AHV:

Procedure

1. Power off the guest VM on which you want to configure WSL2.
2. Log on to any CVM in the cluster with SSH.
3. Run the following command to enable the guest VM to support WSL2:

```
nutanix@CVM~ $ acli vm.update <VM_name> hardware_virtualization=true
```

Note: You can also create a new guest VM (Windows VM) on AHV with Nutanix VirtIO. For more information, see Creating a Windows VM on AHV with Nutanix VirtIO on page 146.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1454

4. (Optional) Retrieve the guest VM details using the following command to check whether all the attributes are correctly set for the guest VM:

   ```
   nutanix@CVM~ $ acli vm.get <VM_name>
   ```

   Observe the following log attributes to verify whether the infrastructure to support WSL2 is configured successfully in the guest VM:

   hardware_virtualization: True

5. Power on the guest VM using the following command:

   ```
   nutanix@CVM~ $ acli vm.on <VM_name>
   ```

6. Enable WSL2 on Windows OS. For information on how to install WSL, see *Install WSL* topic in Microsoft Technical Documentation.

VM-Host Affinity Policies

The VM-host affinity policy controls the placement of a VM. You can use this policy to specify that a selected VM can only run on the members of the affinity host list. This policy checks and enforces where a VM can be hosted when you power on or migrate the VM.

Note:

- VMs with VM-Host affinity policies can only be migrated to the hosts specified in the affinity policy. If only one host is specified, the VM cannot be migrated or started on another host during an HA event. For more information, see Non-Migratable VMs on page 171.
- If you choose to apply the VM-host affinity policy, it limits Acropolis HA and Acropolis Dynamic Scheduling (ADS) in such a way that a virtual machine cannot be powered on or migrated to a host that does not conform to requirements of the affinity policy as this policy is enforced mandatorily.
- VMs configured with host affinity settings retain these settings if the VM is migrated to a new cluster. Remove the VM-Host affinity policies applied to a VM that you want to migrate to another cluster, as the UUID of the host is retained by the VM and it does not allow the VM to restart on the destination cluster. When you attempt to protect such VMs, it is successful. However, some disaster recovery operations like migration fail and attempts to power on these VMs also fail.
- The VM-host anti-affinity policy is not supported.

You can define VM-Host affinity policies for a VM at two levels:

VM-Host Affinity Policies defined in Prism Element

In Prism Element, you can define affinity policies at VM level during the VM create or update operation. You can use an affinity policy to specify that a particular VM can only run on the members of the affinity host list. For more information, see VM-Host Affinity Policies Defined in Prism Element on page 160.

VM-Host Affinity Policies defined in Prism Central

In Prism Central, you can define category-based VM-Host affinity policies, where a set of VMs can be affined to run only on a particular set of hosts. Category-based affinity policy enables you to easily manage affinities for a large number of VMs. For more information, see VM-Host Affinity Policies Defined in Prism Central on page 161.

VM-Host Affinity Policies Defined in Prism Element

In Prism Element, you can define scheduling policies for virtual machines on an AHV cluster at a VM level. By defining these policies, you can control the placement of a virtual machine on specific hosts within a cluster.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1455

You can define the VM-Host affinity policies by using Prism Element during the VM create or update operation. For more information, see Creating a VM (AHV).

For information on how the protection domain-based VM-Host affinity policies are handled during disaster recovery, see Affinity Policies Handling - Protection-Domain Based DR Solution with On-prem Clusters Only.

Limitations of Affinity Rules

Even though if a host is removed from a cluster, the host UUID is not removed from the host-affinity list for a VM.

VM-Host Affinity Policies Defined in Prism Central

In Prism Central, you can define the category-based VM-Host affinity policies, where a set of VMs can be affined (correlated) to run only on a particular set of hosts. Category-based affinity policy enables you to easily manage affinities for a large number of VMs. In case of any changes to the affined hosts, you only need to update the category of the host, and it updates the affinity policy for all the affected VMs.

This policy checks and hard enforces where a VM can be hosted when you start or migrate the VM. If there are no resources available on any of the affined hosts, the VM is not started.

> **Note:**
>
> If you create a VM-Host affinity policy for a VM that is configured for asynchronous replication, you must create similar categories and corresponding policies on the remote site as well. If you define similar categories and policies on the remote site, the system applies the affinity policies when the VMs are migrated to the remote site.

For information on how the category-based VM-Host affinity policies are handled during disaster recovery, see Affinity Policies Handling - PC Based DR Solution with Physically Isolated Locations.

Limitations of VM-Host Affinity Policies

VM-Host affinity policies created in Prism Central have the following limitations:

- The minimum supported versions for VM-Host affinity policies are version 6.1 for Prism Element and version 2022.1 for Prism Central.
- Host category attach or detach takes around five minutes to get reflected in the applicable VM-Host affinity policies.

  When you assign a category to a host and map the host category to the VM-Host affinity policy, you can observe that the host count gets updated immediately in the Entities tab. However, the system takes approximately 5 minutes to update the host count in VM-Host Affinity Policies Summary View on page 164.

  The delay in host count update is due to the usage of different APIs to derive the host count in Entities tab and VM-Host Affinity Policies Summary View on page 164.

  For information about how to create a category, see Creating a Category information in *Prism Central Infrastructure Guide*.

  For information on how to assign a category to host, see Associating Hosts with Categories on page 162

  For information on how to create the VM-Host affinity policy and map the host category to the VM-Host affinity policy, see Creating a VM-Host Affinity Policy on page 163.

VM-Host Affinity Policy Configuration Workflow

About this task

To set up VM-Host affinity policy, perform the following steps:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1456

Procedure

1. Create categories for the following entities:

   a. VMs

   b. Hosts

   For information on how to create a category, see Creating a Category information in *Prism Central Infrastructure Guide*.

2. Apply the VM categories to the VMs and host categories to the hosts.

   For information on how to associate a category to the VMs, see Associating VMs with Categories information in *Prism Central Infrastructure Guide* . For information on associating categories with hosts, see Associating hosts with Categories.

3. Create the VM-Host affinity policy. For more information, see Creating an Affinity Policy information in *Prism Central Infrastructure Guide*.

Associating VMs with Categories

About this task

To associate categories to VMs, perform the following steps:

Procedure

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
   The system displays the **List** tab by default.

3. Select the target VMs checkboxes that you want to associate with a category, and choose **Manage Categories** from the **Actions** dropdown menu.
   The system displays the **Manage VM Categories** window.

4. Type the name of the category in **Set Categories** field.
   The system displays the list of matching categories based on the typed entry.

5. Use the Add icon and Remove Icon explained in Prism Central Landing Page and to add and remove the required categories.

   > **Note:** If the VM category you selected is already part of any affinity policy, the system displays the associated affinity policy details.

6. Click **Save**.

Associating Hosts with Categories

About this task

To associate categories with hosts, perform the following steps:

Procedure

1. Log in to Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1457

2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Hardware** > **Hosts** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
   The system displays the **List** tab by default.
3. Select the target host checkboxes that you want to associate with a category, and choose **Manage Categories** from the **Actions** dropdown menu.
   The system displays the **Manage Host Categories** window.
4. Type the name of the category in **Set Categories** field.
   The system displays the list of matching categories based on the typed entry.
5. Use the Add icon and Remove Icon explained in Prism Central Landing Page and to add and remove the required categories.
6. Click **Save**.

Creating a VM-Host Affinity Policy

About this task

This section describes how to create a VM-Host affinity policy in Prism Central.

Before you begin

Ensure that the following prerequisites are met before you create the VM-Host affinity policy:

- VM and Host categories are created. For information on how to create a category, see Creating a Category in *Prism Central Infrastructure Guide* .
- VMs are associated with VM categories, and hosts with host categories. For more information, see Associating VMs with Categories on page 162 and Associating Hosts with Categories on page 162.

> **Note:**
>
> - The system also allows you to associate VMs with VM category and hosts with host category after creation of VM-Host affinity policy.
> - If you have configured any legacy affinity policy (non-category-based affinity policy) associated with the VMs, you must first remove those legacy affinity policies to allow the creation of category-based VM-Host affinity policies associated with the same VMs.

Procedure

To create the VM-Host affinity policy, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
   The system displays the **List** tab by default.
3. Select **VM-Host Affinity Policies** in the **Policies** tab dropdown menu, and click **Create VM-Host Affinity Policy**.
   The system displays the **Create VM-Host Affinity Policy** window.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1458

4. Specify the following information in the **Create VM-Host Affinity Policy** window:

   - **Name**: Enter the VM-Host affinity policy name.
   - (optional) **Description**: Enter the description for the VM-Host affinity policy.
   - **VM Categories**:Type the name of the VM category. The system displays the list of matching categories based on the typed entry. Use the Add icon and Remove Icon explained in Prism Central Landing Page and to add and remove the required categories.
   - **Host Categories**:Type the name of the host category. The system displays the list of matching categories based on the typed entry. Use the Add icon and Remove Icon explained in Prism Central Landing Page and to add and remove the required categories.

5. Click **Create**.

Managing VM-Host Affinity Policies

This section describes how to manage the existing VM-Host affinity policies in Prism Central.

About this task

You can perform the following actions to manage the existing VM-Host affinity policies in Prism Central:

- Update a VM-Host affinity policy.
- Delete a VM-Host affinity policy.
- Re-enforce a VM-Host affinity policy.

Procedure

To manage the VM-Host affinity policies, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
   The system displays the **List** tab by default.
3. Select **VM-Host Affinity Policies** in the **Policies** tab dropdown menu.
   The system displays the affinity policies created across registered clusters.
4. Select the target VM-Host affinity policy checkbox, and choose **Update** from the **Actions** dropdown menu.
5. Update the fields in the **Update VM-Host Affinity Policy** window as per your requirement, and click **Save**. For information on the fields available in **Update VM-Host Affinity Policy** window, see Creating a VM-Host Affinity Policy on page 163.

   To delete the VM-Host affinity policy, select the target VM-Host affinity policy checkbox and choose **Delete** from the **Actions** dropdown menu. The system prompts you to confirm the delete action. Click **Delete** to confirm the delete affinity policy action.

   To re-enforce the VM-Host affinity policy, select the target VM-Host affinity policy checkbox and choose **Re-enforce** from the **Actions** dropdown menu. The system prompts you to confirm the action. Click **Re-enforce** to apply the updated VM-Host affinity policy.

VM-Host Affinity Policies Summary View

The VM-Host affinity policies summary view enables you to access a list of all the user-defined affinity policies across registered clusters.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1459

To access the summary view of all VM-Host affinity policies:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information on the **Navigation Bar**, see Application-specific Navigation Bar.

   The system displays the **List** tab by default.
3. Select **VM-Host Affinity Policies** in the **Policies** tab dropdown menu.

   The system displays a summary view of VM-Host affinity policies across all registered clusters.

Figure 25: Summary View - All Affinity Policies

Table 20: VM-Host Affinity Policies Page Field Description

Parameter	Description	Values
Name	Displays the VM-Host affinity policy name.	(name)
VMs	Displays the count of VMs associated with the selected VM-Host affinity policy.	(number of VMs)
Hosts	Displays the count of hosts associated with the selected VM-Host affinity policy.	(number of hosts)
VM Compliance Status	Displays the compliance status of the VMs associated with this policy. If the policy is being applied and the compliance status is not yet known, the status is displayed as Pending. If a VM is part of multiple VM-Host affinity policies, the oldest policy is applied on the VM. For rest of the policies, the VM is displayed as non-compliant.	(number of VMs Compliant/Non Compliant/Pending)
Modified By	Displays the name of the user who modified the selected VM-Host affinity policy last time.	(user)
Last Modified	Displays the date and time when the selected VM-Host affinity policy is modified last time.	(date & time)

You can perform the following actions for the affinity policies in the **VM-Host Affinity Policies** summary view:

- Access the detailed information about an individual VM-Host affinity policy. For more information, see VM-Host Affinity Policies Details View on page 166.
- Create a VM-Host affinity policy. For more information, see Creating a VM-Host Affinity Policy on page 163.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1460

- Use the **Actions** dropdown menu to update, delete, or re-enforce VM-Host affinity policy. For more information, see Managing VM-Host Affinity Policies on page 164.

VM-Host Affinity Policies Details View

The VM-Host affinity policy details view allows you access the detailed information about an individual VM-Host affinity policy. It includes four tabs: **Summary**, **Categories**, **Entities** and **Audit**.

To access the details view of an individual VM-Host affinity policy, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information on the **Navigation Bar**, see Application-specific Navigation Bar.

   The system displays the **List** tab by default.
3. Select **VM-Host Affinity Policies** in the **Policies** tab.

   The system displays a summary view of VM-Host affinity policies across all registered clusters.
4. Click the target <*Affinity_Policy_Name*> to view the **Summary** tab of an individual VM-Host affinity policy.

> **Note:** Replace <*VM-Host_Affinity_Policy_Name*> with the actual VM-Host affinity policy name at your site.

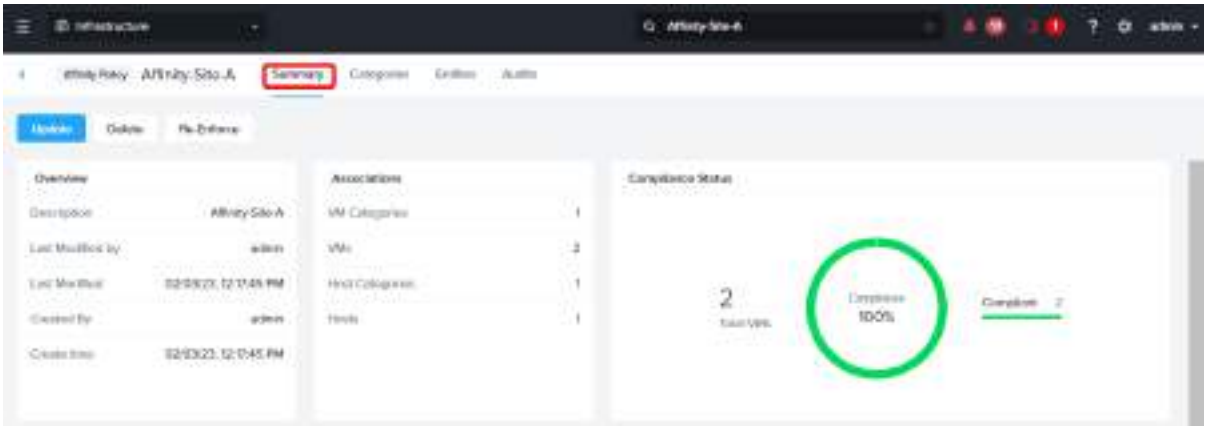


Figure 26: VM-Host Affinity Policies Details view

The **Summary** tab of an individual VM-Host affinity policy provides the following widgets:

- **Overview** - Displays an overview information about the VM-Host affinity policy.
- **Associations**- Displays the associated VM and Host entities and their categories.
- **Compliance Status** - Displays the compliance status of the VMs associated with this policy. If the policy is being applied and the compliance status is not yet known, the status is displayed as Pending. If a VM is part of multiple VM-Host affinity policies, the oldest policy is applied on the VM. For rest of the policies, the VM is displayed as non-compliant.

For information on the fields available in the widgets, see VM-Host Affinity Policy Widgets Field Details on page 166.

<*Action*> available above the widgets. Click the appropriate <*Action*> to run that administrative action on the VM-Host affinity policy. For more information on how to perform any <*Action*>, see Managing VM-Host Affinity Policies on page 164.

VM-Host Affinity Policy Widgets Field Details

The following table describes the fields in the **Overview**, **Associations**, and **Compliance Status** widgets.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1461

Table 21: VM-Host Affinity Policy Widgets Field Description

Field	Description	Values
Overview widget		
Description	Displays the VM-Host affinity policy description specified while creating the VM-Host affinity policy.	(description)
Last Modified By	Displays the name of the user who modified the VM-Host affinity policy last time.	(user)
Last Modified	Displays the date and time when the policy is modified last time.	(date & time)
Created By	Displays the name of the user who created the VM-Host affinity policy	(user)
Create time	Displays the date and time when the VM-Host affinity policy is created.	(date & time)
Associations widget		
VM Categories	Displays the count of VM categories mapped to the selected VM-Host affinity policy.	(number of VM categories)
VMs	Displays the count of VMs associated with the selected VM-Host affinity policy.	(number of VMs)
Host Categories	Displays the count of host categories mapped to the selected VM-Host affinity policy.	(number of host categories)
Hosts	Displays the count of hosts associated with the selected VM-Host affinity policy.	(number of hosts)
Compliance Status widget		
Total VMs	Displays the total number of VMs in the selected VM-Host affinity policy.	(total number of VMs)
Compliance	Displays the compliance status in percentage.	(percentage of complaint VMs)
Compliant, In Progress, or Non compliant	Displays the number of VMs that are compliant and non-compliant with the VM-Host affinity policy. If the compliance check is in progress, the system displays the compliance status as *In progress*.	Compliant, In Progress, or Non compliant

Categories Tab

The **Categories** tab displays the VMs and hosts categories information.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1462

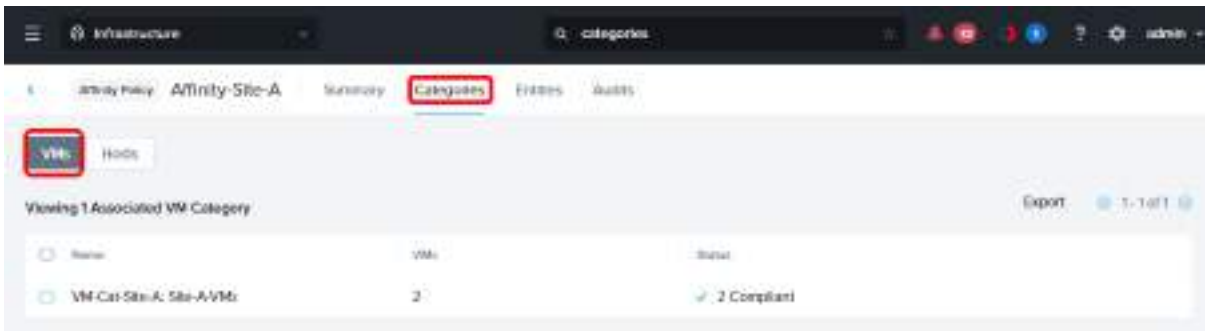


Figure 27: VM-Host Affinity Policies Categories (VMs)

Figure 28: VM-Host Affinity Policies Categories (Hosts)

The following table describes the information displayed in the **Categories** tab

Table 22: Categories Tab Field Description

Field	Description	Values
VMs tab		
Name	Displays the VM category name and its value.	(VM Category Name: Value)
VMs	Displays the count of VMs associated with the selected VM-Host affinity policy.	(number of VMs)
Status	Displays the compliance status.	(number of VMs Compliant|Non-compliant|Pending
Host tab		
Name	Displays the host category name and its value.	(host category Name: Value)
Hosts	Displays the count of hosts associated with the selected VM-Host affinity policy.	(number of hosts)

You can export the table that contains the list of VM categories and host categories and their information to a file in a CSV format. For more information about **Export** option, see Prism Central GUI Organization in *Prism Central Infrastructure Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1463

Entities Tab

The **Entities** tab displays the VMs and hosts entity-related information.

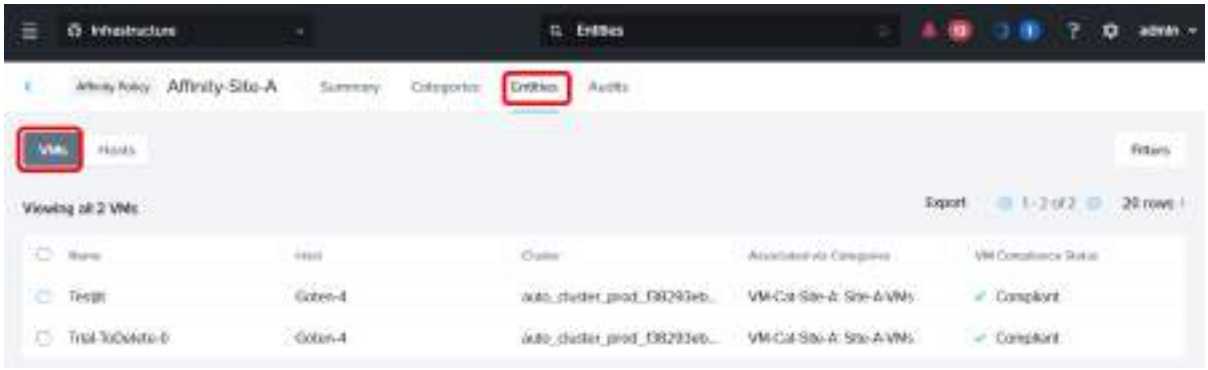


Figure 29: VM-Host Affinity Policies Entities (VMs)

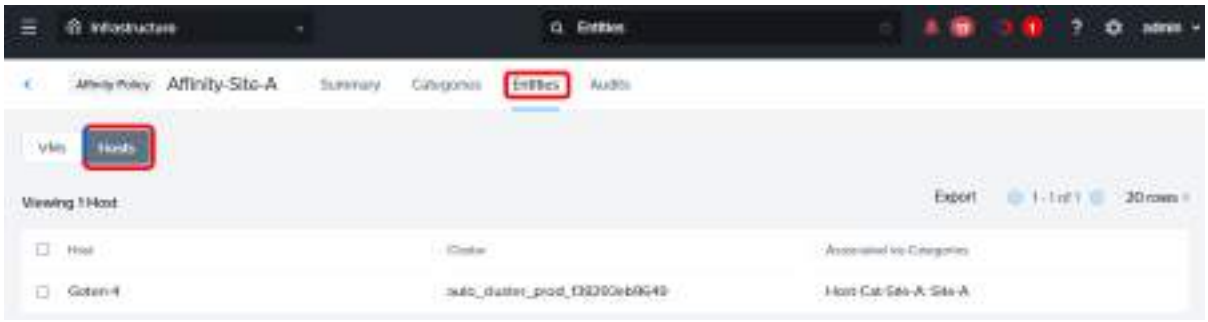


Figure 30: Affinity Policies Entities (Hosts)

The following table describes the information displayed in the **Entities** tab

Table 23: Entities Tab Field Description

Field	Description	Values
VMs tab		
Name	Displays the VM name associated with the selected VM-Host affinity policy.	(VM name)
Host	Displays the host name associated with the selected VM-Host affinity policy.	(host name)
Cluster	Displays the name of the cluster (on which the host resides) associated with the selected VM-Host affinity policy.	(cluster name)
Associated via Categories	Displays the VM category name and its value.	(VM category name: Value)
Compliance Status	Displays the VM compliance status with the selected VM-Host affinity policy.	Compliant|Non-compliant|Pending

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1464

Field	Description	Values
Host tab		
Host	Displays the name of the host associated with the selected VM-Host affinity policy.	(host name
Cluster	Displays the name of the cluster (on which the host resides) associated with the selected VM-Host affinity policy.	(cluster name)
Associated via Categories	Displays the host Category name and its value.	(host category name: Value)

You can export the table that contains the list of VM entities and host entities related information to a file in a CSV format. For more information about **Export** option, see Prism Central GUI Organization in *Prism Central Infrastructure Guide*.

Audits Tab

The **Audits** tab displays the user action-related information for the VM-Host affinity policies.

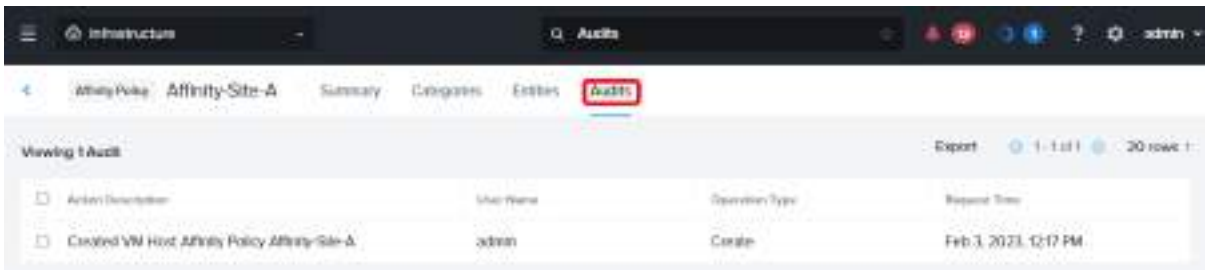


Figure 31: Affinity Policies Audits

The following table describes the information displayed in the **Audits** tab

Table 24: Audits Tab -Field Description

Field	Description	Values
Action Description	Displays the user-action for VM-Host affinity policies.	(action description)
User Name	Displays the name of the user who performed the action.	(host name)
Operation Type	Displays the type of operation performed by the user for VM-Host affinity policies. For example, Create	(cluster name)
Request Time	Displays the date and time of the user action.	(date and time)

You can export the table that contains the list of user actions related information to a file in a CSV format. For more information about **Export** option, see Prism Central GUI Organization in *Prism Central Infrastructure Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1465

Non-Migratable VMs

Guest VMs with GPU passthrough, CPU passthrough, and PCI passthrough, cannot be migrated to other hosts in the cluster.

> **Note:** Guest VMs with host affinity policies also cannot be migrated to other hosts in the cluster, if any of the following condition is met:
>
> - The hosts that are configured as part of the VM-Host affinity policy are not available.
> - The hosts that are part of the VM-Host affinity policy does not have the sufficient resources to run the guest VM.

Such VMs are treated in a different manner in scenarios where VMs are required to migrate to other hosts in the cluster.

Table 25: Scenarios Where VMs Are Required to Migrate to Other Hosts

Scenario	Behavior
One-click upgrade	VM is powered off.
Life-cycle management (LCM)	Pre-check for LCM fails and the VMs are not migrated.
Rolling restart	VM is powered off.
AHV host maintenance mode	Use the tunable option to shut down the VMs while putting the node in maintenance mode. For more information, see Putting a Node into Maintenance Mode using CLI on page 30.

Disaster Recovery Specifications for VM-Host Affinity Policies

This section describes how VM-Host affinity policies are handled in the Disaster Recovery scenario.

Affinity Policies Handling: PC-based DR Solution

This section provides the information about how to handle the affinity policies at the recovery site in a Prism Central-based DR setup.

Failover Phase

After the failover is completed, the VM categories created on the primary site (primary AZ) are synchronized to the recovery site (recovery AZ). The synchronized VM categories are also reflected in the Prism Central instance of the recovery site. The system applies any host affinity policy that exists on the recovery site with synchronized VM categories.

To set up the affinity policies at the recovery site, perform the following actions before a disaster occurs:

1. Create the host categories at the recovery site. For more information, see Creating a Category in *Prism Central Infrastructure Guide*.
2. Create the VM categories at the recovery site with the same name as defined at the primary site. For more information, see Creating a Category in *Prism Central Infrastructure Guide*.
3. Reconfigure the VM affinity policies at the recovery site using the VM categories created in Step 2 and new host categories created in Step 1. For more information, see Creating a VM-Host Affinity Policy on page 163.

> **Important:** If VM-Host affinity policies are defined using Prism element, the VMs never get the affinity after failover, and you need to manually redefine the affinity policies at the recovery site after failover.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1466

Failback Phase

After you perform failback, the VM categories are synchronized back with the primary site, and the affinity policies created on the primary site (primary AZ) are enabled for the VMs.

Synchronous Replication Case

You can also configure the host affinity at the recovery site for the VMs/VM categories that are protected with synchronous replication schedule in the primary site using the following work-flow:

1. Create the host category at the recovery site. For more information, see Creating a Category in *Prism Central Infrastructure Guide*.
2. Create the VM categories at the recovery site with the same name as defined at the primary site. For more information, see Creating a Category in *Prism Central Infrastructure Guide*.
3. Create the VM affinity policies at the recovery site using the VM categories created in Step 2 and new host categories created in Step 1. For more information, see Creating a VM-Host Affinity Policy on page 163.

The following table provides information about host-affinity support for the VMs/VM categories that are protected with synchronous replication:

Table 26: VM-Host Affinity with Synchronous Replication RPO

AOS Release deployed at Primary Site	AOS Release deployed at Recovery Site	Is host affinity with Synchronous replication supported?	Workaround
6.7 or later	6.7 or later	Supported	None
6.6	6.7 or later	Not supported	Upgrade primary site to AOS 6.7 or above release and then configure host affinity with synchronous replication at the primary site.
6.7 or later	6.6	Not supported	Upgrade recovery site to AOS 6.7 or above release and then configure host affinity with synchronous replication at the primary site.

For more information about how to configure the protection policy with a synchronous replication schedule, see Creating a Protection Policy in *Nutanix Disaster Recovery Guide*.

Affinity Policies Handling: PD-based DR Solution

At the recovery site (recovery cluster), when you recover a guest VM protected with asynchronous or nearsync replication schedule using local snapshots, the affinity policies also get applied after you restore and never go stale.

Failover and Failback Phase

When you perform the failover or failback action, the system clears all the VM-Host affinity policies defined using Prism element. The guest VMs can start using any host at the current (migrated) site.

Important:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1467

- If all clusters are registered to one Prism Central instance and the VM-Host affinity policies are defined using Prism Central, the system periodically reconciles the affinity policies and enables you to have consistency in the affinity policies defined at the local site.
- If clusters are registered to multiple Prism Central instances and the VM-Host affinity policies are defined using Prism Central, the system clears the affinity policies, and the guest VMs start using any host at the local site.

Role Based Access Control for VM-Host Affinity Policies

This section describes the Role Based Access Control (RBAC) requirements and limitations for the VM-Host affinity policies. For information on RBAC, see Controlling User Access (RBAC) in *Security Guide*.

Role Based Access Control Requirements for VM-Host Affinity Policies

Before you allocate the VM-Host Affinity Policy Related Permissions on page 173, ensure that the following basic permissions are allocated to the admin user or a custom user to access the VM-Host affinity policies framework in Prism Central:

- View VM
- View category

VM-Host Affinity Policy Related Permissions

In addition to the basic permissions to view VM and categories as specified in Role Based Access Control Requirements for VM-Host Affinity Policies on page 173, you can also assign the following permissions to the admin or custom user to manage the VM-Host affinity policies in Prism Central:

Table 27: VM-Host Affinity Policy Related Permissions

Permission	Description
Create_VM_Host_Affinity_Policy	Admin or custom user can create the VM-Host affinity Policies.
View_VM_Host_Affinity_Policy	Admin or custom user can view the VM-Host affinity policies.
Update_VM_Host_Affinity_Policy	Admin or custom user can update the existing VM-Host affinity policies.
Reenforce_VM_Host_Affinity_Policy	Admin or custom user can re-enforce the existing VM-Host affinity policies.
Delete_VM_Host_Affinity_Policy	Admin or custom user can delete the VM-Host affinity policies.

These permissions also facilitate the admin or custom user to manage the legacy affinity policies (affinity policies that are defined in the Prism Element) from Prism Central.

Role-Based Access Control Limitations for VM-Host Affinity Policies

The following table describes the limitations that apply to RBAC for the VM-Host affinity policies:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1468

Table 28: RBAC Limitations for VM-Host Affinity Policies

Permission Assigned to the Admin or Custom user	Admin or Custom User Action	System Behavior	Limitation
Create_VM_Host_Affinity_Policy Update_VM_Host_Affinity_Policy	Admin or custom user creates or updates the VM-Host affinity policy.	The system applies the VM-Host affinity policy to all the VMs associated with the mapped VM categories.	The system does not check whether the admin or the custom user has permission to access the VMs or hosts mapped in the VM-Host affinity policy.
Update VM Categories	Admin or custom user updates a VM category (for example, attaches a VM to a VM category).	The system applies the VM-Host affinity policy to which the VM category is assigned.	The system does not check whether the admin or the custom user has permission to create or update the VM-Host affinity policy.
Update Host Categories	Admin or custom user updates a Host category (for example, attaches a host to a Host category).	The system applies the affinity policy to which the host category is assigned.	The system does not check whether the admin or the custom user has permission to create or update the VM-Host affinity policy.

VM-VM Anti-Affinity Policies

You can use VM-VM anti-affinity policy to specify anti-affinity between the virtual machines. The VM-VM anti-affinity policy keeps the specified virtual machines apart in such a way that when a problem occurs with one host, you should not lose both the virtual machines.

Important:

The VM-VM anti-affinity policy is a preferential policy. The system does not block any VM operation, such as VM maintenance mode or manual live migration of the VM, even if there is a policy violation. For example, when you manually migrate one VM of a VM-VM pair with an anti-affinity policy, the policy is applied on a best-effort basis only.

The Acropolis Dynamic Scheduling (ADS) always attempts to maintain compliance with the legacy VM-VM anti-affinity policy and ensures that the legacy VM-VM anti-affinity policy is enforced on a commercially reasonable effort. For example, if you manually migrate a VM and the migration leads to non-compliance with the legacy VM-VM anti-affinity policy, ADS performs the following actions:

- Ignores compliance to VM-VM anti-affinity policy, if a host is specified during manual migration.
- Attempts to enforce the policy back into compliance on a commercially reasonable effort, if a host is not specified during manual migration.

For more information on ADS, see Acropolis Dynamic Scheduling in AHV on page 8.

Note: If a VM is cloned that has the affinity policies configured, then the policies are not automatically applied to the cloned VM. However, if a VM is restored from a DR snapshot, the policies are automatically applied to the VM.

You can define VM-VM anti-affinity policies for a VM either from aCLI or Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1469

Legacy VM-VM Anti-Affinity Policies using aCLI

You can configure VM-VM anti-affinity policies from aCLI by creating VM groups and then mapping these VM groups to VM-VM anti-affinity policies. For more information, see Configuring Legacy VM-VM Anti-Affinity Policy on page 175.

> **Important:** Starting with the AOS 7.0 and pc.2024.3 release, you can create category based VM-VM anti-affinity policies from Prism Central.

VM-VM Anti-Affinity Policies defined in Prism Central

In Prism Central, you can define category-based VM-VM anti-affinity policies that ensure to run a set of VMs on different hosts, preventing single host failure from impacting all the VMs. The category-based anti-affinity policy allows you to manage anti-affinities for a large number of VMs easily. For more information, see VM-VM Anti-Affinity Policies Defined in Prism Central on page 176.

Configuring Legacy VM-VM Anti-Affinity Policy

To configure the legacy VM-VM anti-affinity policies, you must first define a group and then add all the VMs on which you want to define the legacy VM-VM anti-affinity policy.

About this task

> **Important:** Starting with the AOS 7.0 and pc.2024.3 release, you can create category based VM-VM anti-affinity policies from Prism Central. For more information, see VM-VM Anti-Affinity Policies Defined in Prism Central on page 176.

To configure the legacy VM-VM anti-affinity policy, follow these steps:

Procedure

1. Log on to the Controller VM with SSH session.
2. Create a group:

   ```
   nutanix@cvm$ acli vm_group.create group_name
   ```

   Replace `group_name` with the name of the group.
3. Add the VMs on which you want to define the legacy anti-affinity to the group:

   ```
   nutanix@cvm$ acli vm_group.add_vms group_name vm_list=vm_name
   ```

   Replace `group_name` with the name of the group. Replace `vm_name` with the name of the VMs that you want to define anti-affinity on. In case of multiple VMs, you can specify comma-separated list of VM names.
4. Create the legacy VM-VM anti-affinity policy.

   ```
   nutanix@cvm$ acli vm_group.antiaffinity_set group_name
   ```

   Replace `group_name` with the name of the group.

   After you configure the group and then power on the VMs, the VMs that are part of the group are started (attempt to start) on the different hosts.

   > **Important:**
   >
   > The legacy VM-VM anti-affinity policy is a preferential policy. The system does not block any VM operation, such as VM maintenance mode or manual live migration of the VM, even if there is a policy

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1470

violation. For example, when you manually migrate one VM of a VM-VM pair with an anti-affinity policy, the policy is applied on a commercially reasonable effort only.

The Acropolis Dynamic Scheduling (ADS) always attempts to maintain compliance with the VM-VM anti-affinity policy and ensures that the legacy VM-VM anti-affinity policy is enforced on a commercially reasonable effort. For example, if you manually migrate a VM and the migration leads to non-compliance with the legacy VM-VM anti-affinity policy, the ADS checks if the host is specified in manual migration, and performs the following actions:

- Ignores compliance to the legacy VM-VM anti-affinity policy, if a host is specified during manual migration.
- Attempts to enforce the policy back into compliance on a best-effort basis, if a host is not specified during manual migration.

For more information on ADS, see Acropolis Dynamic Scheduling in AHV on page 8.

Removing Legacy VM-VM Anti-Affinity Policy

Perform the following procedure to remove the legacy VM-VM anti-affinity policy.

Procedure

1. Log on to the Controller VM with SSH session.
2. Remove the legacy VM-VM anti-affinity policy.

   ```
   nutanix@cvm$ acli vm_group.antiaffinity_unset group_name
   ```

   Replace *group_name* with the name of the group.

   The legacy VM-VM anti-affinity policy is removed for the VMs that are present in the group, and they can start on any host during the next power on operation (as necessitated by the ADS feature).

VM-VM Anti-Affinity Policies Defined in Prism Central

This topic describes the VM-VM anti-affinity policies feature available in Prism Central.

In Prism Central, you can define category-based VM-VM anti-affinity policies that run a set of VMs on different hosts, preventing single host failure from impacting all the VMs. The category-based anti-affinity policy allows you easily to manage anti-affinities for a large number of VMs.

The VM-VM anti-affinity policy is soft enforced. The system does not block any operations, such as VM creation, VM updation, upgrades, host maintenance mode, or manual live migration of the VM, even if such operations result in a policy violation.

Disaster Recovery Considerations

If you create a VM-VM anti-affinity policy for a VM that is configured for replication, and you want those policies to be honored on the remote site, then you must create similar categories and corresponding policies on the remote site as well. When you define similar categories and policies on the remote site, the system applies the VM-VM anti-affinity policies to the VMs that you migrate to the remote site. For more information, see Management of VM-VM Anti-Affinity Policies for PC-Based Disaster Recovery Solution on page 185.

VM-VM Anti-Affinity Policies Summary View

Use VM-VM anti-affinity policies summary view to access a list of all user-defined VM-VM anti-affinity policies.

To access the summary view of all the VM-VM anti-affinity policies, follow these steps:

1. Log in to Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1471

2. From the Application Switcher Function, select **Infrastructure** application and from the navigation bar, select **Compute** > **VMs**.

   The system displays the **List** tab by default.
3. From the **Policies** tab dropdown menu, select **VM-VM Anti-affinity Policies**.

   The system displays a summary view of VM-VM anti-affinity policies.

Table 29: VM-VM Anti-affinity Policies Page Field Description

Parameter	Description	Values
Name	Displays the VM-VM anti-affinity policy name.	(name)
Categories	Displays the count of categories associated with the selected VM-VM anti-affinity policy.	(number of categories)
VMs	Displays the count of VMs associated with the selected VM-VM anti-affinity policy.	(number of VMs)
VM Compliance Status	Displays the compliance status of the VMs associated with the VM-VM anti-affinity policy. If the policy is being applied and the compliance status is not yet known, the system displays the compliance status as **Pending**.	(number of VMs Compliant/Non-Compliant/Pending)
Modified By	Displays the name of the user who last modified the selected VM-VM anti-affinity policy.	(user)
Last Modified	Displays the date and time when the selected VM-VM anti-affinity policy is last modified.	(date & time)

You can perform the following actions for the VM-VM anti-affinity policies in the **VM-VM Anti-affinity Policies** summary view:

- Access the detailed information about an individual VM-VM anti-affinity policy. For more information, see VM-VM Anti-Affinity Policies Details View on page 177.
- Create a VM-VM anti-affinity policy. For more information, see Creating a VM-VM Anti-Affinity Policy on page 181.
- Update a VM-VM anti-affinity policy. For more information, see Updating a VM-VM Anti-Affinity Policy on page 182.
- Delete a VM-VM anti-affinity policy. For more information, see Deleting a VM-VM Anti-Affinity Policy on page 183.
- Remove a legacy VM group. For more information, see Removing a Legacy VM Group on page 183.

VM-VM Anti-Affinity Policies Details View

Use VM-VM anti-affinity policy details view to access detailed information about an individual VM-VM anti-affinity policy.

To access the details view of an individual VM-VM anti-affinity policy, follow these steps:

1. Log in to Prism Central.
2. From the Application Switcher Function, select **Infrastructure** application and from the navigation bar, select **Compute** > **VMs**.

   The system displays the **List** tab by default.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1472

3. From the **Policies** tab dropdown menu, select **VM-VM Anti-affinity Policies**.

   The system displays a summary view of VM-VM anti-affinity policies across all registered clusters.
4. Click the target *<VM-VM Anti-Affinity_Policy_Name>* to view the **Summary** tab of an individual VM-VM Anti-affinity policy.

   > **Note:** Replace *<VM-VM Anti-Affinity_Policy_Name>* with the actual anti-affinity policy name at your site.

The **Summary** tab of an individual VM-VM anti-affinity policy provides the following widgets:

- **Overview**: Displays an overview information about the VM-VM anti-affinity policy.
- **Compliance Status**: Displays the compliance status of the VMs associated with this policy. If the policy is being applied and the compliance status is not yet known, the status is displayed as Pending. If a VM is part of multiple VM-VM anti-affinity policies, the oldest policy is applied on the VM. For rest of the policies, the VM is displayed as non-compliant.

For more information, see VM-VM Anti-Affinity Policy Widgets Field Details on page 178.

VM-VM Anti-Affinity Policy Widgets Field Details

The following table describes the fields in the **Overview** and **Compliance Status** widgets.

Table 30: VM-VM Anti Affinity Policy Widgets Field Description

Field	Description	Values
Overview widget		
Description	Displays the VM-VM anti-affinity policy description specified while creating the anti-affinity policy.	(description)
Last Modified By	Displays the name of the user who modified the VM-VM anti-affinity policy last time.	(user)
Last Modified	Displays the date and time when the VM-VM anti-affinity policy is modified last time.	(date & time)
Created By	Displays the name of the user who created the VM-VM anti-affinity policy.	(user)
Create Time	Displays the date and time when the VM-VM anti-affinity policy is created.	(date & time)
Categories	Displays the count of VM categories mapped to the selected VM-VM anti-affinity policy.	(number of VM categories)
Compliance Status widget		
Total VMs (Unique)	Displays the total number of VMs in the selected VM-VM anti-affinity policy.	(total number of VMs)
Compliance	Displays the compliance status in percentage .	(percentage of complaint VMs)
Compliant, In Progress, or Non compliant	Displays the number of VMs that are compliant and non-compliant with the VM-VM anti-affinity policy. If the compliance check is in progress, the system displays the compliance status as *In progress*.	Compliant, In Progress, or Non compliant

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1473

Clusters Tab

The **Clusters** tab displays the associated clusters information.

The following table describes the information displayed in the **Clusters** tab:

Table 31: Clusters Tab Field Description

Field	Description	Values
Name	Displays the cluster name.	(cluster name)
VMs	Displays the count of VMs associated with the selected VM-VM anti-affinity policy.	(number of VMs)
VM Compliance Status	Displays the number of VMs that are compliant and non-compliant with the VM-VM anti-affinity policy. If the compliance check is in progress, the system displays the compliance status as *In progress*.	(number of VMs Compliant|Non-compliant|Pending

You can export the table that contains the list of VMs and their compliance status information to a file in a CSV format. For more information about **Export** option, see Prism Central GUI Organization in *Prism Central Infrastructure Guide*.

Categories Tab

The **Categories** tab displays the associated VM categories information.

The following table describes the information displayed in the **Categories** tab:

Table 32: Categories Tab Field Description

Field	Description	Values
Name	Displays the VM category name and its value.	(VM Category Name: Value)
VMs	Displays the count of VMs associated with the selected VM-VM anti-affinity policy.	(number of VMs)
VM Compliance Status	Displays the number of VMs that are compliant and non-compliant with the VM-VM anti-affinity policy. If the compliance check is in progress, the system displays the compliance status as *In progress*.	(number of VMs Compliant|Non-compliant|Pending

You can export the table that contains the list of associated VM categories and their information to a file in a CSV format. For more information about **Export** option, see Prism Central GUI Organization in *Prism Central Infrastructure Guide*.

VMs Tab

The **VMs** tab displays the VMs information.

The following table describes the information displayed in the **VMs** tab:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1474

Table 33: VMs Tab Field Description

Field	Description	Values
Name	Displays the VM name associated with the selected VM-VM anti-affinity policy.	(VM name)
Host	Displays the host name associated with the selected VM-VM anti-affinity policy.	(host name)
Cluster	Displays the name of the cluster (on which the host resides) associated with the selected VM-VM anti-affinity policy.	(cluster name)
Category	Displays the VM category name and its value.	(VM category name: Value)
VM Compliance Status	Displays the compliance status of the VM. If the policy is being applied and the compliance status is not yet known, the system displays the compliance status as **Pending** VMs that do not adhere to the anti-affinity placements are displayed as non-compliant. The following are the reasons for displaying a VM as non-compliant: • Cluster Not Supported: When the VM is running on clusters earlier to 6.9 version. • Conflicting Legacy Anti-Affinity Policy: When the VM is already part of the PE based legacy policy. • Conflicting Anti-Affinity Policy: When is VM is part of multiple VM-VM anti-affinity policies, the policy having the oldest creation time is applied on the VM. • Not Enough Hosts: The number of powered on VMs is greater than the number of schedulable hosts. • Not Enough Resources: The scheduler is unable to place the VMs in a manner that conforms with the policy.	(Compliant/Pending/ Cluster Not Supported/ Conflicting Legacy Anti-Affinity Policy/Conflicting Anti-Affinity Policy/ Not Enough Hosts/Not Enough Resources)

You can export the table that contains the list of VM entities related information to a file in a CSV format. For more information about **Export** option, see Prism Central GUI Organization in *Prism Central Infrastructure Guide*.

Audits Tab

The **Audits** tab displays the user action-related information for the VM-VM anti-affinity policies.

The following table describes the information displayed in the **Audits** tab:

Table 34: Audits Tab Field Description

Field	Description	Values
Action Description	Displays the user-action for the VM-VM anti-affinity policies.	(action description)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1475

Field	Description	Values
User Name	Displays the name of the user who performed the action.	(host name)
Operation Type	Displays the type of operation performed by the user for the VM-VM anti-affinity policies.	(cluster name)
Request Time	Displays the date and time of the user action.	(date and time)

You can export the table that contains the list of user actions related information to a file in a CSV format. For more information about **Export** option, see Prism Central GUI Organization in *Prism Central Infrastructure Guide*.

Limitations of VM-VM Anti-Affinity Policies

This topic outlines the limitations of the VM-VM anti-affinity policies.

The VM-VM anti-affinity policies created in Prism Central have the following limitations:

- When you attach or detach a VM category, Prism Central takes approximately seven minutes to reflect the change in the applicable VM-VM anti-affinity policies.
- When you assign a category to a VM and map the VM category to the VM-VM anti-affinity policy, you can observe that the VM count updates immediately in the VMs Tab on page 179. However, Prism Central takes approximately seven minutes to update the VM count in the VM-VM Anti-Affinity Policies Summary View on page 176.
- You can associate a maximum of 20 VM categories to a single VM-VM anti-affinity policy.
- When the VM is part of multiple VM-VM anti-affinity policies, the policy with the oldest creation time is applied on the VM.
- When the VM is part of a legacy VM-VM anti-affinity policy and PC based VM-VM anti-affinity policy, the legacy VM-VM anti-affinity policy takes precedence over PC based VM-VM anti-affinity policy.

VM-VM Anti-Affinity Policy Configuration Workflow

This topic describes the workflow to create a VM-VM anti-affinity policy.

About this task

To configure a VM-VM anti-affinity policy, follow these steps:

Procedure

1. Create a category.
   For more information, see Creating a Category information in the *Prism Central Infrastructure Guide*.
2. Apply the category to the VMs.
   For more information on how to associate a category to the VMs, see Associating VMs with Categories.
3. Create the VM-VM anti-affinity policy.
   For more information, see Creating a VM-VM Anti-Affinity Policy on page 181.

Creating a VM-VM Anti-Affinity Policy

This task describes how to create a VM-VM anti-affinity policy from Prism Central.

Before you begin

Ensure that you meet following prerequisites before you create the VM-VM anti-affinity policy:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1476

- You are on AOS 7.0 or later and pc.2024.3 or later.
- A category is created. For information on how to create a category, see Creating a Category in the *Prism Central Infrastructure Guide* .
- VMs are associated with VM categories. For more information, see Associating VMs with Categories on page 162.

  Note: Prism Central also allows you to associate VMs with VM category after creation of VM-VM anti-affinity policy.

- If you configured any legacy VM-VM anti-affinity policy (non-category-based anti-affinity policy) associated with the VMs, you must first remove those legacy anti-affinity policies to allow the creation of category-based anti-affinity policies associated with the same VMs. For more information, see Removing a Legacy VM Group on page 183.

About this task

To create a VM-VM anti-affinity policy, follow these steps:

Procedure

1. Log in to Prism Central.
2. From the Application Switcher Function, select **Infrastructure** application and from the navigation bar, select **Compute** > **VMs**.
   The system displays the **List** tab by default.
3. From the **Policies** tab dropdown menu, select **VM-VM Anti-affinity Policies**.
4. Click **Create VM-VM Anti-affinity Policy**.
5. Enter the following information in the **Create VM-VM Anti-affinity Policy** window:
   - **Name**: Enter the VM-VM anti-affinity policy name.
   - (Optional) **Description**: Enter the description for the VM-VM anti-affinity policy.
   - **VM Categories**: Type the name of the VM category. The system displays the list of matching categories based on the typed entry. Use the add icon and remove icon explained in Prism Central Landing Page to add and remove the required categories.
6. Click **Create**.

Updating a VM-VM Anti-Affinity Policy

This task describes how to update a VM-VM anti-affinity policy from Prism Central.

About this task

To update a VM-VM anti-affinity policy, follow these steps:

Procedure

1. Log in to Prism Central.
2. From the Application Switcher Function, select **Infrastructure** application and from the navigation bar, select **Compute** > **VMs**.
   The system displays the **List** tab by default.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1477

3. From the **Policies** tab dropdown menu, select **VM-VM Anti-affinity Policies**.
   The system displays the VM-VM anti-affinity policies created across registered clusters.
4. Select the target VM-VM anti-affinity policy checkbox, and from the **Actions** dropdown menu, choose **Update**.
5. Update the fields in the **Update VM-VM Anti-affinity Policy** window as needed and click **Update**.
   For information on the fields available in the **Update VM-VM Anti-affinity Policy** window, see Creating a VM-VM Anti-Affinity Policy on page 181.

Deleting a VM-VM Anti-Affinity Policy

This task describes how to delete a VM-VM anti-affinity policy from Prism Central.

About this task

To delete a VM-VM anti-affinity policy, follow these steps:

Procedure

1. Log in to Prism Central.
2. From the Application Switcher Function, select **Infrastructure** application and from the navigation bar, select **Compute** > **VMs**.
   The system displays the **List** tab by default.
3. From the **Policies** tab dropdown menu, select **VM-VM Anti-affinity Policies**.
   The system displays the VM-VM anti-affinity policies created across registered clusters.
4. Select the target VM-VM anti-affinity policy checkbox and from the **Actions** dropdown menu, choose **Delete**.
   The system prompts you to confirm the delete action.
5. Click **Delete**.

Removing a Legacy VM Group

This task describes how to remove a legacy VM Group from Prism Central.

About this task

The VM-VM anti-affinity policies configured from aCLI are called legacy anti-affinity policies and the VM groups mapped to these policies are called legacy VM groups in Prism Central. If you previously created any legacy VM groups that are associated with VM-VM anti-affinity policies, you must first remove those legacy VM groups to use the new Prism Central based VM-VM anti-affinity policies for those VMs.

To remove the legacy VM Group from Prism Central, follow these steps:

Procedure

1. Log in to Prism Central.
2. From the Application Switcher Function, select **Infrastructure** application and from the navigation bar, select **Compute** > **VMs**.
   The system displays the **List** tab by default.
3. From the **Policies** tab dropdown menu, select **VM-VM Anti-affinity Policies**.
   The system displays a summary view of VM-VM anti-affinity policies across all registered clusters.
4. Click **You have Legacy VM Group defined through the CLI** banner.
   The system displays **Legacy VM-VM Anti-affinity Policies** window.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1478

5. Select the target **VM Groups** checkbox, and select **Delete selected group**.

6. Click **Delete**.

Role Based Access Control for the VM-VM Anti-Affinity Policies

This topic describes the Role Based Access Control (RBAC) requirements and limitations for VM-VM anti-affinity policies.

Using RBAC, you can provide the necessary permissions for users to access the VM-VM anti-affinity policies. For information on RBAC, see Controlling User Access (RBAC) in *Security Guide*.

RBAC Requirements for the VM-VM Anti-Affinity Policies

Before you allocate the VM-VM Anti-Affinity Policy Related Permissions on page 184, ensure that the view VM permission is allocated to the admin user or a custom user to access the VM-VM anti-affinity policies in Prism Central.

VM-VM Anti-Affinity Policy Related Permissions

In addition to the view VM permission, you can also assign the following permissions to the admin or custom user to manage the VM-VM anti-affinity policies in Prism Central:

Table 35: VM-VM Anti-Affinity Policy Related Permissions

Permission	Description
Create_VM_Anti_Affinity_Policy	Admin or custom user can create anti-affinity policies.
View_VM_Anti_Affinity_Policy	Admin or custom user can view anti-affinity policies.
Update_VM_Anti_Affinity_Policy	Admin or custom user can update the existing anti-affinity policies.
View_VM_Anti_Affinity_Policy_VM_Compliance_State	Admin or custom user can view the compliance state of anti-affinity policies.
Delete_VM_Anti_Affinity_Policy	Admin or custom user can delete anti-affinity policies.
View_Legacy_VM_Anti_Affinity_Policy	Admin or custom user can view legacy anti-affinity policies.
Delete_Legacy_VM_Anti_Affinity_Policy	Admin or custom user can delete legacy anti-affinity policies.

RBAC Limitations for the VM-VM Anti-Affinity Policies

The following table describes the limitations that apply to RBAC for the VM-VM anti-affinity policies:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1479

Table 36: RBAC Limitations for VM-VM Anti-Affinity Policies

Permission Assigned to the Admin or Custom User	Admin or Custom User Action	System Behavior	Limitation
Create_VM_Anti_Affinity_Policy Update_VM_Anti_Affinity_Policy	Admin or custom user creates or updates the VM-VM anti-affinity policy.	The system applies the VM-VM anti-affinity policy to all VMs associated with the mapped VM categories.	The system does not check whether the admin or the custom user has permission to access the VMs mapped in the VM-VM anti-affinity policy.
Update_VM_Categories	Admin or custom user updates a VM category (for example, attaches a VM to a VM category).	The system applies the VM-VM anti-affinity policy to which the VM category is assigned.	The system does not check whether the admin or the custom user has permission to create or update the VM-VM anti-affinity policy.

Disaster Recovery Specifications for VM-VM Anti-Affinity Policies

This section describes how VM-VM anti-affinity policies are handled in the Disaster Recovery scenario.

Management of VM-VM Anti-Affinity Policies for PC-Based Disaster Recovery Solution

This section describes how to manage VM-VM anti-affinity policies in a Prism Central-based Disaster Recovery (DR) setup.

Managing Failover Operation

This section describes how to set up VM-VM anti-affinity policies at the recovery site for a failover operation.

About this task

After the failover is completed, the VM categories assigned to the VM on the primary site (primary AZ) are synchronized to the recovery site (recovery AZ). The synchronized VM categories are also reflected in the Prism Central instance of the recovery site.

To set up the VM-VM anti-affinity policies at the recovery site, perform the following actions before a disaster occurs:

Procedure

1. Create the VM categories at the recovery site with the same name as defined at the primary site.
   For more information, see Creating a Category in *Prism Central Infrastructure Guide*.
2. Reconfigure the VM-VM anti-affinity policies at the recovery site using the VM categories created at the recovery site.
   For more information, see Creating a VM-VM Anti-Affinity Policy in *Prism Central Infrastructure Guide*.

   Important: If the legacy VM-VM anti-affinity policies are defined using Prism element, the policies are not replicated during failover, and you need to manually redefine the anti-affinity policies at the recovery site after failover.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1480

Overview of Failback Operation

This section describes how failback operation functions for VM-VM anti-affinity policies at the primary site in a Prism Central-based Disaster Recovery setup.

After you perform failback, the VM categories are synchronized back to the primary site, and the anti-affinity policies created on the primary site (primary AZ) are enabled for the VMs.

Managing Synchronous Replication

This section describes how to set up VM-VM anti-affinity policies at the recovery site for a synchronous replication operation.

About this task

You can configure the VM-VM anti-affinity policy at the recovery site for the VMs or VM categories that are protected with synchronous replication schedule in the primary site using the following workflow:

Procedure

1. Create the VM categories at the recovery site with the same name as defined at the primary site.
   For more information, see Creating a Category in *Prism Central Infrastructure Guide*.
2. Create the VM-VM anti-affinity policies at the recovery site using the VM categories created at the recovery site.
   For more information, see Creating a VM-VM Anti-Affinity Policy in *Prism Central Infrastructure Guide*.

   Note: For more information about how to configure the protection policy with a synchronous replication schedule, see Creating a Protection Policy in *Nutanix Disaster Recovery Guide*.

Management of VM-VM Anti-Affinity Policies for PD-based Disaster Recovery Solution

At the recovery site (recovery cluster), when you recover a guest VM protected with asynchronous or nearsync replication schedule using local snapshots, the VM-VM anti-affinity policies also get applied after you restore and never go stale.

Failover and Failback Phase

When you perform the failover or failback action, the system clears all the VM-VM anti-affinity policies defined using Prism element. The guest VMs can start using any host at the current (migrated) site.

Performing Power Operations on VMs by Using Nutanix Guest Tools (aCLI)

You can initiate safe and graceful power operations such as soft shutdown and restart of the VMs running on the AHV hosts by using the aCLI. Nutanix Guest Tools (NGT) initiates and performs the soft shutdown and restart operations within the VM. This workflow ensures a safe and graceful shutdown or restart of the VM. You can create a pre-shutdown script that you can choose to run before a shutdown or restart of the VM. In the pre-shutdown script, include any tasks or checks that you want to run before a VM is shut down or restarted. You can choose to cancel the power operation if the pre-shutdown script fails. If the script fails, an alert (guest_agent_alert) is generated in the Prism web console.

Before you begin

Ensure that you have met the following prerequisites before you initiate the power operations:

1. NGT is enabled on the VM. All operating systems that NGT supports are supported for this feature.
2. NGT version running on the Controller VM and guest VM is the same.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1481

3. (Optional) If you want to run a pre-shutdown script, place the script in the following locations depending on your VMs:

   - Windows VMs: installed_dir\scripts\power_off.bat

     The file name of the script must be **power_off.bat**.

   - Linux VMs: installed_dir/scripts/power_off

     The file name of the script must be **power_off**.

About this task

> **Note:** You can also perform these power operations by using the V3 API calls. For more information, see developer.nutanix.com.

Perform the following steps to initiate the power operations:

Procedure

1. Log on to a Controller VM with SSH.
2. Do one of the following:

   » Soft shut down the VM.

   ```
   nutanix@cvm$ acli vm.guest_shutdown vm_name enable_script_exec=[true or false]
    fail_on_script_failure=[true or false]
   ```

   Replace `vm_name` with the name of the VM.

   » Restart the VM.

   ```
   nutanix@cvm$ acli vm.guest_reboot vm_name enable_script_exec=[true or false]
    fail_on_script_failure=[true or false]
   ```

   Replace `vm_name` with the name of the VM.

   Set the value of enable_script_exec to **true** to run your pre-shutdown script and set the value of fail_on_script_failure to **true** to cancel the power operation if the pre-shutdown script fails.

UEFI Support for VM

UEFI firmware is a successor to legacy BIOS firmware that supports larger hard drives, faster boot time, and provides more security features.

VMs with UEFI firmware have the following advantages:

- Boot faster
- Avoid legacy option ROM address constraints
- Include robust reliability and fault management
- Use UEFI drivers

> **Note:**
>
> - Nutanix supports starting of the guest VMs with UEFI firmware in an AHV cluster. However, if a guest VM is added to a protection domain and later restored on a different cluster, the guest VM loses boot configuration. You can restore the lost boot configuration. For more information, see Setting up Boot Device Order using the UEFI Firmware Menu on page 191.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1482

- Nutanix also provides limited support for VMs migrated from a Hyper-V cluster.

You can create or update VMs with UEFI firmware by using `acli` commands, Prism Element web console, or Prism Central.

- For more information on how to create a VM using the Prism Element web console, see Creating a VM (AHV) on page 112.
- For more information on how to create a VM using Prism Central, see Creating a VM through Prism Central (AHV) information in *Prism Central Infrastructure Guide*.
- For information on how to create a VM by using aCLI, see Creating UEFI VMs by Using aCLI on page 188.

Note: If you create a VM using aCLI commands, you can define the location of the storage container for UEFI firmware and variables. Prism Element web console or Prism Central does not provide the option to define the storage container to store UEFI firmware and variables.

For more information on the supported operating systems for the guest VMs, see the *AHV Guest OS* section in the Compatibility and Interoperability Matrix.

Creating UEFI VMs by Using aCLI

In AHV clusters, you can create a virtual machine (VM) to start with UEFI firmware by using Acropolis CLI (aCLI). This topic describes the procedure to create a VM by using aCLI.

Before you begin

Ensure that the VM has an empty vDisk.

About this task

Perform the following procedure to create a UEFI VM by using aCLI:

Procedure

1. Log on to any Controller VM in the cluster with SSH.
2. Create a UEFI VM.

```
nutanix@cvm$ acli vm.create vm-name uefi_boot=true
```

A VM is created with UEFI firmware. Replace `vm-name` with a name of your choice for the VM. By default, the UEFI firmware and variables are stored in an NVRAM container. If you would like to specify a location of the NVRAM storage container to store the UEFI firmware and variables, do so by running the following command.

```
nutanix@cvm$ acli vm.create vm-name uefi_boot=true
 nvram_container=NutanixManagementShare
```

Replace `NutanixManagementShare` with a storage container in which you want to store the UEFI variables.

The UEFI variables are stored in a default NVRAM container. Nutanix recommends you to choose a storage container with at least RF2 storage policy to ensure the VM high availability for node failure scenarios. For more information on RF2 storage policy, see Failure and Recovery Scenarios in the *Prism Element Web Console Guide*.

Note: When you update the location of the storage container, clear the UEFI configuration and update the location of `nvram_container` to a container of your choice.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1483

What to do next

Go to the UEFI BIOS menu and configure the UEFI firmware settings. For more information on accessing and setting the UEFI firmware, see Getting Familiar with UEFI Firmware Menu on page 189.

Getting Familiar with UEFI Firmware Menu

After you launch a VM console from the Prism Element web console, the UEFI firmware menu allows you to do the following tasks for the VM.

- Changing default boot resolution
- Setting up boot device
- Changing boot-time value

Changing Boot Resolution

You can change the default boot resolution of your Windows VM from the UEFI firmware menu.

Before you begin

Ensure that the VM is in powered on state.

About this task

Perform the following procedure to change the default boot resolution of your Windows VM by using the UEFI firmware menu.

Procedure

1. Log on to the Prism Element web console.
2. Launch the console for the VM.
   For more information, see Managing a VM (AHV) section in *Prism Element Web Console Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1484

3. To go to the UEFI firmware menu, press the **F2** keys on your keyboard.

> **Tip:** To enter UEFI menu, open the VM console, select **Reset** in the **Power off/Reset VM** dialog box, and immediately press **F2** when the VM starts to boot.

> **Important:** Resetting the VM results in VM downtime. Nutanix recommends that you reset the VM only during off-production hours or during a maintenance period.

Figure 32: UEFI Firmware Menu

4. Use the up or down arrow key to go to **Device Manager** and press **Enter**.
   The **Device Manager** page appears.

5. In the **Device Manager** screen, use the up or down arrow key to go to **OVMF Platform Configuration** and press **Enter**.

Figure 33: OVMF Settings

The **OVMF Settings** page appears.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1485

6. In the **OVMF Settings** page, use the up or down arrow key to go to the **Change Preferred** field and use the right or left arrow key to increase or decrease the boot resolution.
   The default boot resolution is 1280X1024.
7. Do one of the following.
   - » To save the changed resolution, press the **F10** key.
   - » To go back to the previous screen, press the **Esc** key.
8. Select **Reset** and click **Submit** in the **Power off/Reset** dialog box to restart the VM.
   After you restart the VM, the OS displays the changed resolution.

Setting up Boot Device Order using the UEFI Firmware Menu

This section describes how to set up the boot device for a UEFI VM using the UEFI firmware menu.

About this task

You can set the boot device order for UEFI VMs using both Acropolis Command Line Interface (aCLI) and the UEFI firmware menu. Currently, Nutanix does not support setting up the boot order for UEFI VMs using the Prism Central or Prism Element web console.

For information on how to set up the boot device order using aCLI, see Setting up Boot Device Order Using aCLI on page 193.

When you set or change the boot device order for the UEFI VM, the system behavior varies based on the VM condition. For more information, see System Behavior based on VM condition on page 192.

Before you begin

Ensure that VM is powered on when you use the UEFI firmware menu to set the boot device order.

Procedure

To set up the boot device for a UEFI VM from the UEFI firmware menu, perform the following steps:

1. Launch the console for the VM.
   For more information, see Managing a VM (AHV) section in the *Prism Element Web Console Guide*.
2. To go to the UEFI firmware menu, press the **F2** keys on your keyboard.

   Tip: To enter UEFI menu, open the VM console, select **Reset** in the **Power off/Reset VM** dialog box, and immediately press **F2** when the VM starts to boot.

   Important: Resetting the VM results in VM downtime. We suggest that you reset the VM only during off-production hours or during a maintenance period.
3. Use the up or down arrow key to go to **Boot Manager** and press **Enter**.
   The **Boot Manager** screen displays the list of available boot devices in the cluster based on the VM disks configuration.
4. In the **Boot Manager** screen, use the up or down arrow key to select the boot device and press **Enter**.
   The boot device order is saved. After you select and save the boot device, the VM boots up with the new boot device.
5. To go back to the previous screen, press **Esc**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1486

System Behavior based on VM condition

When you set or change the boot device order for the UEFI VM, the following system behavior applies based on the VM condition:

Table 37: System Behavior based on VM condition

Condition	System Behavior
VM is installed with UEFI and the EFI boot partition exists.	Any change made to the boot device order persists and the changes are saved in the nvVars file in the EFI partition.
No guest OS is installed on the VM but the EFI boot partition exists.	
VM with no EFI boot partition.	Any change made to the boot device order persists only while the VM is on (or rebooted), but a power off/on action reverts the boot order change to the previous setting.

Changing Boot Time-Out Value

The boot time-out value determines how long the boot menu is displayed (in seconds) before the default boot entry is loaded to the VM. This topic describes the procedure to change the default boot-time value of 0 seconds.

About this task

Ensure that the VM is in powered on state.

Procedure

1. Log on to the Prism Element web console.
2. Launch the console for the VM.

   For more details about launching console for the VM, see Managing a VM (AHV) section in *Prism Element Web Console Guide*.
3. To go to the UEFI firmware menu, press the **F2** keys on your keyboard.

> **Tip:** To enter UEFI menu, open the VM console, select **Reset** in the **Power off/Reset VM** dialog box, and immediately press **F2** when the VM starts to boot.

> **Important:** Resetting the VM results in VM downtime. We suggest that you reset the VM only during off-production hours or during a maintenance period.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1487

4. Use the up or down arrow key to go to **Boot Maintenance Manager** and press **Enter**.

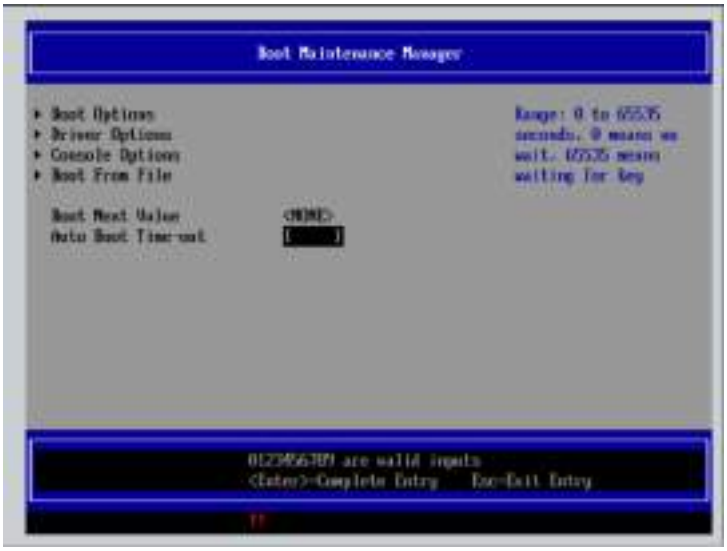


Figure 34: Boot Maintenance Manager

5. In the **Boot Maintenance Manager** screen, use the up or down arrow key to go to the **Auto Boot Time-out** field.
   The default boot-time value is 0 seconds.

6. In the **Auto Boot Time-out** field, enter the boot-time value and press **Enter**.

   > **Note:** The valid boot-time value ranges from 1 second to 9 seconds.

   The boot-time value is changed. The VM starts after the defined boot-time value.

7. To go back to the previous screen, press **Esc**.

Setting up Boot Device Order Using aCLI

This section describes how to set up the boot device order for a UEFI VM using Acropolis Command Line Interface (aCLI).

About this task

You can set the boot device order for UEFI VMs using both aCLI and the UEFI firmware menu. Currently, Nutanix does not support setting up the boot order for UEFI VMs using the Prism Central or Prism Element web console.

For information on how to set up the boot device order using the UEFI firmware menu, see Setting up Boot Device Order using the UEFI Firmware Menu on page 191.

When you set or change the boot device order for the UEFI VM, the system behavior varies based on the VM condition. For more information, see System Behavior based on VM condition on page 192.

Before you begin

Ensure that VM is powered off when you use acli to set the boot device order.

Procedure

To set up the boot device order for a UEFI VM from aCLI, follow these steps:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1488

1. Log on to a Controller VM in the cluster with SSH, and run the following command:

   ```
   nutanix@cvm$ acli vm.update_boot_device vm-name boot_device_order=boot device1,boot
    device2,boot device3
   ```

   Replace:

   - *vm-name* with the target UEFI VM name.
   - *boot device1*, *boot device2*, *boot device3* with the required boot device order. The possible boot options are kCdrom, kDisk, and kNetwork.

   For example:

   ```
   nutanix@cvm$ acli vm.update_boot_device vm-name
    boot_device_order=kNetwork,kDisk,kCdrom
   ```

2. Verify the updated boot device order setting of the UEFI VM:

   ```
   nutanix@cvm$ acli vm.get vm-name
   ```

   Replace *vm-name* with the target UEFI VM name.

   Observe the `boot` section in the command output:

   ```
   boot {
   boot_device_order: "kNetwork"
   boot_device_order: "kDisk"
   boot_device_order: "kCdrom"
   ...
   ```

3. **Power Cycle** the UEFI VM to make the new boot order effective. For more information on how to perform the power cycle operation, see Managing a VM (AHV) on page 117.

Secure Boot Support for VMs

The pre-operating system environment is vulnerable to attacks by possible malicious loaders. Secure boot addresses this vulnerability with UEFI secure boot using policies present in the firmware along with certificates, to ensure that only properly signed and authenticated components are allowed to execute.

Supported Operating Systems

For more information about the supported operating systems for the guest VMs, see the *AHV Guest OS* section in Compatibility and Interoperability Matrix.

Secure Boot Considerations

This section provides the limitations and requirements to use Secure Boot.

Limitations

Secure Boot for guest VMs has the following limitations:

- Nutanix does not support converting a VM that uses IDE disks or legacy BIOS to VMs that use Secure Boot.
- The minimum supported version of the Nutanix VirtIO package for Secure boot-enabled VMs is 1.1.6.
- Secure boot VMs do not permit NICs hot plug.

Requirements

Secure Boot is supported only on the Q35 machine type.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1489

Creating/Updating a VM with Secure Boot Enabled

You can enable Secure Boot with UEFI firmware, either while creating a VM or while updating a VM by using aCLI commands or Prism Element web console.

For information on how to enable Secure Boot from Prism Element web console, see Creating a VM (AHV) on page 112.

Creating a VM with Secure Boot Enabled

About this task

To create a VM with Secure Boot enabled:

Procedure

1. Log on to any Controller VM in the cluster with SSH.
2. To create a VM with Secure Boot enabled:

```
nutanix@cvm$ acli vm.create  <vm_name> secure_boot=true machine_type=q35
```

> **Note:** Specifying the machine type is required to enable the secure boot feature. UEFI is enabled by default when the Secure Boot feature is enabled.

Updating a VM to Enable Secure Boot

About this task

To update a VM to enable Secure Boot:

Procedure

1. Log on to any Controller VM in the cluster with SSH.
2. To update a VM to enable Secure Boot, ensure that the VM is powered off.

```
nutanix@cvm$ acli vm.update <vm_name> secure_boot=true machine_type=q35
```

> **Note:**
>
> - If you disable the secure boot flag alone, the machine type remains q35, unless you disable that flag explicitly.
> - UEFI is enabled by default when the Secure Boot feature is enabled. Disabling Secure Boot does not revert the UEFI flags.

Securing AHV VMs with Virtual Trusted Platform Module (aCLI)

Overview

A Trusted Platform Module (TPM) is used to manage cryptographic keys for security services like encryption and hardware (and software) integrity protection. AHV vTPM is software-based emulation of the TPM 2.0 specification that works as a virtual device.

You can use the AHV vTPM feature to secure virtual machines running on AHV.

> **Note:**

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1490

- You can enable vTPM using aCLI or Prism Central. For more information, see Securing AHV VMs with Virtual Trusted Platform Module in the *Security Guide*.
- AHV vTPM does NOT require OR use a hardware TPM.

vTPM Use Cases

AHV vTPM provides virtualization-based security support for the following primary use cases.

- Microsoft Credential Guard: vTPM is utilized to protect Windows credentials. See *Microsoft documentation* for details on Microsoft Windows Defender Credential Guard.
- Windows 11 Installation: Windows 11 requires TPM 2.0 and Secure Boot to be enabled for optimal security. For more information, see Microsoft website for Windows 11 specs, features, and computer requirements.
- Secure Boot for Windows: vTPM is compatible with Secure Boot, enhancing system security. For information on how to create or update a guest VM with secure boot enabled, see Creating a VM through Prism Central (AHV) and Managing a VM through Prism Central (AHV) sections in *Prism Central Infrastructure Guide*.
- Windows BitLocker: vTPM can support BitLocker with specific caveats, see Limitations for details.

Considerations for Enabling vTPM in AHV VMs (aCLI)

Requirements

Supported Software Versions:

- AHV version 20220304.242 or above
- AOS version 6.5.1 or above

VM Requirements:

- You must enable UEFI on the VM on which you want to enable vTPM. For more information, see UEFI Support for VM on page 187.
- You must enable Secure Boot (applicable if using Microsoft Windows BitLocker). For more information, see Creating a VM with Secure Boot Enabled on page 195.

Limitations

- All Secure Boot limitations apply to vTPM VM.
- Disaster Recovery limitations apply when protecting vTPM-enabled VMs.
- If you take a third-party backup of vTPM-enabled guest VMs, the vTPM data, including crucial encryption keys, is not protected. External systems, such as third-party backup software, do not have access to this data. Therefore, third-party backups of vTPM-enabled guest VMs cannot protect the vTPM device data.

  Note: If the data stored in the vTPM device is critical, such as encryption keys for Windows BitLocker, restoring a VM from a third-party backup might render it unusable and result in unrecoverable data loss. In such cases, if the data in the vTPM device is not critical, such as for Windows Secure Boot, the backup software or user would need to attach a new vTPM device during the restore process.

Creating AHV VMs with vTPM (aCLI)

About this task

You can create a virtual machine with the vTPM configuration enabled using the following aCLI procedure.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1491

Procedure

1. Log on to any Controller VM in the cluster with SSH.
2. At the CVM prompt, type `acli` to enter the Acropolis CLI mode.
3. Create a VM with the required configuration using one of the following methods.

   » Create a VM using Prism Element or Prism Central web console. If you choose to create the VM using Prism Element or Prism Central, proceed to *Step 4*.

   > **Note:** For simplicity, Nutanix recommends you use Prism Element or Prism Central web console to create VMs. For more information, see Creating a VM.

   » Create a VM using aCLI. You can enable vTPM at the time of creating a VM. To enable vTPM during VM creation, do the following and proceed to *step 5* (skip *step 4*).

   Use the "vm.create" command with required arguments to create a VM. For details on VM creation command ("vm.create") and supported arguments using aCLI, see "vm" in the Command Reference Guide.

   ```
   acli> vm.create vm-name machine_type=q35 uefi_boot=true secure_boot=true
    virtual_tpm=true argument(s)
   ```

   Replace *vm-name* with the name of the VM and *argument(s)* with one or more arguments as needed for your VM.

4. Enable vTPM.

   ```
   acli> vm.update vm-name virtual_tpm=true
   ```

   In the above command, replace *vm-name* with name of the newly created VM.

5. Start the VM.

   ```
   acli> vm.on vm-name
   ```

   Replace *vm-name* with the name of the VM.

   vTPM is enabled on the VM.

Enabling vTPM for Existing AHV VMs (aCLI)

About this task

You can update the settings of an existing virtual machine (that satisfies vTPM requirements) to enable vTPM using the following aCLI procedure.

Procedure

1. Log on to any Controller VM in the cluster with SSH.
2. At the CVM prompt, type `acli` to enter the acropolis CLI mode.
3. Shut down the VM to enforce an update on the VM.

   ```
   acli> vm.shutdown vm-name
   ```

   Replace *vm-name* with the name of the VM.

4. Enable vTPM.

   ```
   acli> vm.update <vm-name> virtual_tpm=true
   ```

   Replace <vm-name> with the name of the VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1492

5. Start the VM.

```
acli> vm.on <vm-name>
```

Replace <vm-name> with the name of the VM.

vTPM is enabled on the VM.

Virtual Machine Network Management

Virtual machine network management involves configuring connectivity for guest VMs through virtual switches, VLANs, and VPCs.

For information on how to create or update a virtual switch and other VM network options, see Network & Security Management information in *Prism Central Infrastructure Guide*. Virtual switch creation and updates are also covered in Network Management in *Prism Web Console Guide*.

Virtual Machine Memory and CPU Hot-Plug Configurations

Memory and CPUs are hot-pluggable on guest VMs running on AHV. You can increase the memory allocation and the number of CPUs on your VMs while the VMs are powered on. You can change the number of vCPUs (sockets) while the VMs are powered on. However, you cannot change the number of cores per socket while the VMs are powered on.

> **Note:** You cannot decrease the memory allocation and the number of CPUs on your VMs while the VMs are powered on.

You can change the memory and CPU configuration of your VMs by using the Acropolis CLI (aCLI). For more information, see Managing a VM (AHV) in the *Prism Element Web Console Guide* or see Managing a VM (AHV) and Managing a VM (Self Service) in the *Prism Central Infrastructure Guide*.

For information on operating systems on which you can hot plug memory and CPUs, see the AHV Guest OS Compatibility Matrix .

Memory OS Limitations

1. On Linux operating systems, the Linux kernel might not make the hot-plugged memory online. If the memory is not online, you cannot use the new memory. Perform the following procedure to make the memory online.
   1. Identify the memory block that is offline.

      Display the status of all of the memory.

      ```
      $ cat /sys/devices/system/memory/memoryXXX/state
      ```

      Display the state of a specific memory block.

      ```
      $ grep line /sys/devices/system/memory/*/state
      ```

   2. Make the memory online.

      ```
      $ echo online > /sys/devices/system/memory/memoryXXX/state
      ```

2. If your VM has CentoOS 7.2 as the guest OS and less than 3 GB memory, hot plugging more memory to that VM so that the final memory is greater than 3 GB, results in a memory-overflow condition. To resolve the issue, restart the guest OS (CentOS 7.2) with the following setting:

   ```
   swiotlb=force
   ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1493

CPU OS Limitation

On CentOS operating systems, if the hot-plugged CPUs are not displayed in /proc/cpuinfo, you might have to bring the CPUs online. For each hot-plugged CPU, run the following command to bring the CPU online.

```
$ echo 1 > /sys/devices/system/cpu/cpun/online
```

Replace *n* with the number of the hot plugged CPU.

Hot-Plugging the Memory and CPUs on Virtual Machines (AHV)

About this task

Perform the following procedure to hot plug the memory and CPUs on the AHV VMs.

Procedure

1. Log on the Controller VM with SSH.
2. Update the memory allocation for the VM.

   ```
   nutanix@cvm$ acli vm.update vm-name memory=new_memory_size
   ```

   Replace *vm-name* with the name of the VM and *new_memory_size* with the memory size.
3. Update the number of CPUs on the VM.

   ```
   nutanix@cvm$ acli vm.update vm-name num_vcpus=n
   ```

   Replace *vm-name* with the name of the VM and *n* with the number of CPUs.

Disable CPU Hot-Plug on VMs

By default, AHV enables CPU hot-plug when you create a VM on its host. This default behavior creates several empty sockets for plugging in future virtual CPUs.

Windows server automatically creates processor groups to accommodate more than 64 processors. However, when a large number of empty sockets are present, Windows Server intentionally creates processor groups to support complete socket utilization. This approach might impact performance for VMs without plugged-in CPUs. For VMs that do not need CPU hot-plugging, you can disable it from aCLI.

You can disable the CPU hot-plug during the following VM operations:

- Creating a VM
- Updating an existing VM

Important Considerations

Consider the following when you disable CPU hot-plug:

- You cannot hot-plug CPU regardless of the VM guest OS type.
- You cannot re-enable CPU hot-plug functionality when the VM is powered on.
- After a planned or unplanned failover (DR), the CPU hotplug property of VMs is enabled by default on the recovery cluster if it was disabled on the primary cluster. This can prevent VMs from booting if the applications running on them do not support this setting.

  To ensure a smooth recovery process for VMs that require CPU hotplug to remain disabled, upgrade all Prism Central and Prism Element (cluster) instances to the latest version. If Prism Central is fully updated but the recovery cluster does not support disabling CPU hotplug, the system will generate a recovery plan job alert. However, if Prism Central is running an unsupported version, this alert will not be generated.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1494

Disabling CPU Hot-Plug During VM Creation

AHV enables CPU hot-plug by default on every VM. However, if your workload requires it, you can disable the CPU hot-plug during VM creation.

About this task

To disable CPU hot-plug when you are creating VMs on an AHV cluster, follow these steps:

Procedure

1. Log on to any Controller VM in the cluster with SSH.

   ```
   $ ssh nutanix@cvm_ip_address
   ```

   Replace `cvm_ip_address` with the IP address of your CVM.

2. Disable CPU hot-plug when you are creating a VM with the required configuration:

   ```
   nutanix@cvm$ acli vm.create <vm_name> num_vcpus=x \
   num_cores_per_vcpu=x memory=xG \
   num_vnuma_nodes=x cpu_hotplug_enabled=false
   ```

   Replace `vm-name` with the name of the VM and `argument` with one or more arguments as needed for your VM. For more information on VM creation command and supported arguments using aCLI, see *vm* in the Command Reference Guide.

3. Verify that CPU hot-plug is disabled for the VM:

   ```
   nutanix@cvm$ acli vm.get vm-name | grep "cpu_hotplug"
   ```

   Replace `vm-name` with the name of the VM.

   Example output:

   ```
   cpu_hotplug_enabled: False
   ```

4. Power on the VM:

   ```
   nutanix@cvm$ acli vm.on vm-name
   ```

   Replace `vm-name` with the name of the VM.

Disabling CPU Hot-Plug in an Existing VM

AHV enables CPU hot-plug by default on every VM. However, if your workload requires it, you can disable CPU hot-plug on an existing VM.

Before you begin

You must power off the VM before disabling the CPU hot-plug. Perform a graceful shutdown from the operating system of the VM.

About this task

To disable CPU hot-plug on your VMs running on an AHV cluster, follow these steps:

Procedure

1. Log on to any Controller VM in the cluster with SSH.

   ```
   $ ssh nutanix@cvm_ip_address
   ```

   Replace `cvm_ip_address` with the IP address of your CVM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1495

2. Disable CPU hot-plug:

   ```
   nutanix@cvm$ acli vm.update vm-name cpu_hotplug_enabled=false
   ```

   Replace *vm-name* with the name of the VM.

3. Verify that CPU hot-plug is disabled for the VM:

   ```
   nutanix@cvm$ acli vm.get vm-name | grep "cpu_hotplug"
   ```

   Replace *vm-name* with the name of the VM.

   Example output:

   ```
   cpu_hotplug_enabled: False
   ```

4. Power on the VM:

   ```
   nutanix@cvm$ acli vm.on vm-name
   ```

   Replace *vm-name* with the name of the VM.

Disable the SCSI Controller on VMs

By default, AHV adds SCSI controllers when you create a VM. For applications that do not require SCSI controller, you can disable it from aCLI.

You can disable the SCSI controller during the following VM operations:

- Creating a VM
- Updating an existing VM

Important Considerations

Consider the following when you disable the SCSI controller:

- You cannot add SCSI disks to the VM.
- You cannot re-enable the SCSI controller functionality when the VM is powered-on.
- After a planned or unplanned failover, the Virtual SCSI property of VMs is enabled by default on the recovery cluster if it was disabled on the primary cluster. This can prevent VMs from booting if the applications running on them do not support this setting.

  To ensure a smooth recovery process for VMs that require Virtual SCSI to remain disabled, upgrade all Prism Central and Prism Element (cluster) instances to the latest version. If Prism Central is fully updated but the recovery cluster does not support disabling Virtual SCSI, the system will generate a recovery plan job alert. However, if Prism Central is running an unsupported version, this alert will not be generated.

Disabling SCSI Controller During VM Creation

AHV adds the SCSI controller by default on every VM. However, if your workload requires it, you can disable the SCSI controller during VM creation.

About this task

To disable the SCSI controller when you are creating VMs on an AHV cluster, follow these steps:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1496

Procedure

1. Log on to any Controller VM in the cluster with SSH.

   ```
   $ ssh nutanix@cvm_ip_address
   ```

   Replace *cvm_ip_address* with the IP address of your CVM.

2. Disable the SCSI controller when you are creating a VM with the required configuration:

   ```
   nutanix@cvm$ acli vm.create <vm_name> num_vcpus=x \
   num_cores_per_vcpu=x memory=xG \
   num_vnuma_nodes=x scsi_controller_enabled=false
   ```

   Replace *vm-name* with the name of the VM and *argument* with one or more arguments as needed for your VM. For more information on VM creation command and supported arguments using aCLI, see *vm* in the Command Reference Guide.

3. Verify that the SCSI controller is disabled for the VM:

   ```
   nutanix@cvm$ acli vm.get vm-name | grep "scsi_controller_enabled"
   ```

   Replace *vm-name* with the name of the VM.

   Example output:

   ```
   scsi_controller_enabled: False
   ```

4. Power on the VM:

   ```
   nutanix@cvm$ acli vm.on vm-name
   ```

   Replace *vm-name* with the name of the VM.

Disabling SCSI Controller in an Existing VM

AHV enables the SCSI controller by default on every VM. However, if your workload requires it, you can disable the SCSI controller on an existing VM.

Before you begin

You must power off the VM before disabling the SCSI controller. Perform a graceful shutdown from the operating system of the VM.

About this task

To disable SCSI controller on your VMs running on an AHV cluster, follow these steps:

Procedure

1. Log on to any Controller VM in the cluster with SSH.

   ```
   $ ssh nutanix@cvm_ip_address
   ```

   Replace *cvm_ip_address* with the IP address of your CVM.

2. Disable the SCSI controller:

   ```
   nutanix@cvm$ acli vm.update vm-name scsi_controller_enabled=false
   ```

   Replace *vm-name* with the name of the VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1497

3. Verify that the SCSI controller is disabled for the VM:

   ```
   nutanix@cvm$ acli vm.get vm-name | grep "scsi_controller_enabled"
   ```

   Replace *vm-name* with the name of the VM.

   Example output:

   ```
   scsi_controller_enabled: False
   ```

4. Power on the VM:

   ```
   nutanix@cvm$ acli vm.on vm-name
   ```

   Replace *vm-name* with the name of the VM.

Virtual Machine Memory Management (vNUMA)

AHV hosts support Virtual Non-uniform Memory Access (vNUMA) on virtual machines. You can enable vNUMA on VMs when you create or modify the VMs to optimize memory performance.

Non-uniform Memory Access (NUMA)

In a NUMA topology, the memory access times of a VM depend on the memory location relative to a processor. A VM accesses memory local to a processor faster than the non-local memory. If the VM uses both CPU and memory from the same physical NUMA node, you can achieve optimal resource utilization. If you are running the CPU on one NUMA node (for example, node 0) and the VM accesses the memory from another node (node 1) then memory latency occurs. Ensure that the virtual topology of VMs matches the physical hardware topology to achieve minimum memory latency.

Virtual Non-uniform Memory Access (vNUMA)

vNUMA optimizes the memory performance of virtual machines that require more vCPUs or memory than the capacity of a single physical NUMA node. In a vNUMA topology, you can create multiple vNUMA nodes where each vNUMA node includes vCPUs and virtual RAM. When you assign a vNUMA node to a physical NUMA node, the vCPUs can intelligently determine the memory latency (high or low). Low memory latency within a vNUMA node results in low latency in the physical NUMA node as well.

Enabling and Disabling vNUMA on Virtual Machines

Before you begin

Before you enable vNUMA, see AHV Best Practices Guide under *Solutions Documentation*.

About this task

Perform the following procedure to enable vNUMA on your VMs running on the AHV hosts.

Procedure

1. Log on to a Controller VM with SSH.
2. Check how many NUMA nodes are available on each AHV host in the cluster.

   ```
   nutanix@cvm$ hostssh "numactl --hardware"
   ```

   The console displays an output similar to the following:

   ```
   ============= 10.x.x.x ============
   available: 2 nodes (0-1)
   node 0 cpus: 0 1 2 3 4 5 6 7 16 17 18 19 20 21 22 23
   node 0 size: 128837 MB
   node 0 free: 862 MB
   ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1498

```
node 1 cpus: 8 9 10 11 12 13 14 15 24 25 26 27 28 29 30 31
node 1 size: 129021 MB
node 1 free: 352 MB
node distances:
node   0   1
  0:  10  21
  1:  21  10
============= 10.x.x.x ============
available: 2 nodes (0-1)
node 0 cpus: 0 1 2 3 4 5 12 13 14 15 16 17
node 0 size: 128859 MB
node 0 free: 1076 MB
node 1 cpus: 6 7 8 9 10 11 18 19 20 21 22 23
node 1 size: 129000 MB
node 1 free: 436 MB
node distances:
node   0   1
  0:  10  21
  1:  21  10
============= 10.x.x.x ============
available: 2 nodes (0-1)
node 0 cpus: 0 1 2 3 4 5 12 13 14 15 16 17
node 0 size: 128859 MB
node 0 free: 701 MB
node 1 cpus: 6 7 8 9 10 11 18 19 20 21 22 23
node 1 size: 129000 MB
node 1 free: 357 MB
node distances:
node   0   1
  0:  10  21
  1:  21  10
============= 10.x.x.x ============
available: 2 nodes (0-1)
node 0 cpus: 0 1 2 3 4 5 12 13 14 15 16 17
node 0 size: 128838 MB
node 0 free: 1274 MB
node 1 cpus: 6 7 8 9 10 11 18 19 20 21 22 23
node 1 size: 129021 MB
node 1 free: 424 MB
node distances:
node   0   1
  0:  10  21
  1:  21  10
============= 10.x.x.x ============
available: 2 nodes (0-1)
node 0 cpus: 0 1 2 3 4 5 12 13 14 15 16 17
node 0 size: 128837 MB
node 0 free: 577 MB
node 1 cpus: 6 7 8 9 10 11 18 19 20 21 22 23
node 1 size: 129021 MB
node 1 free: 612 MB
node distances:
node   0   1
  0:  10  21
  1:  21  10
```

The example output shows that each AHV host has two NUMA nodes.

3. Do one of the following:

   » Enable vNUMA if you are creating a VM.

   ```
   nutanix@cvm$ acli vm.create <vm_name> num_vcpus=x \
   ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1499

```
num_cores_per_vcpu=x memory=xG \
num_vnuma_nodes=x
```

» Enable vNUMA if you are modifying an existing VM.

```
nutanix@cvm$ acli vm.update vm_name \
num_vnuma_nodes=x
```

» Disable vNUMA if you are modifying an existing VM.

```
nutanix@cvm$ acli vm.update vm_name num_vnuma_nodes=0
```

Replace *vm_name* with the name of the VM on which you want to enable vNUMA or vUMA. Replace *x* with the values for the following indicated parameters:

- num_vcpus: Type the number of vCPUs for the VM.
- num_cores_per_vcpu: Type the number of cores per vCPU.
- memory: Type the memory in GB for the VM.
- num_vnuma_nodes: Type the number of vNUMA nodes for the VM.

For example:

```
nutanix@cvm$ acli vm.create test_vm num_vcpus=20 memory=150G num_vnuma_nodes=2
```

This command creates a VM with 2 vNUMA nodes, 10 vCPUs and 75 GB memory for each vNUMA node.

GPU and vGPU Support

AHV supports GPU-accelerated computing for guest VMs. You can configure either GPU pass-through or a virtual GPU.

> **Note:** You can configure either pass-through or a vGPU for a guest VM but not both.

This guide describes the concepts related to the GPU and vGPU support in AHV. For the configuration procedures, see the Prism Element Web Console Guide.

For driver installation instructions, see the NVIDIA Grid Host Driver for Nutanix AHV Installation Guide.

> **Note:** VMs with GPU passthrough are not migrated to other hosts in the cluster. For more information, see Non-Migratable VMs on page 171.

Supported GPUs

For information on supported GPUs based on AOS release and AHV version, see NVIDIA Drivers on the *Compatibility and Interoperability Matrix* page.

GPU Pass-Through for Guest VMs

AHV hosts support GPU pass-through for guest VMs, allowing applications on VMs direct access to GPU resources. The Nutanix user interfaces provide a cluster-wide view of GPUs, allowing you to allocate any available GPU to a VM. You can also allocate multiple GPUs to a VM. However, in a pass-through configuration, only one VM can use a GPU at any given time.

> **Note:** AHV supports up to four pass-through GPUs to a single VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1500

Host Selection Criteria for VMs with GPU Pass-Through

When you power on a VM with GPU pass-through, the VM is started on the host that has the specified GPU, provided that the Acropolis Dynamic Scheduler determines that the host has sufficient resources to run the VM. If the specified GPU is available on more than one host, the Acropolis Dynamic Scheduler ensures that a host with sufficient resources is selected. If sufficient resources are not available on any host with the specified GPU, the VM is not powered on.

If you allocate multiple GPUs to a VM, the VM is started on a host if, in addition to satisfying Acropolis Dynamic Scheduler requirements, the host has all of the GPUs that are specified for the VM.

If you want a VM to always use a GPU on a specific host, configure host affinity for the VM.

Support for Graphics and Compute Modes

AHV supports running GPU cards in either graphics mode or compute mode. If a GPU is running in compute mode, Nutanix user interfaces indicate the mode by appending the string `compute` to the model name. No string is appended if a GPU is running in the default graphics mode.

Switching Between Graphics and Compute Modes

If you want to change the mode of the firmware on a GPU, put the host in maintenance mode, and then flash the GPU manually by logging on to the AHV host and performing standard procedures as documented for Linux VMs by the vendor of the GPU card.

Typically, you restart the host immediately after you flash the GPU. After restarting the host, redo the GPU configuration on the affected VM, and then start the VM. For example, consider that you want to re-flash an NVIDIA Tesla® M60 GPU that is running in graphics mode. The Prism web console identifies the card as an `NVIDIA Tesla M60` GPU. After you re-flash the GPU to run in compute mode and restart the host, redo the GPU configuration on the affected VMs by adding back the GPU, which is now identified as an `NVIDIA Tesla M60.compute` GPU, and then start the VM.

Supported GPU Cards

For information on the list of supported GPUs, see Supported GPUs on page 205.

Limitations

GPU pass-through support has the following limitations:

- Live migration of VMs with a GPU configuration is not supported. Live migration of VMs is necessary when the BIOS, BMC, and the hypervisor on the host are being upgraded. During these upgrades, VMs that have a GPU configuration are powered off and then powered on automatically when the node is back up.
- VM pause and resume are not supported.
- Hot add and hot remove support is not available for GPUs.
- You can change the GPU configuration of a VM only when the VM is turned off.
- When you have configured a VM with the vGPU driver, you cannot access the VM with the Prism web console. Before you configure GPU pass-through for a VM, set up an alternative means to access the VM. For example, enable remote access over RDP.

  Removing GPU pass-through from a VM restores console access to the VM through the Prism web console.

Configuring GPU Pass-Through

For information on configuring GPU pass-through for guest VMs, see Creating a VM (AHV).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1501

NVIDIA GRID Virtual GPU Support on AHV

AHV supports NVIDIA GRID technology, which enables multiple guest VMs to use the same physical GPU concurrently. Concurrent use is made possible by dividing a physical GPU into discrete virtual GPUs (vGPUs) and allocating those vGPUs to guest VMs. Each vGPU is allocated a fixed range of the physical GPUs framebuffer and uses all the GPU processing cores in a time-sliced manner.

Virtual GPUs (vGPUs) are of different types (vGPU types are also called vGPU profiles) and differ by the amount of physical GPU resources allocated to them and the class of workload that they target. The number of vGPUs into which a single physical GPU can be divided therefore depends on the vGPU profile that is used on a physical GPU.

Each physical GPU supports more than one vGPU profile, but a physical GPU cannot run multiple vGPU profiles concurrently. After a vGPU of a given profile is created on a physical GPU (that is, after a vGPU is allocated to a VM that is powered on), the GPU is restricted to that vGPU profile until it is freed up completely. To understand this behavior, consider that you configure a VM to use an M60-1Q vGPU. When the VM is powering on, it is allocated an M60-1Q vGPU instance only if a physical GPU that supports M60-1Q is either unused or already running the M60-1Q profile and can accommodate the requested vGPU.

If an entire physical GPU that supports M60-1Q is free at the time the VM is powering on, an M60-1Q vGPU instance is created for the VM on the GPU, and that profile is locked on the GPU. In other words, until the physical GPU is completely freed up again, only M60-1Q vGPU instances can be created on that physical GPU (that is, only VMs configured with M60-1Q vGPUs can use that physical GPU).

> **Note:** NVIDIA does not support Windows Guest VMs on the C-series NVIDIA vGPU types. For more information, see the NVIDIA documentation on Virtual GPU software.

NVIDIA Grid Host Drivers and License Installation

To enable guest VMs to use vGPUs on AHV, you must install NVIDIA drivers on the guest VMs, install the NVIDIA GRID host driver on the hypervisor, and set up an NVIDIA GRID License Server.

For information on how to enable guest VMs to use vGPUs on AHV and the NVIDIA GRID host driver installation instructions, see the NVIDIA Grid Host Driver for Nutanix AHV Installation Guide.

vGPU Profile Licensing

vGPU profiles are licensed through an NVIDIA GRID license server. The choice of license depends on the type of vGPU that the applications running on the VM require. Licenses are available in various editions, and the vGPU profile that you want might be supported by more than one license edition.

> **Note:** If the specified license is not available on the licensing server, the VM starts up and functions normally, but the vGPU runs with reduced capability.

You must determine the vGPU profile that the VM requires, install an appropriate license on the licensing server, and configure the VM to use that license and vGPU type. For information about licensing for different vGPU types, see the NVIDIA GRID licensing documentation.

Guest VMs check out a license over the network when starting up and return the license when shutting down. As the VM is powering on, it checks out the license from the licensing server. When a license is checked back in, the vGPU is returned to the vGPU resource pool.

When powered on, guest VMs use a vGPU in the same way that they use a physical GPU that is passed through.

Supported GPU Cards

For information on the list of supported GPUs, see Supported GPUs on page 205.

High Availability Support for VMs with vGPUs

Nutanix conditionally supports high availability (HA) of VMs that have NVIDIA GRID vGPUs configured. The cluster does not reserve any specific resources to guarantee High Availability for the VMs with vGPUs. The vGPU

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1502

VMs are restarted on commercially reasonable effort in the event of a node failure. You can restart a VM with vGPUs on another (failover) host which has compatible or identical vGPU resources available. The vGPU profile available on the failover host must be identical to the vGPU profile configured on the VM that needs HA. The system attempts to restart the VM after an event. If the failover host has insufficient memory and vGPU resources for the VM to start, the VM fails to start after failover.

The following conditions are applicable to HA of VMs with vGPUs:

- Memory is not reserved for the VM on the failover host by the HA process. When the VM fails over, if sufficient memory is not available, the VM cannot power on.
- vGPU resource is not reserved on the failover host. When the VM fails over, if the required vGPU resources are not available on the failover host, the VM cannot power on.

Limitations for vGPU Support

vGPU support on AHV has the following limitations:

- When you have configured a VM with the vGPU driver, you cannot access the VM with the Prism web console. Before you add multiple vGPUs to a VM, set up an alternative means to access the VM. For example, enable remote access over RDP. For Linux VMs, instead of RDP, use Virtual Network Computing (VNC) or equivalent.
- The vGPU on AHV supports only the guest operating systems that are supported by NVIDIA.

Console Support for VMs with vGPU

Like other VMs, you can access a VMs with a single vGPU using the console. Enable or disable console support for a VM with only one vGPU configured. Enabling console support for a VM with multiple vGPUs is not supported. By default, console support for a vGPU VM is disabled.

Recovery of vGPU Console-enabled VMs

With AHV, you can recover vGPU console-enabled guest VMs efficiently. When you perform DR of vGPU console-enabled guest VMs, the VMs recovers with the vGPU console. The guest VMs fail to recover when you perform cross-hypervisor disaster recovery (CHDR).

For AHV with minimum AOS versions 6.1, 6.0.2.4 and 5.20:

- vGPU-enabled VMs can be recovered when protected by protection domains in PD-based DR or protection policies in Nutanix Disaster Recovery based solutions using asynchronous, NearSync, or Synchronous (Nutanix Disaster Recovery only) replications.

  > **Note:** GPU Passthrough is not supported.

- If both site A and site B have the same GPU boards (and the same assignable vGPU profiles), failovers work seamlessly. With Nutanix Disaster Recovery, vGPU console settings do not persist after recovery. However, with protection domains, no additional steps are required. GPU profiles are restored correctly and vGPU console settings persist after recovery.
- If site A and site B have different GPU boards and vGPU profiles, you must manually remove the vGPU profile before you power on the VM in site B.

The vGPU console settings are persistent after recovery and all failovers are supported for the following:

Table 38: Persistent vGPU Console Settings with Failover Support

Recovery using	For vGPU enabled AHV VMs
Protection Domain based Disaster Recover	Yes

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1503

Recovery using	For vGPU enabled AHV VMs
VMware SRM with Nutanix SRA	Not applicable

Cross Cluster Live Migration of VMs enabled with GPU passthrough is not supported.

Cross Cluster Live Migration of VMs enabled with vGPU console is supported.

For more information, see Recovery of vGPU-enabled VMs in the *Data Protection and Recovery with Prism Element* guide.

For information on configuring the console support for vGPU VMs, see Enabling or Disabling Console Support for vGPU VMs on page 215.

For information on SRA and SRM support, see the Nutanix SRA documentation.

ADS support for VMs with vGPUs

AHV supports Acropolis Dynamic Scheduling (ADS) for VMs with vGPUs.

> **Note:** ADS support requires live migration of VMs with vGPU (vGPU-enabled VMs) be operational in the cluster. For information on the minimum NVIDIA and AOS versions that support live migration of vGPU-enabled VMs, see Live Migration of vGPU-enabled VMs on page 213.

ADS triggers migrations that involve vGPU-enabled VMs if there are resource hotspots or if there is a need to defragment the cluster to power on the incoming vGPU-enabled VMs. ADS can migrate vGPU-enabled VMs to other hosts in the cluster only if:

- The other hosts support compatible or identical vGPU resources as the source host (hosting the vGPU-enabled VMs).
- The host affinity is not set for the vGPU-enabled VM.

For information on live migration limitations, see Live Migration of vGPU-enabled VMs on page 213 and Limitations for Live Migration of vGPU-enabled VMs on page 214.

For more information on ADS, see Acropolis Dynamic Scheduling in AHV on page 8.

Multiple Virtual GPU Support

Prism Central and Prism Element Web Console can deploy VMs with multiple virtual GPU instances. This support harnesses the capabilities of NVIDIA GRID virtual GPU (vGPU) support for multiple vGPU instances for a single VM.

> **Note:** Multiple vGPUs on the same VM are supported on NVIDIA Virtual GPU (vGPU) software version 10.1 (440.53) or later.

You can deploy virtual GPUs (vGPUs) of different types. A single physical GPU can be divided into the number of vGPUs depending on the type of vGPU profile that is used on the physical GPU. Each physical GPU on a GPU board supports more than one type of vGPU profile. For example, a Tesla® M60 GPU device provides different types of vGPU profiles like M60-0Q, M60-1Q, M60-2Q, M60-4Q, and M60-8Q.

You can only add multiple vGPUs of the same type of vGPU profile to a single VM. For example, consider that you configure a VM on a Node that has one NVIDIA Tesla® M60 GPU board. Tesla® M60 provides two physical GPUs, each supporting one M60-8Q (profile) vGPU, thus supporting a total of two M60-8Q vGPUs for the entire host.

For information on restrictions while configuring multiple vGPUs on the same VM, see Restrictions for Multiple vGPU Support on page 210.

For information on steps to add multiple vGPUs to the same VM, see Creating a VM (AHV) and Adding Multiple vGPUs to a VM in *Prism Element Web Console Guide* or Creating a VM through Prism Central (AHV) and Adding Multiple vGPUs to a VM in *Prism Central Infrastructure Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1504

Restrictions for Multiple vGPU Support

You can configure multiple vGPUs subject to the following restrictions:

- All the vGPUs that you assign to one VM must be of the same type. In the aforesaid example, with the Tesla® M60 GPU device, you can assign multiple M60-8Q vGPU profiles. You cannot assign one vGPU of the M60-1Q type and another vGPU of the M60-8Q type.

  > **Note:** You can configure any number of vGPUs of the same type on a VM. However, the cluster calculates a maximum number of vGPUs of the same type per VM. This number is defined as max_instances_per_vm. This number is variable and changes based on the GPU resources available in the cluster and the number of VMs deployed. If the number of vGPUs of a specific type that you configured on a VM exceeds the max_instances_per_vm number, then the VM fails to power on and the following error message is displayed:

```
Operation failed: NoHostResources: No host has enough available GPU for VM <name of
 VM>(UUID of VM).
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1505

```
You could try reducing the GPU allotment...
```

When you configure multiple vGPUs on a VM, after you select the appropriate vGPU type for the first vGPU assignment, Prism (Prism Central and Prism Element Web Console) automatically restricts the selection of vGPU type for subsequent vGPU assignments to the same VM.

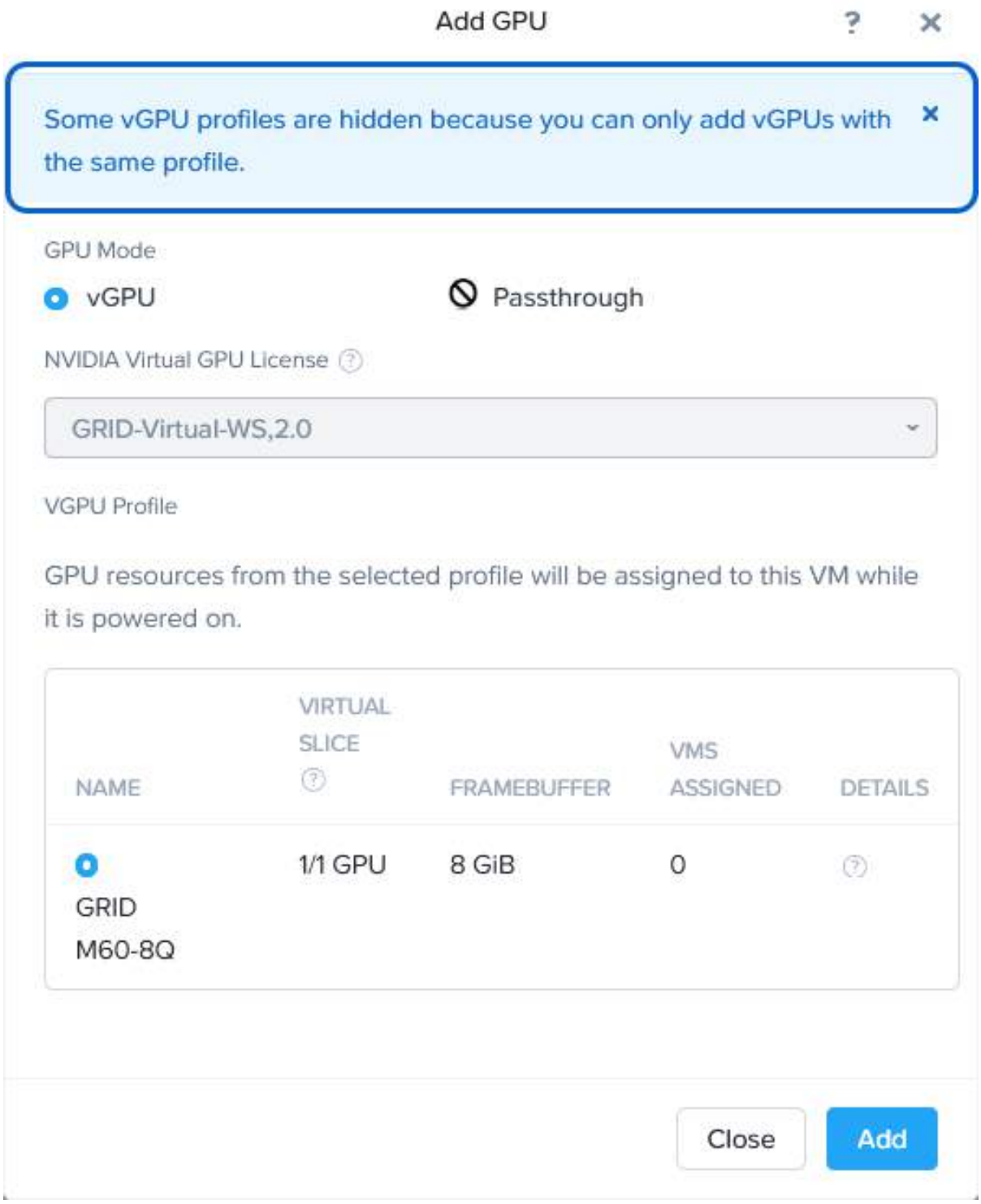


Figure 35: vGPU Type Restriction Message

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1506

Note:

You can use CLI (acli) to configure multiple vGPUs of multiple types to the same VM. For more information, see *Acropolis Command-Line Interface (aCLI)*. Use the vm.gpu_assign <vm.name> gpu=<gpu-type> command multiple times, once for each vGPU, to add multiple vGPUs of multiple types to the same VM.

For information on the combinations of the number and types of vGPUs profiles supported by the GPU resources installed in the cluster, see the GPU board and software documentation . For example, see the NVIDIA Virtual GPU Software Documentation for the vGPU type and number combinations on the Tesla® M60 board.

- Configure multiple vGPUs only of the highest type using Prism. The highest type of vGPU profile is based on the driver deployed in the cluster. In the aforesaid example, on a Tesla® M60 device, you can only configure multiple vGPUs of the M60-8Q type. Prism prevents you from configuring multiple vGPUs of any other type such as M60-2Q.

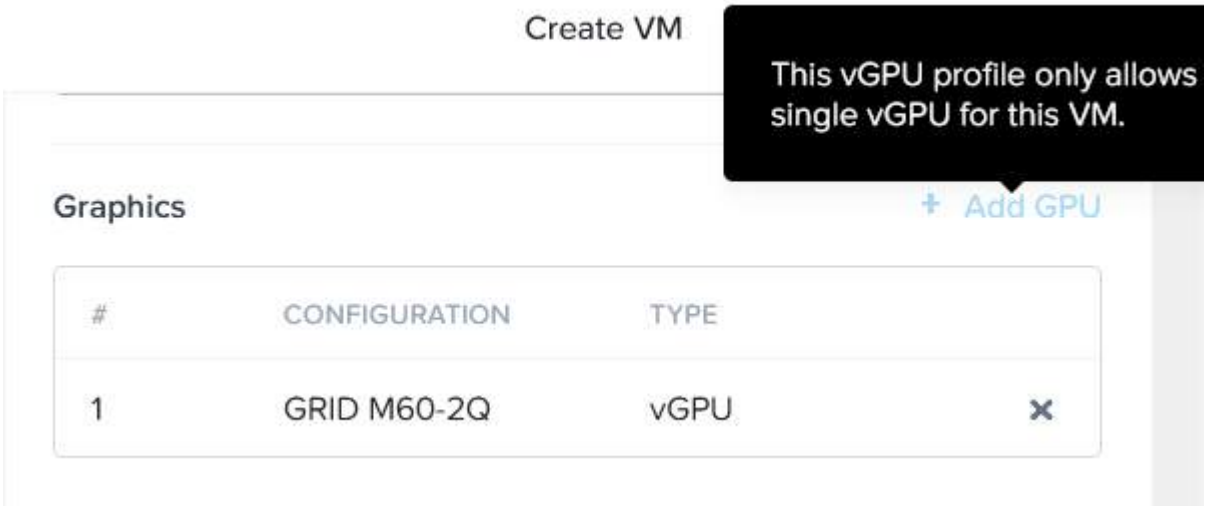


Figure 36: vGPU Type Restriction Message

Note:

You can use CLI (acli) to configure multiple vGPUs of other available types. See *Acropolis Command-Line Interface (aCLI)* for the aCLI information. Use the vm.gpu_assign <vm.name> gpu=<gpu-type> command multiple times, once for each vGPU, to configure multiple vGPUs of other available types.

For more information, see the GPU board and software documentation.

- Configure either a passthrough GPU or vGPUs on the same VM. You cannot configure both passthrough GPU and vGPUs. Prism automatically disallows such configurations after the first GPU is configured.
- The VM powers on only if the requested type and number of vGPUs are available in the host.

  In the aforesaid example, the VM, which is configured with two M60-8Q vGPUs, fails to power on if another VM sharing the same GPU board is already using one M60-8Q vGPU. This is because the Tesla® M60 GPU board allows only two M60-8Q vGPUs. Of these, one is already used by another VM. Thus, the VM configured with two M60-8Q vGPUs fails to power on due to unavailability of required vGPUs.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1507

- Multiple vGPUs on the same VM are supported on NVIDIA Virtual GPU (vGPU) software version 10.1 (440.53) or later. Ensure that the relevant GRID version license is installed and select it when you configure multiple vGPUs.

Adding Multiple vGPUs to the Same VM

About this task

You can add multiple vGPUs of the same vGPU type when you create a new VM or update an existing VM.

- For information on how to create a VM, see Creating a VM through Prism Central (AHV).
- For information on how to update an existing VM, see Updating a VM through Prism Central (AHV).

For more information on multiple vGPU support, see Multiple Virtual GPU Support.

Before you begin

Ensure that the following prerequisites are met before you add multiple vGPUs to the VM:

- Select the license for NVIDIA Virtual GPU (vGPU) software version 10.1 (440.53) or later.
- Observe the guidelines and restrictions specified in Multiple Virtual GPU Support and Restrictions for Multiple vGPU Support.

Procedure

To add multiple vGPUs to the same VM, perform the following steps:

1. Click **Add GPU** in the **Resources** step of create VM workflow or update VM workflow. For more information, see Creating a VM through Prism Central (AHV) or Updating a VM through Prism Central (AHV)
2. In the **Add GPU** window, click **Add**.

   The License field is grayed out and you cannot select a different license when you add a vGPU for the same VM.

   The **VGPU Profile** is auto-selected. The system allows you to select additional vGPU of the same vGPU type as indicated by the message at the top of the **Add GPU** window.

   The newly added vGPU appears in the **Create VM** or **Update VM** window.
3. Repeat the steps for each vGPU addition to the VM.

Live Migration of vGPU-enabled VMs

You can perform the live migration of VMs enabled with virtual GPUs (vGPU-enabled VMs) only on commercially reasonable effort, if the destination node is equipped to provide enough resources to the vGPU-enabled VMs. However, if the destination node is not equipped with the enough resources, the vGPU-enabled VMs are shut down and the VMs might experience downtime.

In a successful migration case, the vGPUs can continue to run while the VMs that are running the vGPUs are seamlessly migrated in the background.

During LCM update, LCM looks at the vGPU resources of the cluster, treats the vGPU-enabled VMs as non-HA protected VMs, and attempts to migrate the non-HA-protected VMs on commercially reasonable effort. LCM shuts down the vGPU-enabled VMs if the destination node is not equipped with the enough resources or there is any compatibility issue between the VM GPU drivers and AHV host GPU drivers.

For more information on live migration limitations for vGPU-enabled VMs, see Limitations for Live Migration of vGPU-enabled VMs.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1508

Table 39: Minimum Versions

Component	Supports	With Minimum Version
AOS	Live migration within the same cluster	5.18.1
AHV	Live migration within the same cluster	20190916.294
AOS	Live migration across cluster	6.1
AHV	Live migration across cluster	20201105.30142

> **Important:** In an HA event involving any GPU node, the node locality of the affected vGPU-enabled VMs is not restored after GPU node recovery. The affected vGPU-enabled VMs are not migrated back to their original GPU host intentionally to avoid extended VM stun time expected during migration. If vGPU-enabled VM node locality is required, migrate the affected vGPU-enabled VMs to the desired host manually.

Virtual GPU Limitations

Important frame buffer and VM stun time considerations are:

- The GPU board (for example, NVIDIA Tesla M60) vendor provides the information for maximum frame buffer size of vGPU types (for example, M60-8Q type) that can be configured on VMs. However, the actual frame buffer usage may be lower than the maximum sizes.
- The VM stun time depends on the number of vGPUs configured on the VM being migrated. Stun time may be longer in case of multiple vGPUs operating on the VM.

  The stun time also depends on the network factors such bandwidth available for use during the migration.

Live Migration Workflows

You can live migrate a vGPU-enabled VM to the following destinations:

- To another host within the same cluster. Both Prism Web Console (Prism Element) and Prism Central allow you to live migrate a vGPU-enabled VM to another host within the same cluster.
- To a host outside the cluster, that is, a host in another cluster. Only Prism Central allows you to migrate a vGPU-enabled VM to a host outside the cluster.)

For information on the steps to live migrate a vGPU-enabled VM, see the following:

- Migrating Live a vGPU-enabled VM Within the Cluster in the *Prism Web Console Guide*.
- Migrating Within the Cluster in the *Prism Central Infrastructure Guide*.

Limitations for Live Migration of vGPU-enabled VMs

The following limitations apply to live migration of virtual GPU (vGPU) enabled VMs:

- Live migration is supported only for VMs configured with single or multiple virtual GPUs. It is not supported for VMs configured with passthrough GPUs.
- Live migration to a host in another cluster is supported only if the VM is protected by protection policy with Synchronous replication schedule.
- The target host for the live migration must have adequate and available GPU resources, with the same vGPU types as configured for the VMs to be migrated, to support the vGPUs on the VMs that need to be migrated.

  For more information, see Restrictions for Multiple vGPU Support on page 210.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1509

- Live migration is not supported for the vGPU-enabled VMs that are in powered off state.
- The source and target hosts must have the same GPU software license type.

  Ensure that you have the appropriate GPU software license (an appropriate license of NVIDIA GRID software version) that supports live migration of vGPUs.
- For a cluster that has AOS 7.0 or later version, the live migration of VMs with vGPUs is only supported with AHV 10.0 or later version

Enabling or Disabling Console Support for vGPU VMs

About this task

Enable or disable console support for a VM with only one vGPU configured. Enabling console support for a VM with multiple vGPUs is not supported. By default, console support for a vGPU VM is disabled.

To enable or disable console support for each VM with vGPUs, do the following:

Procedure

1. Run the following aCLI command to check if console support is enabled or disabled for the VM with vGPUs.

   ```
   acli> vm.get vm-name
   ```

   Where `vm-name` is the name of the VM for which you want to check the console support status.

   The step result includes the following parameter for the specified VM:

   ```
   gpu_console=False
   ```

   Where False indicates that console support is not enabled for the VM. This parameter is displayed as True when you enable console support for the VM. The default value for `gpu_console=` is False since console support is disabled by default.

   > **Note:** The console may not display the `gpu_console` parameter in the output of the `vm.get` command if the `gpu_console` parameter was not previously enabled.

2. Run the following aCLI command to enable or disable console support for the VM with vGPU:

   ```
   vm.update vm-name gpu_console=true | false
   ```

   Where:

   - true—indicates that you are enabling console support for the VM with vGPU.
   - false—indicates that you are disabling console support for the VM with vGPU.

3. Run the `vm.get` command to check if gpu_console value is true indicating that console support is enabled or false indicating that console support is disabled as you configured it.

   If the value indicated in the `vm.get` command output is not what is expected, then perform **Guest Shutdown** of the VM with vGPU. Next, run the `vm.on vm-name` aCLI command to turn the VM on again. Then run `vm.get` command and check the gpu_console= value.

4. Click a VM name in the **VM** table view to open the VM details page. Click **Launch Console**.
   The Console opens but only a black screen is displayed.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1510

5. Click on the console screen. Click one of the following key combinations based on the operating system you are accessing the cluster from.

   » For Apple Mac OS: Control+Option+2

   » For MS Windows: Ctrl+Alt+2

   The console is fully enabled and displays the content.

PXE Configuration for AHV VMs

You can configure a VM to boot over the network in a Preboot eXecution Environment (PXE). Booting over the network is called PXE booting and does not require the use of installation media. When starting up, a PXE-enabled VM communicates with a DHCP server to obtain information about the boot file it requires.

Configuring PXE boot for an AHV VM involves performing the following steps:

- Configuring the VM to boot over the network.
- Configuring the PXE environment.

The procedure for configuring a VM to boot over the network is the same for managed and unmanaged networks. The procedure for configuring the PXE environment differs for the two network types, as follows:

- An unmanaged network does not perform IPAM functions and gives VMs direct access to an external Ethernet network. Therefore, the procedure for configuring the PXE environment for AHV VMs is the same as for a physical machine or a VM that is running on any other hypervisor. VMs obtain boot file information from the DHCP or PXE server on the external network.
- A managed network intercepts DHCP requests from AHV VMs and performs IP address management (IPAM) functions for the VMs. Therefore, you must add a TFTP server and the required boot file information to the configuration of the managed network. VMs obtain boot file information from this configuration.

A VM that is configured to use PXE boot boots over the network on subsequent restarts until the boot order of the VM is changed.

Configuring the PXE Environment for AHV VMs

The procedure for configuring the PXE environment for a VM on an unmanaged network is similar to the procedure for configuring a PXE environment for a physical machine on the external network and is beyond the scope of this document. This procedure configures a PXE environment for a VM in a managed network on an AHV host.

About this task

To configure a PXE environment for a VM on a managed network on an AHV host, do the following:

Procedure

1. Log on to the Prism web console, click the gear icon, and then click **Network Configuration** in the menu.
2. On **Network Configuration** > **Subnets** tab, click the **Edit** action link of the network for which you want to configure a PXE environment.

   The VMs that require the PXE boot information must be on this network.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1511

3. In the **Update Subnet** dialog box:

   a. Select the **Enable IP address management** check box and complete the following configurations:

   - In the **Network IP Prefix** field, enter the network IP address, with prefix, of the subnet that you are updating.
   - In the **Gateway IP Address** field, enter the gateway IP address of the subnet that you are updating.
   - To provide DHCP settings for the VM, select the **DHCP Settings** check box and provide the following information.

Fields	Description and Values
Domain Name Servers	Provide a comma-separated list of DNS IP addresses. Example: 8.8.8.8, or 9.9.9.9
Domain Search	Enter the VLAN domain name. Use only the domain name format. Example: nutanix.com
TFTP Server Name	Enter a valid TFTP host server name of the TFTP server where you host the host boot file. The IP address of the TFTP server must be accessible to the virtual machines to download a boot file. Example: tftp_vlan103
Boot File Name	The name of the boot file that the VMs need to download from the TFTP host server. Example: boot_ahv202010

4. Under **IP Address Pools**, click **Create Pool** to add IP address pools for the subnet.

   (Mandatory for Overlay type subnets) This section provides the `Network IP Prefix` and `Gateway IP` fields for the subnet.

   (Optional for VLAN type subnet) Check this box to display the `Network IP Prefix` and `Gateway IP` fields and configure the IP address details.

5. (Optional and for VLAN networks only) Check the **Override DHCP Server** dialog box and enter an IP address in the **DHCP Server IP Address** field.

   You can configure a DHCP server using the **Override DHCP Server** option only in case of VLAN networks.

   The DHCP Server IP address (reserved IP address for the Acropolis DHCP server) is visible only to VMs on this network and responds only to DHCP requests. If this box is not checked, the DHCP Server IP Address field is not displayed and the DHCP server IP address is generated automatically. The automatically generated address is `network_IP_address_subnet.254`, or if the default gateway is using that address, `network_IP_address_subnet.253`.

   Usually the default DHCP server IP is configured as the last usable IP in the subnet (For example, its 10.0.0.254 for 10.0.0.0/24 subnet). If you want to use a different IP address in the subnet as the DHCP server IP, use the override option.

6. Click **Close**.

Configuring a VM to Boot over a Network

To enable a VM to boot over the network, update the VM's boot device setting. Currently, the only user interface that enables you to perform this task is the Acropolis CLI (aCLI).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1512

About this task

To configure a VM to boot from the network, do the following:

Procedure

1. Log on to any CVM in the cluster using SSH.
2. Create a VM.

   ```
   nutanix@cvm$ acli vm.create vm num_vcpus=num_vcpus memory=memory
   ```

   Replace *vm* with a name for the VM, and replace *num_vcpus* and *memory* with the number of vCPUs and amount of memory that you want to assign to the VM, respectively.

   For example, create a VM named nw-boot-vm.

   ```
   nutanix@cvm$ acli vm.create nw-boot-vm num_vcpus=1 memory=512
   ```

3. Create a virtual interface for the VM and place it on a network.

   ```
   nutanix@cvm$ acli vm.nic_create vm network=network
   ```

   Replace *vm* with the name of the VM and replace *network* with the name of the network. If the network is an unmanaged network, make sure that a DHCP server and the boot file that the VM requires are available on the network. If the network is a managed network, configure the DHCP server to provide TFTP server and boot file information to the VM. For more information, see Configuring the PXE Environment for AHV VMs on page 216.

   For example, create a virtual interface for VM nw-boot-vm and place it on a network named network1.

   ```
   nutanix@cvm$ acli vm.nic_create nw-boot-vm network=network1
   ```

4. Obtain the MAC address of the virtual interface.

   ```
   nutanix@cvm$ acli vm.nic_list vm
   ```

   Replace *vm* with the name of the VM.

   For example, obtain the MAC address of VM nw-boot-vm.

   ```
   nutanix@cvm$ acli vm.nic_list nw-boot-vm
   00-00-5E-00-53-FF
   ```

5. Update the boot device setting so that the VM boots over the network.

   ```
   nutanix@cvm$ acli vm.update_boot_device vm mac_addr=mac_addr
   ```

   Replace *vm* with the name of the VM and *mac_addr* with the MAC address of the virtual interface that the VM must use to boot over the network.

   For example, update the boot device setting of the VM named nw-boot-vm so that the VM uses the virtual interface with MAC address 00-00-5E-00-53-FF.

   ```
   nutanix@cvm$ acli vm.update_boot_device nw-boot-vm mac_addr=00-00-5E-00-53-FF
   ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1513

6. Power on the VM.

```
nutanix@cvm$ acli vm.on vm_list [host="host"]
```

Replace *vm_list* with the name of the VM. Replace *host* with the name of the host on which you want to start the VM.

For example, start the VM named nw-boot-vm on a host named host-1.

```
nutanix@cvm$ acli vm.on nw-boot-vm host="host-1"
```

Uploading Files to DSF for Microsoft Windows Users

If you are a Microsoft Windows user, you can securely upload files to DSF by using the following procedure.

Procedure

1. Use WinSCP, with SFTP selected, to connect to Controller VM through port 2222 and start browsing the DSF datastore.

   Note: The root directory displays storage containers and you cannot change it. You can only upload files to one of the storage containers and not directly to the root directory. To create or delete storage containers, you can use the Prism user interface.

2. Authenticate by using Prism username and password or, for advanced users, use the public key that is managed through the Prism cluster lockdown user interface.

Enabling Load Balancing of vDisks in a Volume Group

AHV hosts support load balancing of vDisks in a volume group for guest VMs. Load balancing of vDisks in a volume group enables IO-intensive VMs to use the storage capabilities of multiple Controller VMs (CVMs).

About this task

If you enable load balancing on a volume group, the guest VM communicates directly with each CVM hosting a vDisk. Each vDisk is served by a single CVM. Therefore, to use the storage capabilities of multiple CVMs, create more than one vDisk for a file system and use the OS-level striped volumes to spread the workload. This configuration improves performance and prevents storage bottlenecks.

Note:

- vDisk load balancing is disabled by default for volume groups that are directly attached to VMs.

  However, vDisk load balancing is enabled by default for volume groups that are attached to VMs by using a data services IP address.
- If you use web console to clone a volume group that has load balancing enabled, the volume group clone does not have load balancing enabled by default. To enable load balancing on the volume group clone, you must set the load_balance_vm_attachments parameter to true using acli or Rest API.
- You can attach a maximum number of 10 load balanced volume groups per guest VM.
- For Linux VMs, ensure that the SCSI device timeout is 60 seconds. For information about how to check and modify the SCSI device timeout, see the *Controlling the SCSI Command Timer and Device Status* information in Red Hat documentation.

Perform the following procedure to enable load balancing of vDisks by using aCLI.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1514

Procedure

1. Log on to a Controller VM with SSH.
2. Do one of the following:

   » Enable vDisk load balancing if you are creating a volume group.

   ```
   nutanix@cvm$ acli vg.create vg_name load_balance_vm_attachments=true
   ```

   Replace *vg_name* with the name of the volume group.

   » Enable vDisk load balancing if you are updating an existing volume group.

   ```
   nutanix@cvm$ acli vg.update vg_name load_balance_vm_attachments=true
   ```

   Replace *vg_name* with the name of the volume group.

   > **Note:** To modify an existing volume group, you must first detach all the VMs that are attached to that volume group before you enable vDisk load balancing.

3. Verify if vDisk load balancing is enabled.

   ```
   nutanix@cvm$ acli vg.get vg_name
   ```

   An output similar to the following is displayed:

   ```
   nutanix@cvm$ acli vg.get ERA_DB_VG_xxxxxxxx
   ERA_DB_VG_xxxxxxxx {
     attachment_list {
       vm_uuid: "xxxxx"
   .
   .
   .
   .
   iscsi_target_name: "xxxxx"
   load_balance_vm_attachments: True
   logical_timestamp: 4
   name: "ERA_DB_VG_xxxxxxxx"
   shared: True
   uuid: "xxxxxx"
   }
   ```

   If vDisk load balancing is enabled on a volume group, load_balance_vm_attachments: True is displayed in the output. The output does not display the load_balance_vm_attachments: parameter at all if vDisk load balancing is disabled.

4. (Optional) Disable vDisk load balancing.

   ```
   nutanix@cvm$ acli vg.update vg_name load_balance_vm_attachments=false
   ```

   Replace *vg_name* with the name of the volume group.

VM High Availability in Acropolis

Acropolis uses the segment-based reservation method to enable VM high availability. The host-based reservation method is deprecated, and not supported.

If you have not enabled High Availability, in case of host failure, the VMs are restarted from the failed host to any available space on the other hosts in the cluster. Once the failed host joins the cluster again, VMs are migrated back to the host. This type of VM high availability is implemented without reserving any resources. Admission control is not enforced and hence there may not be sufficient capacity available to start all the VMs.

> **Note:**

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1515

- Nutanix does not support VMs that are running with 100% remote storage for High Availability. The VMs must have at least one local disk that is present on the cluster.
- The VM HA does not reserve the memory for the non-migratable VMs. For information on how to check the non-migratable VMs, see Checking Live Migration Status of a VM in the *Prism Central Infrastructure Guide*.

The VM HA uses the Guarantee mode with segment-based reservation method.

In segment-based reservation, the cluster is divided into segments to ensure that enough space is reserved for any host failure. Each segment corresponds to the largest VM that is guaranteed to be restarted in case the failure occurs. The other factor is the number of host failures that can be tolerated. Using these inputs, the scheduler implements admission control to always have enough resources reserved so that the VMs can be restarted upon failure of any host in the cluster.

The segment size ensures that the largest VM can be powered on in HA failover when cluster is fully loaded (if the cluster is fully used except the reserved segments). The number of segments that is reserved is such a way that for each host enough resources are reserved to ensure that any host failure in the cluster is tolerated. Multiple VMs may fit into a segment. If anything changes in the cluster, the reservation is computed again. The total resources reserved for segments can be more than the resources used by running VMs. This implementation guarantees successful failover even in the case of fragmentation of segments. The actual number of reserved resources depends on the current load of the cluster, but it is typically at 1 to 1.25 times the resource usage on the most loaded host.

If the host enters maintenance mode (in case of host upgrade), you might not be protected against further host failures. Maintenance mode uses reservations made for HA for migrating VMs from the host. Although you are not protected against host failure if you have reservation for HA, hypervisor upgrade occurs without any difficulty because from the perspective of a user it is the same as host failure except that the VMs are migrated (instead of restarted) and hence no runtime state is lost. The HA status goes through the same states as it goes when the host failure had occurred.

Fault Detection for High Availability

Acropolis version 6.1 (with minimum supported AHV version 20201105.2229) onwards, the fault detection mechanism for High Availability checks for the heartbeat of the management services on the host. If any one of the services are down, then the host is marked as disconnected.

In addition to this, the fault detection mechanism also performs the following health checks for the host:

- Root file system corruption
- Read-only root file system

If any of the above-mentioned health checks are affirmative, then the host is marked as disconnected.

If the host remains in the disconnected status for 40 seconds, the VMs running on the affected host are automatically restarted (based on the resource availability) .

You can view the alerts raised for any of the above-mentioned checks in the **Activity** > **Alerts** view in Prism UI.

Enabling High Availability for the Cluster

In Acropolis managed clusters, you can enable high availability for the cluster to ensure that VMs can be migrated and restarted on another host in case of failure.

About this task

After you enable high availability for the cluster, if a host failure occurs the cluster goes through following changes.

- OK: This state implies that the cluster is protected against a host failure.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1516

- Healing: Healing period is the time that Acropolis brings the cluster to the protected state. There are two phases to this state. The first phase occurs when the host fails. The VMs are restarted on the available host. After restarting all the VMs if there are enough resources to protect the VM, the HA status of the cluster comes back to OK state. If this does not occur, the cluster goes into critical state. The second phase occurs when the host comes back from the failure. Once the host comes back from failure, no VMs are present on the host and hence during this healing phase restore locality task occurs (VMs are migrated back). Apart from restoring the locality of the VMs, the restore locality task ensures that the cluster is back to the same state before the HA failure. Once it is finished, the HA status is back to OK state.
- Critical: If the host is down, the HA status of the cluster goes into Critical state. This happens because the cluster cannot tolerate any more host failures. You have to ensure that you bring back the host so that your cluster is protected against any further host failures.

  Note: On a less loaded cluster, it is possible for HA to go directly back to OK state if enough resources is reserved to protect another host failure. The start and migrate operations on the VMs are restricted in the Critical state because Acropolis continuously tries to ensure that the HA status is back to the OK state.

Procedure

1. Log in to the Prism Element web console.
2. Click the gear icon in the main menu and then select **Manage VM High Availability** in the **Settings** page.

   Note: This option does not appear in clusters that do not support this feature.

   The **Manage VM High Availability** dialog box appears.
3. Check the **Enable HA Reservation** box and then click the **Save** button to enable.

Viewing list of restarted VMs after an HA event

This section provides the information about how to view the list of VMs that are restarted after an HA event in the AHV cluster.

About this task

If an AHV host becomes inaccessible or fails due to some unplanned event, the AOS restarts the VMs across the remaining hosts in the cluster.

Procedure

To view the list of restarted VMs after an HA event:

1. Log in to Prism Central or Prism web console.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1517

2. View the list of restarted VMs on either of the following pages:

   - **Events** page:

     1. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Activity** > **Events** in Prism Central. For more information, see Prism Central Alerts and Events Reference Guide.

        Navigate to **Alerts** > **Events** from the main menu to access the **Events** page in the *Prism web console*.
     2. Locate or search for the following string, and hover over or click the string:

        VMs restarted due to HA failover

        The system displays the list of restarted VMs in the **Summary** page and as a hover text for the selected event.

        For example:

        ```
        VMs restarted due to HA failover: VM_Name1, VM_Name2, VM_Name3, VM_Name4. VMs
         were running on host X.X.X.1 prior to HA.
        ```

     Observe `VM_Name1`, `VM_Name2`, `VM_Name3`, and `VM_Name4` as the actual VMs in your cluster.

   - **Tasks** page:

     1. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Activity** > **Tasks** in Prism Central.

        Navigate to **Tasks** from the main menu to access the **Tasks** page in the Prism web console.
     2. Locate or search for the following task, and click **Details**:

        HA failover

        The system displays a list of related tasks for the HA failover event.
     3. Locate or search for the following related task, and click **Details**:

        Host restart all VMs

        The system displays **Restart VM group** task for the HA failover event.
     4. In the **Entity Affected** column, click **Details**, or hover over the **VMs** text for **Restart VM group** task:

     The system displays the list of restarted VMs:

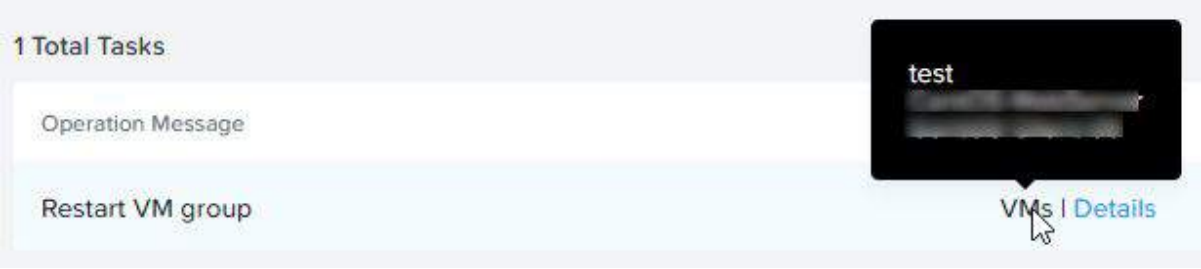


Figure 37: List of restarted VMs

Live vDisk Migration Across Storage Containers

vDisk migration allows you to change the container of a vDisk. You can migrate vDisks across storage containers while they are attached to guest VMs without the need to shut down or delete VMs (live migration). You can either migrate all vDisks attached to a VM or migrate specific vDisks to another container.

In a Nutanix solution, group the vDisks into storage containers and attach vDisks to guest VMs. AOS applies storage attributes such as replication factor, encryption, compression, deduplication, and erasure coding at the storage container level. If you apply a storage policy to a storage container, AOS enables that policy on all the vDisks of the container. If you want to change the policies of the vDisks (for example, from RF2 to RF3), create another container with a different policy and move the vDisk to that container. With live migration of vDisks across containers, you can migrate vDisk across containers even if those vDisks are attached to a live VM. Thus, live migration of vDisks across storage containers enables you to efficiently manage storage policies for guest VMs.

General Considerations

You cannot migrate images or volume groups.

You cannot perform the following operations during an ongoing vDisk migration:

- Clone the VM
- Resize the VM
- Take a snapshot

> **Note:** During vDisk migration, the logical usage of a vDisk is more than the total capacity of the vDisk. The issue occurs because the logical usage of the vDisk includes the space occupied in both the source and destination containers. Once the migration is complete, the logical usage of the vDisk returns to its normal value.
>
> Migration of vDisks stalls if sufficient storage space is not available in the target storage container. Ensure that the target container has sufficient storage space before you begin migration.

Disaster Recovery Considerations

Consider the following points if you have a disaster recovery and backup setup:

- You cannot migrate vDisks of a VM that is protected by a protection domain or protection policy. When you start the migration, ensure that the VM is not protected by a protection domain or protection policy. If you want to migrate vDisks of such a VM, do the following:
  - Remove the VM from the protection domain or protection policy.
  - Migrate the vDisks to the target container.
  - Add the VM back to the protection domain or protection policy.
  - Configure the remote site with the details of the new container.

  vDisk migration fails if the VM is protected by a protection domain or protection policy.
- If you are using a third-party backup solution, AOS temporarily blocks snapshot operations for a VM if vDisk migration is in progress for that VM.

Migrating vdisk from Prism Central

Starting with Prism Central 2023.4, the individual VM disks can be migrated using Prism Central UI. You can change the storage container of the disk from the **Storage Container** field:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1519

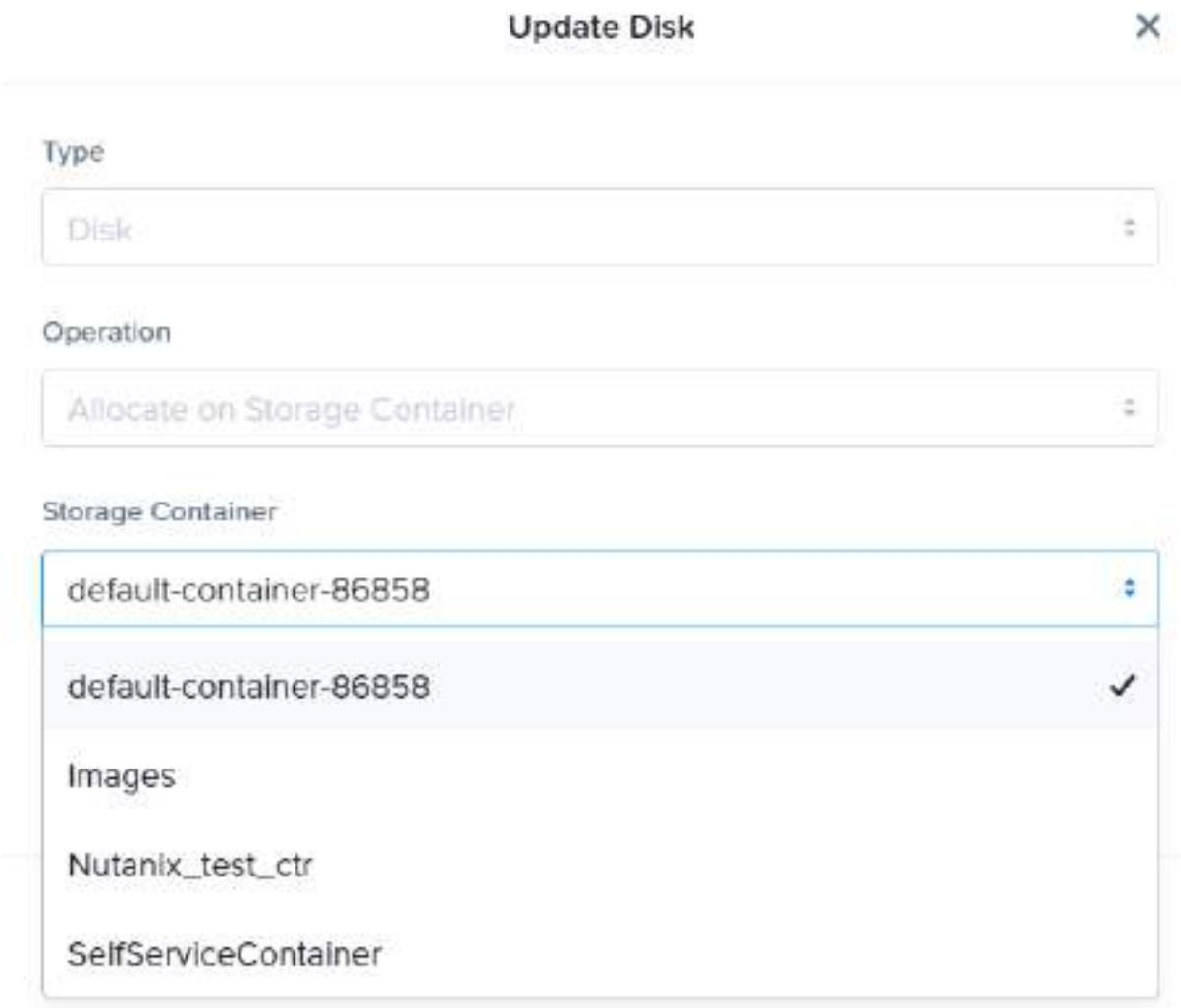


Figure 38: Storage Container Update

For more information, see Updating a VM through Prism Central (AHV) section in *Prism Central Infrastructure Guide*. If more granular control is required, perform the steps through acli as described in Migrating a vDisk to Another Container on page 225.

Migrating a vDisk to Another Container

You can either migrate all vDisks attached to a VM or migrate specific vDisks to another container.

About this task

> **Note:** Starting with Prism Central 2023.4, the individual VM disks can be migrated using Prism Central UI. For more information, see Migrating vdisk from Prism Central on page 224. However, if more granular control is required, perform the steps through acli as described in this section.

Procedure

Perform the following steps to migrate vDisks across storage containers:

1. Log on to a CVM in the cluster with SSH.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1520

2. Do one of the following:

   » Migrate all vDisks of a VM to the target storage container.

   ```
   nutanix@cvm$ acli vm.update_container vm-name container=target-container
    wait=false
   ```

   Replace *vm-name* with the name of the VM whose vDisks you want to migrate and *target-container* with the name of the target container.

   » Migrate specific vDisks by using either the UUID of the vDisk or address of the vDisk.

   Migrate specific vDisks by using the UUID of the vDisk.

   ```
   nutanix@cvm$ acli vm.update_container vm-name device_uuid_list=device_uuid
    container=target-container wait=false
   ```

   Replace *vm-name* with the name of VM, *device_uuid* with the device UUID of the vDisk, and *target-container* with the name of the target storage container.

   Run `nutanix@cvm$ acli vm.get vm-name` to determine the device UUID of the vDisk.

   You can migrate multiple vDisks at a time by specifying a comma-separated list of device UUIDs of the vDisks.

   Alternatively, you can migrate vDisks by using the address of the vDisk.

   ```
   nutanix@cvm$ acli vm.update_container vm-name disk_addr_list=disk-address
    container=target-container wait=false
   ```

   Replace *vm-name* with the name of VM, *disk-address* with the address of the disk, and *target-container* with the name of the target storage container.

   Run `nutanix@cvm$ acli vm.get vm-name` to determine the address of the vDisk.

   Following is the format of the vDisk address:

   ```
   bus.index
   ```

   Following is a section of the output of the `nutanix@cvm$ acli vm.get vm-name` command:

   disk_list { addr { bus: "scsi" index: 0 }

   Combine the values of bus and index as shown in the following example:

   ```
   nutanix@cvm$ acli vm.update_container TestUVM_1 disk_addr_list=scsi.0
    container=test-container-17475
   ```

   You can migrate multiple vDisks at a time by specifying a comma-separated list of vDisk addresses.

3. Check the status of the migration in the **Tasks** menu of the Prism Element web console.

4. (Optional) Cancel the migration if you no longer want to proceed with it.

   ```
   nutanix@cvm$ ecli task.cancel task_list=task-ID
   ```

   Replace *task-ID* with the ID of the migration task.

   To determine the task ID, run the following command:

   ```
   nutanix@cvm$ ecli task.list
   ```

   Look for the task with **Component** as `anduril` and **Type** as `VmChangeDiskContainer`, and note the ID of the task.

   For example:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1521

```
Task UUID                                Parent Task UUID
 Component       Sequence-id     Type                    Status          Creation
 Time(UTC)   Completion Time(UTC)
a8389df9-64c0-4d79-43ed-7bbd002e1d2f    3aafa550-a81f-4128-5925-a45c8bcf8114
 anduril         8114            VmChangeDiskContainer   kRunning        2024-12-18
 21:21:56
```

Note: Note the following points about canceling migration:

- If you cancel an ongoing migration, AOS retains the vDisks that have not yet been migrated in the source container. AOS does not migrate vDisks that have already been migrated to the target container back to the source container.
- If sufficient storage space is not available in the original storage container, migration of vDisks back to the original container stalls. To resolve the issue, ensure that the source container has sufficient storage space.

Memory Overcommit

The Memory Overcommit feature enables you to optimize the physical memory utilization of a VM. It allows the host to automatically detect whether the memory is under-utilized or over-utilized for a VM. Using Prism Central, you can enable the Memory Overcommit feature. For information on how to enable the Memory Overcommit feature, see Memory Overcommit Management on page 232.

After you enable the Memory Overcommit feature, the host performs the following actions:

- Automatically combines and uses the excess or unutilized memory of a VM, or even uses the disk space to swap out VM memory.
- Uses the reclaimed physical memory to provision the memory requirements of another VM, or to create another VM.

Note:

- Memory overcommit enables the host to optimize and overcommit memory for any existing or new VM within the host. It does not support the utilization of memory for VMs across the hosts. For example, overcommitted memory of VM1 on Host1 cannot be utilized on VMs on Host2. It can only be utilized for another VM on Host1 itself.
- The reclaiming of unutilized VM memory requires the system to observe multiple memory usage cycles of the VM to conclude on the memory usage pattern of the VM. The system might take up to 3 minutes for memory accounting process to reclaim the unutilized memory.

Caution: AHV does not support a memory overcommit of more than four times the allocated physical memory. For High Availability - Reserved Segments (HA-RS) setup, a memory overcommit beyond 33% of allocated physical memory leads to performance issues, and the system disallows the VM power on operation.

With the Memory Overcommit feature enabled on the host, the total memory assigned to all the VMs by the host can be greater than the total physical memory installed on the host. For more information on VM memory allocation with Memory Overcommit feature, see the deployment example described in Memory Overcommit Deployment Example on page 228.

Deployment Workflow

You can enable or disable the Memory Overcommit feature using Prism Central on new or existing VMs.

Note: Ensure the VMs are shut down before you enable or disable the Memory Overcommit feature.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1522

Memory Overcommit is useful in test and development environments to verify the performance of the VM. Based on the memory usage of the VM, AHV calculates an appropriate memory size for each VM enabled with Memory Overcommit.

Essential Concepts

Over Provisioned VM

A VM with a memory allocation that is more than the actual requirement to run the application on it is called an Over Provisioned VM. For example, a VM with an allocation of 10 GB memory to run an SQL server that only requires 7 GB of memory to operate is categorized as an Over Provisioned VM. In this case, the VM is over provisioned by 3 GB. This over provisioned memory is unused by the VM. The host can use this unutilized memory to add a new VM or allocate more memory to an existing VM, even if the physical memory is not available on the host.

Memory Overcommitted VM

A memory overcommitted VM is a VM that has the Memory Overcommit feature enabled and shares its unutilized memory with the host. By default, each VM is guaranteed to have at least 25% of its memory provisioned as physical memory. The remaining 75% is either unutilized in the VM and reclaimed for use in other VMs or swapped out to the host swap disks.

Memory Overcommit is required for the following types of VMs:

- A VM with an unutilized memory due to over provisioning.
- A VM with workloads which are not sensitive to frequent memory access. The frequency of memory access is increased due to swapping of VM memory to host swap disks.

Host Swap

After installing or upgrading the current AOS version of the cluster to AOS 6.0.2 with AHV 20201105.30007 or later, Memory Overcommit is available for the cluster. Swap disks are created on the ADSF for every host in the cluster.

Memory Overcommit reclaims memory from a guest VM that has unutilized memory by default. The host swap memory is utilized when the guest VM does not permit the reclamation of memory due to the amount of memory utilized in the guest VM.

> **Note:** The performance of the swap memory depends on the hardware, workload, and the guest VM. The swap memory defined in the operating system of the guest VM (guest VM swap) may result in better performance characteristics than host swap. It is always recommended to increase guest VM swap instead of relying on host swap. For example, you can increase the guest VM swap up to RAM size of the guest VM.

Memory Overcommit Deployment Example

Example: A 128 GB host with three VMs (64 GB + 32 GB + 32 GB)

Observations Before Memory Overcommit

Observe the following attributes before you enable Memory Overcommit:

- The physical memory of the host is equal to the total memory of all the VMs.
- The host cannot add a new VM as the host's physical memory is fully committed.

Action

Enable the Memory Overcommit feature on all the three VMs. For more information, see Memory Overcommit Management on page 232.

> **Note:**

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1523

Ensure that you adhere to the requirements and Nutanix recommendations for Memory Overcommit. For more information, see Requirements and Recommendations for Memory Overcommit on page 230.

Observations After Memory Overcommit

If the VMs are not fully utilizing their allocated memory, the host allows you to create a new VM with a memory size that is equal to or less than the amount of unutilized memory. When the new VM is started, the host attempts to reclaim the unutilized memory from the running VMs and makes it available for the new VM.

The following table shows the example of a 128 GB host with the total utilized and unutilized memory:

Table 40: Memory Overcommit Example

Host 1 (128 GB)			
VMs	**VM Memory (GB)**	**Utilized Memory (GB)**	**Unutilized Memory (GB)**
VM1	64 GB	48 GB	16 GB
VM2	32 GB	20 GB	12 GB
VM3	32 GB	24 GB	8 GB
Total	128 GB	92 GB	36 GB

In this example, the host can combine the 36 GB of unutilized physical memory to create a new VM up to an aggregate size of 36 GB. Even though the unutilized memory can be reclaimed from a running VM, all the new VMs memory must be allocated from physical memory. In this case, you can start a new VM only with less than or equal to the total memory that is reclaimable from other VMs.

In the following table, you can observe the following attributes:

- VMs 1,2 and 3 are over-committed by 16 GB, 12 GB, and 8 GB respectively (thus over-committed by 36 GB cumulatively) which can be reclaimed by the host.
- The information on the memory reclaim process is also indicated in the *Utilized Memory (GB)* column.
- The host creates a new VM - VM4 with an allocated memory of 32 GB.

In this scenario, if the VM4 is only utilizing 28 GB of the allocated 32 GB, it is possible to start a new VM with up to 8GB of memory allocated with reclamation of unutilized memory of 4 GB.

Table 41: Memory Overcommit Example

Host 1 (128 GB)			
VMs	**VM Memory (GB)**	**Utilized Memory (GB)**	**Unutilized Memory (GB)**
VM1	64 GB	48 GB	4 GB
VM2	32 GB	20 GB	
VM3	32 GB	24 GB	
VM4	32 GB	28 GB	4 GB
Total	160 GB	120 GB	8 GB

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1524

> **Note:** Before the Memory Overcommit feature is enabled, the physical memory of the host is equal to the total memory of all the VMs. After the memory overcommit feature is enabled on the host, the total of all the memory assigned to VMs by the host can *appear* to be greater than the total physical memory installed on the host.

*Important:*The above example is subject to the considerations mentioned in Requirements and Limitations sections. The guest VM utilizes the memory, which is reclaimed to permit the starting of a new VM, only when it experiences a greater memory pressure. In this case, the system identifies the requirement of additional memory for the guest VM and attempts to correctly balance the memory in other VMs based on their memory utilization. If the system is not able to reduce the memory pressure with unutilized memory, it falls back to utilize the host swap to reduce the memory pressure of the guest VM. For example, if VM1 listed in the above table requires an additional 10GB of memory, the system attempts to recover the unutilized 1GB from VM2, 1GB from VM3 and 4GB from VM4. You can observe that a shortfall of 4GB occurs to reduce the memory pressure in VM1, even when the system applies this action. In this case, the system allocates the shortfall memory of 4GB from host swap.

> **Note:** ADS tracks the memory usage on the host and, if the host is in an over-committed state for memory, it is required to migrate VMs to mitigate over-committed memory hotspots.

Requirements and Recommendations for Memory Overcommit

Ensure that you meet the following requirements to enable Memory Overcommit feature:

- Install the balloon drivers. For example, for Windows VM, install the latest VirtIO driver package.

  The balloon drivers enable the system to get visibility of the OS memory usage and reclaim the unutilized memory.

  The latest VirtIO drivers ensure minimal impact on the performance of the Windows VM enabled with Memory Overcommit.

- With a minimum Prism Central version of pc.2022.4, you can enable or disable the Memory Overcommit feature using Prism Central on new or existing VMs.

Nutanix Recommendations for Memory Overcommit

Nutanix recommends that you adhere to the following guidelines for optimal performance of the guest VM when you enable Memory Overcommit:

- The swap memory defined in the operating system of the guest VM is greater than or equal to the RAM size of the guest VM.
- The appropriate balloon drivers are installed on the guest VMs.
- The guest VMs should have more than 1 vCPUs. This is to ensure that the guest VMs, for which you intend to enable the Memory Overcommit, has appropriate vCPUs to reclaim memory.

  > **Note:** The Memory Overcommit functionality might be impacted if you have only 1 vCPU allocated to the guest VM.

Limitations of Memory Overcommit

Memory overcommit has the following limitations:

- You can enable or disable Memory Overcommit only while the VM is powered off.
- Power off the VM enabled with memory overcommit before you change the memory allocation for the VM.

  For example, you cannot update the memory of a VM that is enabled with memory overcommit when it is still running. The system displays the following alert: InvalidVmState: Cannot complete request in state on.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1525

- Memory overcommit is not supported with VMs that use GPU configurations (both GPU passthrough and vGPU) or vNUMA.

  For example, you cannot update a VM to a vNUMA VM when it is enabled with memory overcommit. The system displays the following alert: InvalidArgument: Cannot use memory overcommit feature for a vNUMA VM error.

- Memory overcommit feature can slow down the performance and the predictable performance of the VM.

  For example, migrating a VM enabled with Memory Overcommit takes longer than migrating a VM not enabled with Memory Overcommit.

- There may be a temporary spike in the aggregate memory usage in the cluster during the migration of a VM enabled with Memory Overcommit from one node to another.

  For example, when you migrate a VM from Node A to Node B, the total memory used in the cluster during migration is greater than the memory usage before the migration.

  The memory usage of the cluster eventually drops back to pre-migration levels when the cluster reclaims the memory for other VM operations.

- Using Memory Overcommit heavily can cause a spike in the disk space utilization in the cluster. This spike is caused because the Host Swap uses some of the disk space in the cluster.

  If the VMs do not have a swap disk, then in case of memory pressure, AHV uses space from the swap disk created on ADSF to provide memory to the VM. This can lead to an increase in disk space consumption on the cluster.

- All DR operations except Cross Cluster Live Migration (CCLM) are supported.

  On the destination side, if a VM fails when you enable Memory Overcommit, the failed VM fails over (creating the VM on the remote site) as a fixed size VM. You can enable Memory Overcommit on this VM after the failover is complete.

- When Memory Overcommit is enabled, you cannot perform *Memory hot add* to include additional memory resources for a VM.

Total Memory Allocation Mechanism on Linux and Windows VM

The guest OS for the VM should have the balloon drivers installed. For example, VirtIO drivers are needed for the Windows VM. This enables the system to get a visibility of the OS memory usage and reclaim the unutilized memory. For more information, see Requirements and Recommendations for Memory Overcommit on page 230.

When you enable the Memory Overcommit on a Linux VM and Windows VM with the same memory size, you can observe the following difference in memory allocation mechanism between Linux VM and Windows VM:

- In the *Linux VM* case, the system adjusts the *Total Memory* to accommodate the balloon driver memory consumption.
- In the *Windows VM* case, the system adjusts the *Used Memory* (memory usage) to accommodate the balloon driver memory consumption. The *Total Memory* always remains the same as assigned during initial provisioning.

The following table provides the information about the memory allocation observations made on the Linux VM and Windows VM:

Note:

- The cache, shared, and buffer memories are intentionally not shown in the following table. The system adjusts the cache memory in the Free Memory.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1526

- The following attributes are used in the following table:
  - X - Indicates the Total Memory assigned to the VM during initial provisioning.
  - Y - Indicates the memory consumed by the Linux or Windows Balloon Drivers
  - Z -Indicates the Used Memory (VM memory usage)

Table 42: Memory Allocation - Linux VM and Windows VM

Total Memory assigned to the VM (in GB	VM OS	Balloon Drivers Memory Consumption (GB)	Memory Allocation Observation on VM		
			Used Memory (in GB)	Free Memory (in GB)	Total Memory (in GB)
X	Linux	Y	Z	X - Z	X – Y
	Windows		Z + Y	X - (Y +Z)	X
For example, if X = 16, Y = 0.5, and Z = 2.5					
16	Linux	0.5	2.5	13.5	15.5
	Windows		3	13	16

Memory Overcommit Management

This section describes how to enable and disable the Memory Overcommit function using Prism Central and CLI.

Enabling Memory Overcommit While Creating a VM

This procedure helps you enable memory overcommit in a VM that you create in Prism Central. You need a minimum Prism Central version of pc.2022.4 for this procedure.

Before you begin

Ensure that the following prerequisites are met before you enable Memory Overcommit:

- Check the requirements and recommendations as described in Requirements and Recommendations for Memory Overcommit on page 230.
- Check all the limitations as described in Limitations of Memory Overcommit on page 230.

About this task

When you are creating a VM, you can enable memory overcommit for it.

You cannot enable the memory overcommit feature using the Prism Element Web Console. Enable memory overcommit on a VM that you create by using Prism Central. If you create a VM using Prism Web Console, then you can enable memory overcommit on that VM using Prism Central. For the procedure to enable memory overcommit on a VM that you have already created, see Enabling or Disabling Memory Overcommit on Existing VMs on page 233.

Procedure

To enable memory commit while creating a VM, perform the following steps:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1527

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-Specific Navigation Bar.
   The system displays the page with **Lists** tab by default with all the VMs across registered clusters.
3. Click **Create VM**.
   The system displays the **Create VM** window.
4. Enter all the details necessary to create the VM, and select the **Enable Memory Overcommit** checkbox.
5. Click **Next**.
6. Provide the details necessary for the VM creation in the **Resources** and **Management** steps, and click **Next**.

   For more information, see Creating a VM through Prism Central (AHV) information in the *Prism Central Infrastructure Guide* .
7. In the **Review** step, ensure that the **Memory Overcommit** configuration is displayed as **Enabled**.

   If **Memory Overcommit** configuration is not displayed as **Enabled**, click **Edit** to go back to the **Configuration** step, and select the **Enable Memory Overcommit** checkbox.
8. Click **Save**.

What to do next

The **Tasks** page displays the VM creation task. After it is successfully completed, check the **VMs** dashboard to verify that the VM is created and the value in the **Memory Overcommit** column displays **Enabled**.

> **Note:** The default **General** list view does not provide the **Memory Overcommit** column. Create your own customized view and add the **Memory Overcommit** column to that view. You can also add other columns to your customized view.

Click the newly created VM to open the VM details page. In the **Summary** tab, the **Properties** widget displays **Enabled** for the **Memory Overcommit** property.

Enabling or Disabling Memory Overcommit on Existing VMs

The procedures in this section enable you to enable memory overcommit in one or more existing VMs. You need a minimum Prism Central version of pc.2022.4 for this procedure.

Before you begin

Ensure that the following prerequisites are met before you enable Memory Overcommit:

- Check the requirements and recommendations as described in Requirements and Recommendations for Memory Overcommit on page 230.
- Check all the limitations as described in Limitations of Memory Overcommit on page 230.
- The guest VM on which you want to enable memory overcommit is powered off. If the VM is powered on or is in **Soft Shutdown** state, the **Enable Memory Overcommit** action is not available in the **Actions** dropdown list.

Procedure

To enable memory overcommit in one or more existing VM, perform the following steps:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1528

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-Specific Navigation Bar.
   The system displays the page with **Lists** tab by default with all the VMs across registered clusters.
3. Select the target VM checkbox, and choose **Enable Memory Overcommit** from the actions dropdown menu.
   You can select one VM or multiple VMs at a time as a bulk update to enable memory overcommit.
4. In the **Actions** dropdown list, click the **Enable Memory Overcommit** action.

   > **Note:** For an individual VM, you can also enable the memory overcommit from the update VM workflow. For more information, see Updating a VM through Prism Central (AHV) information in *Prism Central Infrastructure Guide*.

   To disable the memory overcommit, select the target VM checkbox, and choose **Disable Memory Overcommit** from the **Actions** dropdown menu.

What to do next

You can check the update tasks in the **Tasks** page. If you selected multiple VMs to enable or disable memory overcommit, the **Task** page displays the update for each VM as a separate **Update VM** task. For more information, see Tasks View information in *Prism Central Infrastructure Guide*.

You can verify the memory overcommit status as **Enabled** or **Disabled** using the following methods:

- Select **Performance** from the **View By** option in VMs Summary View.
- Navigate to the VM Details View , and observe the Memory Overcommit field in the **Properties** widget.

Enabling Memory Overcommit using CLI

You can configure memory overcommit on a new VM or on an existing VM after shutting it down and enabling memory overcommit on it.

Before you begin

Ensure that the following prerequisites are met before you enable Memory Overcommit:

- Check the requirements and recommendations as described in Requirements and Recommendations for Memory Overcommit on page 230.
- Check all the limitations as described in Limitations of Memory Overcommit on page 230.
- The guest VM on which you want to enable memory overcommit is powered off.

About this task

Perform the following procedure to enable memory overcommit on an existing VM after shutting it down:

Procedure

1. Log on to the Controller VM using SSH.
2. At the CVM prompt, type `acli` to enter the acropolis CLI mode.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1529

3. Shut down the VM to enforce an update on the VM.

   ```
   acli> vm.shutdown vm-name
   ```

   Replace *vm-name* with the name of the VM.

4. Update the VM to enable memory overcommit.

   ```
   acli> vm.update vm-name memory_overcommit=True
   ```

   Replace *vm-name* with the name of the VM.

   > **Note:** Use the wildcard * to list out VMs of similar naming scheme and enable memory overcommit on them.
   >
   > `acli> vm.update vm-name* memory_overcommit=True`
   >
   > Use *vm-name** to update multiple VMs that follow identical naming scheme.
   >
   > For example, Host 1 has six VMs (VM1, VM2, VM3, FileServer, SQL server, VM4), then `vm.update VM* memory_overcommit=True` CLI command will only update VM1, VM2, VM3, and VM4. It will not update the FileServer and SQL Server VMs on the host.

   > **Note:** Use your discretion while using the wildcard * without mentioning the VM naming scheme. Doing so will update all the VMs in the cluster, including the VMs that you may not want to configure with memory overcommit.

5. Verify memory overcommit configuration.

   The memory_overcommit parameter should be set to `True`.

   ```
   acli> vm.get vm-name
   ```

   Replace *vm-name* with the name of the VM.

6. Start the VM.

   ```
   acli> vm.on vm-name
   ```

   Replace *vm-name* with the name of the VM.

Disabling Memory Overcommit using CLI

You can disable memory overcommit on an existing VM after shutting it down and changing the memory overcommit configuration of the VM.

Before you begin

Ensure that the following prerequisites are met before you disable Memory Overcommit:

- Check the requirements and recommendations as described in Requirements and Recommendations for Memory Overcommit on page 230.
- Check all the limitations as described in Limitations of Memory Overcommit on page 230.
- The guest VM on which you want to disable memory overcommit is powered off.

About this task

Perform the following procedure to disable memory overcommit on an existing VM:

Procedure

1. Log on to the Controller VM using SSH.
2. At the CVM prompt, type `acli` to enter the acropolis CLI mode.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1530

3. Shut down the VM.

   ```
   acli> vm.shutdown vm-name
   ```

   Replace *vm-name* with the name of the VM.

4. Update the VM to disable memory overcommit.

   ```
   acli> vm.update vm_name memory_overcommit=False
   ```

   Replace *vm-name* with the name of the VM.

   > **Note:** Use the wildcard * to list out VMs of similar naming scheme and disable memory overcommit on them.
   >
   > `acli> vm.update vm-name* memory_overcommit=False`
   >
   > Use *vm-name** to update multiple VMs that follow identical naming scheme.
   >
   > For example, Host 1 has six VMs (VM1, VM2, VM3, File Server, SQL server, VM4), then `vm.update VM* memory_overcommit=False` CLI command will only update VM1, VM2, VM3, and VM4. It will not update the File Server and SQL Server VMs on the host.

   > **Note:** Use your discretion while using the wildcard * without mentioning the VM naming scheme. Doing so will update all the VMs in the cluster, including the VMs that you may not want to configure with memory overcommit.

5. Start the VM.

   ```
   acli> vm.on vm-name
   ```

   Replace *vm-name* with the name of the VM.

OVAs

An Open Virtual Appliance (OVA) file is a tar archive file created by converting a virtual machine (VM) into an Open Virtualization Format (OVF) package for easy distribution and deployment. OVA helps you to quickly create, move or deploy VMs on different hypervisors.

Prism Central helps you perform the following operations with OVAs:

- Export an AHV VM as an OVA file.
- Upload OVAs of VMs or virtual appliances (vApps). You can import (upload) an OVA file with the QCOW2 or VMDK disk formats from a URL or the local machine.
- Deploy an OVA file as a VM.
- Download an OVA file to your local machine.
- Rename an OVA file.
- Delete an OVA file.
- Track or monitor the tasks associated with OVA operations in **Tasks**.

The access to OVA operations is based on your role. See *Role Details View* in the Prism Central Admin Center Guide to check if your role allows you to perform the OVA operations.

For information on:

- Restrictions applicable to OVA operations, see OVA Restrictions on page 237.
- The OVAs dashboard, see OVAs View in the *Prism Central Infrastructure Guide*.
- Exporting a VM as an OVA, see Exporting a VM as an OVA in the *Prism Central Infrastructure Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1531

- Other OVA operations, see OVA Management in the *Prism Central Infrastructure Guide*.

OVA Restrictions

You can perform the OVA operations subject to the following restrictions:

- Export to or upload OVAs with one of the following disk formats:
  - QCOW2: Default disk format auto-selected in the **Export as OVA** window. For more information, see Exporting a VM as an OVA information in *Prism Central Infrastructure Guide*.
  - VMDK: Deselect QCOW2 and select VMDK, if required, before you submit the VM export request when you export a VM.
  - When you export a VM or upload an OVA and the VM or OVA does not have any disks, the disk format is irrelevant.
- Upload an OVA to multiple clusters using a **URL** as the source for the OVA. You can upload an OVA only to a single cluster when you use the local **OVA File** source. For more information, see Uploading an OVA information in *Prism Central Infrastructure Guide*.
- Perform the OVA operations only with appropriate permissions. You can run the OVA operations that you have permissions for, based on your assigned user role.
- The OVA that results from exporting a VM on AHV is compatible with any AHV version 5.18 or later.
- The minimum supported versions for performing OVA operations are AOS 5.18, Prism Central 2020.8, and AHV-20190916.253.
- OVAs are not supported for vTPM and credential guard.

VM Generation UUID and BIOS UUID Support in AHV

This section provides the information about VM Generation UUID and BIOS UUID.

The VM Generation UUID is a 64-bit unique virtual machine identifier that is used to identify the occurrence of any time shift event for the VM. The BIOS UUID is a 64-bit unique hardware identifier that helps you to identify any underlying hardware change for the VM. BIOS UUID is only relevant to the VM, and does not qualify as a VM identity for any external communication.

The AHV allocates the Generation UUID and BIOS UUID to the guest VM.

The VM Generation UUID enables you to identify any change to the VM's place in time and apply necessary safety measures to protect the application environment during VM rollback, recovery, or any operation that affects the VM's place in time.

For more information about Virtual Machine Generation Identifier, see *Virtual machine generation identifier* topic in *Microsoft Technical Documentation*.

The following table describes the scenarios in which a new Generation UUID and BIOS UUID is allocated to the guest VM or the existing Generation UUID and BIOS UUID are retained.

Scenarios	New Generation UUID
VM Creation VM Creation using Template VM Creation using OVA	Yes
VM Update	No
VM Reboot	No

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1532

Scenarios	New Generation UUID
VM Host Reboot	No
VM Clone from another VM	Yes
VM Clone, copy, or import from VM Snapshot	Yes
VM Pause or resume	No
High Availability (HA) restart case	No
VM Migration within a cluster	No
Recover VM from backup	Yes
VM Restore from AHV snapshot, recovery point, or Cerebro snapshots	Yes
Unplanned failover with Asynchronous Replication Schedule	Yes
Planned failover with Asynchronous Replication Schedule	No
Unplanned failover with Synchronous Replication Schedule	Yes
Planned Failover with Synchronous Replication Schedule	No
Cross-Cluster Live Migration (CCLM) On-Demand CCLM Cold Migration using Move	The system persists the existing Generation U site supports Generation UUID and BIOS UU
Cross Hypervisor Disaster Recovery (CHDR)	

Checking VM Generation UUID and BIOS UUID of a Guest VM

This section describes how to check the VM Generation UUID and BIOS UUID of a guest VM using acli.

Before you begin

Ensure you meet the following requirements before you check the VM Generation UUID and BIOS UUID of a guest VM:

- Deploy the AOS 6.6.1 version or later at your site.
- **Power Cycle** the guest VMs if you have upgraded to AOS 6.6.1 release or later. For more information, see Managing a VM (AHV) on page 117.

Procedure

To check the Generation UUID and BIOS UUID of a guest VM, perform the following steps:

1. Log on to any CVM in the cluster using SSH.
2. Retrieve the guest VM details using the following command:

   ```
   nutanix@CVM ~ $ acli vm.get VM_Name
   ```

   Replace *VM_Name* with the guest VM name at your site.

   Observe the following log attributes to check the BIOS UUID and VM Generation UUID:

   bios_uuid: "cba7dc40-a45f-4823-8a8d-7b2e7119be64"

   generation_uuid: "0304dbc1-b1e0-452a-a104-ee2100d21c10"

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1533

Automatic Cluster Selection for VM Placement

Automatic cluster selection in Prism Central (PC) enables you to place guest VMs on a system-selected cluster without manually selecting the cluster for guest VM placement. The system intelligently performs load balancing to identify the target cluster where sufficient resources are available for the functioning of the guest VM and places the guest VM on it.

> **Note:** Automatic cluster selection performs load balancing only during the initial VM deployment, and Acropolis Dynamic Scheduling (ADS) then manages individual host load within the cluster. For more information on ADS, see Acropolis Dynamic Scheduling in AHV on page 8.

For more information on how the system performs the load balancing with automatic cluster selection, see Sample Scenarios for Automatic Cluster Selection on page 240.

Supported Configuration Workflows for Automatic Cluster Selection

You can configure automatic cluster selection by using any of the following methods (workflows):

- Creating a VM from Prism Central. For more information, see Creating a VM through Prism Central (AHV) in *Prism Central Infrastructure Guide*.
- Deploying a VM from OVA. For more information, see Deploying an OVA as VM in *Prism Central Infrastructure Guide*.
- Creating a VM or deploying a VM from OVA using v3 API. For more information, see Nutanix Dev page.

> **Note:** The system also supports the existing functionality of manual cluster selection while creating a VM, deploying a VM using OVA, or deploying a VM using a VM template.

VM Policies with Automatic Cluster Selection

The automatic cluster selection function ensures that the VM is auto-placed only in one of the clusters that can satisfy the hardware requirements of the VM and the following policies that you define for VM functioning.

- Storage policies: The automatic cluster selection honors all aspects of storage policies, such as data replication (replication factor), data security (encryption), data reduction (compression), and QoS (IOPS or throughput throttling).
- Host affinity policies that you define using Prism Central, and VM-VM anti-affinity policy that you define using acli in Prism Element: For example, if the host affinity policy is configured for the VM with hosts in a single cluster or across clusters, the system considers the host affinity policy and appropriately places the VM only on the cluster that is aligned to the host affinity policy and the load balancing result.

  > **Note:** You can use the host affinity policies to restrict the VM auto-placement in the clusters that are designated for test workloads, licensed for specific workloads, in a specific location, or any other restrictions around where a workload can run.

- Image management policies: The automatic cluster selection honors the image placement policies.

For more information on VM Policies, see Policies in Infrastructure section in *Prism Central Infrastructure Guide*.

For more information on how the system considers the policies with automatic cluster selection, see Sample Scenarios for Automatic Cluster Selection on page 240.

Automatic Cluster Selection Interaction with Self-Service Projects

When a project is specified during VM deployment, the automatic cluster selection considers the cluster scope of the project and quota defined in Nutanix Self-Service (formerly Nutanix Calm) while placing the VMs in the cluster. The system places the VMs only in the clusters that can offer the vCPU, memory, and disk requirements to the VM within the defined quota limits.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1534

For more information, see the Setting Up Quota Defaults section in the *Self-Service Administration and Operations Guide*.

Requirements for Automatic Cluster Selection

Ensure that you meet the following requirements before you use automatic cluster selection:

- All the intended clusters are on AOS 6.7 or later release.
- Prism central version should be upgraded to PC 2024.1 or later release.
- All the intended clusters must be hosted with AHV hypervisor. The ESXi hypervisor and mixed hypervisor clusters are not supported.
- If you use APIs directly, use only V3 APIs to configure VM auto-cluster scheduling. For information on v3 documentation, see Nutanix Dev page.
- Only a super admin user with permission to create a VM and management privileges for all intended clusters can configure automatic cluster selection. For more information, see the Controlling User Access (RBAC) section in the *Security Guide*.

Limitations of Automatic Cluster Selection

The following limitations apply to automatic cluster selection:

- While placing a VM based on an existing image with automatic cluster selection, the system always places the VM on one of the registered clusters where the VM image is present.
- Automatic cluster selection configuration for VM deployments using VM templates is not supported.
- Automatic cluster selection configuration for VMs with GPU specifications or advanced processor compatibility settings is not supported.

  For information on advanced processor compatibility, see Advanced Processor Compatibility in AHV on page 242.
- When you configure automatic cluster selection from Prism Central, you can select overlay subnets only. However, if you use API to configure automatic cluster selection, the system supports both VLAN and overlay subnet.

Sample Scenarios for Automatic Cluster Selection

Assumption

A sample Prism Central deployment with the following specifications:

- Total number of clusters registered with Prism Central: 4
- Cluster Specifications:

Cluster Name	Cluster A	Cluster B	Cluster C
Number of Nodes	5	3	1
Aggregate Memory Capacity	600 GB	753 GB	62 GB
Aggregate CPU capacity	100	100	100
Storage	RF3 capable	RF2 capable	-
The total capacity of all clusters is: 600 +753 + 62 + 450 = 1865 GB			

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1535

- Image placement policies with multiple images placed across clusters
- Host affinity policies with hosts across clusters

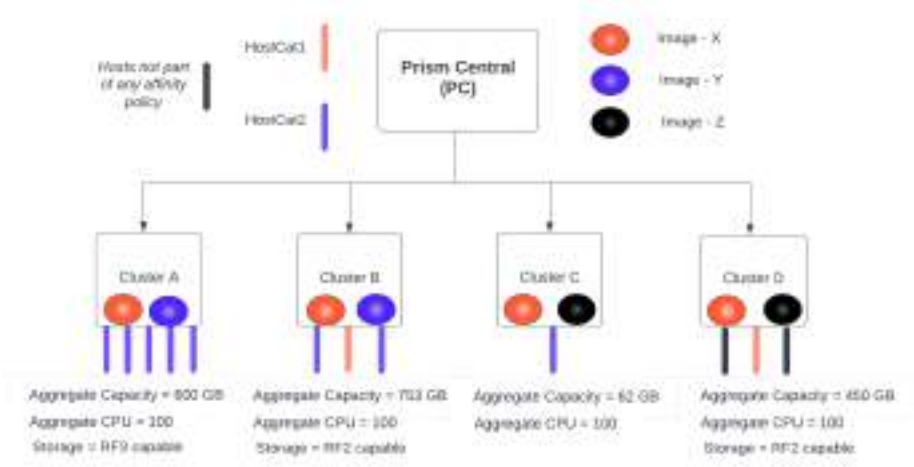


Figure 39: Sample Prism Central Deployment with Automatic Cluster Selection

Scenario 1

Placement of VMs when Image placement, host affinity, and storage policies are defined for the VM.

Create a VM		**Configured Policies at the Site**		
Image Used	**Configured Host Category for Host Affinity**	**Image placement**	**Host Affinity**	**Storage**
X	HostCat1	X image in Cluster A, Cluster B, Cluster C, and Cluster D Y image in Cluster A and Cluster B Z image in Cluster C and Cluster D	HostCat1 with hosts used across Cluster B and Cluster D HostCat2 with hosts used across Cluster A, Cluster B, and Cluster C	RF2 configu
X	HostCat2			
Y	HostCat1			
Y	HostCat2			
Z	HostCat1			
Z	HostCat2			

Scenario 2

Load balancing with automatic cluster selection with image placement policies consideration.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1536

Total VMs created using X image	Image Placement Policy Configured	VM approximate Distribution Count	
		Cluster A	Cluster B
100	X image in Cluster A, Cluster B, Cluster C, and Cluster D	32	41

Advanced Processor Compatibility in AHV

Acropolis, by default, automatically assigns a CPU generation to all the guest VMs. The automatically assigned CPU generation represents the highest subset of CPU features available on all nodes in the PE cluster.

> **Note:** The automatically assigned CPU generation name might change when you add a node from a different CPU generation to a cluster. A power cycle may be required to ensure VM mobility for ADS and maintenance scenarios. The system provides a notification when a power cycle is required for individual VMs after the cluster expansion operation.

You can migrate a guest VM to a destination cluster only if the CPU capabilities of the guest VM are present in the destination cluster.

AHV provides an advanced processor compatibility feature that enables you to customize the CPU capabilities for the guest VMs. You can associate the required CPU capabilities (CPU generation name) to the guest VM from the supported CPU capabilities presented by the cluster and can enhance the ability of the VM to migrate between nodes or clusters with different CPU generations. For example, you can successfully migrate the guest VMs from the source cluster with higher CPU capabilities to the destination cluster with lower CPU capabilities.

This feature also provides the following additional benefits:

- Provides a distinct set of CPU features to any guest VM, irrespective of changes in the AHV version. This prevents the guest VM from being exposed to advanced CPU features with which it might not function correctly.
- Associate a distinct CPU family with a guest VM. This helps you to configure guest VMs as requiring specific CPU capabilities requirements. For example, the guest VM might require AES-NI to mitigate timing-based attacks against cryptographic algorithms or to configure a guest VM with Windows 11 to boot on Skylake CPUs only.
- Reduces the number of guest VMs in the cluster that require a power cycle when you add a node with a different CPU generation to the cluster during cluster expansion, which changes the supported CPU generations of the cluster.

The guest VMs with advanced processor compatibility enabled might be configured to use a CPU generation that is supported on the expanded cluster and, hence, does not require a restart after cluster expansion. However, the guest VMs that use the automatically assigned CPU generation might require a restart.

You can select the CPU generation based on the considerations required at your site:

- Select the oldest CPU generation to maximize the cross-cluster live migration (CCLM) capability of the guest VM. For example, you can select Sandybridge on Intel and Naples on AMD processors.
- Select the latest CPU generation to maximize the performance of the guest VM with less consideration for cross-cluster live migration (CCLM) capability.

> **Note:**
>
> - By default, Acropolis selects the CPU generation, which is compatible with a wide range of hardware when you enable advanced processor compatibility for the guest VM. For more information, see Creating a VM through Prism Central (AHV) or Updating a VM through Prism Central (AHV) in the *Prism Central Infrastructure Guide*.
> - Acropolis only allows the selection of a CPU generation, which is supported by all nodes in the cluster.
> - The choice of CPU generation with advanced processor compatibility varies between CPU vendors. For example, with AMD CPU, the system provides you the option to select either Naples or Rome, but with

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1537

Intel CPU, the system provides you the option to select Sandybridge, Ivybridge, Haswell, Broadwell, Skylake, Cascadelake, or Icelake. For more information, refer to the CPU manufacturer documentation.

- The list of CPU generation names available when you enable advanced processor compatibility, depends on the cluster (PE registered with Prism Central) you select to host the guest VM during the VM creation workflow. If the cluster that you select uses Intel CPU, the options for CPU generation name selection show only the supported Intel CPU generation names.
- For successful cross-cluster VM migration, the destination cluster must have all the CPU capabilities that are available with the guest VMs in the source cluster after advanced processor compatibility is applied to them.
- The CPU generation that you directly associate with the guest VM using advanced processor compatibility persists after the VM power cycle, VM migration, or VM restart in a high-availability setup. Acropolis does not update the CPU generation associated with the guest VM, even if the destination cluster supports a higher CPU generation level.

Using Prism Central, you can change the automatically assigned CPU family (CPU generation name) to any of the cluster-supported CPU families. For more information, see Supported Configuration Workflows for Advanced Processor Compatibility on page 244.

If advanced processor compatibility is not enabled, and no CPU generation name is associated with the guest VM, the Acropolis performs the following actions:

- Automatically selects the most recent CPU generation supported on the cluster each time the VM is powered on and provides those CPU capabilities to the guest VM to maximize the system performance.
- Permits live migration of the guest VM to any cluster that can support the automatically selected CPU generation.

For information on the supported CPU families and the CPU capabilities exposed to the guest, see Supported CPU Generation Names for Advanced Processor Compatibility on page 244.

Requirements for Advanced Processor Compatibility

Ensure that you meet the following prerequisites to enable Advanced processor compatibility:

- Upgrade the cluster to AOS 6.8 or later release.
- Host the cluster with AHV and upgrade to AHV 20230302.100173 or later release.
- Prism central version should be upgraded to PC 2024.1 or later release.

Limitations and Considerations of Advanced Processor Compatibility

The following limitations apply to advanced processor compatibility:

- Only AHV clusters are supported.
- During Disaster Recovery, the following behavior applies when advanced processor compatibility is enabled for the guest VM:
  - For the guest VM that is protected with an asynchronous or nearsync replication schedule, the advanced processor compatibility configuration of guest VMs is not restored from the recovery point on the destination cluster, and the guest VM can start on the destination cluster without the advanced processor compatibility configuration.
  - For the guest VM that is protected with a synchronous replication schedule, the advanced processor compatibility configuration of the guest VM is replicated to the destination cluster, and the Acropolis permits

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1538

the live migration only at the destination cluster that supports the directly assigned or automatically assigned CPU generation of the running guest VM.

> **Note:** In case of unplanned failover of the guest VMs replicated using synchronous replication, the guest VM might fail to start at the destination cluster if the destination cluster does not support the CPU capabilities (CPU generation name) associated with the guest VM. However, you can manually edit the advanced processor compatibility configuration of the guest VMs at the destination cluster according to the CPU capabilities of the destination cluster to start the guest VM.
>
> Nutanix recommends that you reduce the selected CPU generation to one supported by both source and destination clusters to avoid interruptions during unplanned failover of VMs using advanced processor compatibility.

- If you manually create a recovery point for the guest VM that has advanced processor compatibility enabled and attempt to either restore the guest VM or create a new VM using the same recovery point, the advanced processor compatibility configuration of the guest VM is not restored. To re-enable the advanced processor compatibility configuration for the guest VM, you must shut down the guest VM, reconfigure the advanced processor compatibility configuration, and start the guest VM again. For more information, see the Creating Recovery Points Manually (Out-of-Band Snapshots) section in the *Nutanix Disaster Recovery Guide*.
- When you trigger an on-demand cross-cluster live migration for the guest VM with advanced processor compatibility enabled, the Acropolis permits the live migration only at the destination cluster that supports the directly assigned or automatically assigned CPU generation of the running guest VM.
- You can migrate the guest VMs only to the clusters that can provide all features of the CPU generation name associated with the guest VMs through advanced processor compatibility.
- You cannot enable the advanced processor compatibility functionality for guest VMs configured to use CPU pass-through.
- You cannot configure CPU pass-through for the guest VMs for which the advanced processor compatibility functionality is enabled.
- Advanced processor compatibility is not currently enabled for use with VM Templates or with automatic cluster selection.

  For information on VM templates, see VM Template Management section in *Prism Central Infrastructure Guide*.

  For information on automatic cluster selection, see Automatic Cluster Selection for VM Placement on page 239.

Supported Configuration Workflows for Advanced Processor Compatibility

You can configure advanced processor compatibility for a VM using the following workflows:

- Creating a VM from Prism Central. For more information, see Creating a VM through Prism Central (AHV) in *Prism Central Infrastructure Guide*.
- Updating a VM from Prism Central. For more information, see Updating a VM through Prism Central (AHV) in *Prism Central Infrastructure Guide*.

> **Note:** You must shut down the guest VM to configure advanced processor compatibility.

Supported CPU Generation Names for Advanced Processor Compatibility

This section provides information about the supported CPU generation names and their capabilities for advanced processor compatibility.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1539

Intel CPU

The following table provides information about the supported Intel CPU generation name and their capabilities for advanced processor compatibility.

CPU Generation Name	Available Features
Intel Sandy Bridge	This CPU generation exposes the following capabilities: • Base features of Intel Sandy Bridge CPUs, including AVX and SSE. • Support of additional nested virtualization using Intel VMX for VMs with th • Hyper-V enlightenments for Microsoft Windows VMs that include STIMER SPINLOCK, TLBFLUSH, and IPI. **Note:** This CPU generation is the maximum Intel CPU generation supported by
Intel Ivy Bridge	This CPU generation exposes the following capabilities: • All CPU features from Intel Sandy Bridge plus additional CPU features that • Additional CPU features for nested virtualization that include APICV-VID,
Intel Haswell	This CPU generation exposes the following capabilities: • All CPU features from Intel Ivy Bridge plus additional CPU features that inc MOVBE. • Additional CPU features for nested virtualization that include EPTP-SWITC VMEXIT-FIELDS, and SHADOW-VMCS.
Intel Broadwell	This CPU generation exposes the following capabilities: • All CPU features from Intel Haswell plus additional CPU features that inclu SSBD. • Additional CPU features for nested virtualization that include PML and RDS **Note:** This is the default Intel CPU generation when no CPU generation name is sufficient to run most guests (For Windows 11, see Intel Skylake) and has migrati
Intel Skylake	This CPU generation exposes the following capabilities: • All CPU features from Intel Broadwell plus additional CPU features that inc CLWB, PDPE1GB, AVX512BW, AVX512VL, AVX512CD, and XSAVES • Additional CPU features for nested virtualization that include XSAVES and **Note:** This CPU generation is the minimum Intel CPU generation supported by V
Intel Cascade Lake	This CPU generation exposes all CPU features from Intel Skylake plus a CAPABILITIES, SKIP-L1DFL-VMENTRY, IBRS-ALL, MDS-NO, RDCTL-

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1540

CPU Generation Name	Available Features
Intel Ice Lake	This CPU generation exposes the following capabilities: • All CPU features from Intel Cascade Lake plus additional CPU features that NO, LA57, AVX512BITALG, GFNI, PSCHANGE-MC-NO, WBNOINVD AVX512IFMA, RDPID, and FSRM. • Additional CPU features for nested virtualization that include PAGE-WALK
Intel Sapphire Rapids	This CPU generation exposes all the CPU features from Intel Ice Lake p INT8, AMX-TILE, AVX512-FP16, AVX512-BF16, AVX-VNNI, MOVDIRI, REP MOVSB, fast short REP STOSB, fast short REP CMPSB, fast shor

AMD CPU

The following table provides information about the supported AMD CPU generation names and their capabilities for advanced processor compatibility.

CPU Generation Name	Available Features
AMD Naples	This CPU generation exposes the following capabilities: • Base features of AMD Naples CPUs that include AVX, SSE, and PREFET • Additional nested virtualization using AMD SVM for VMs with Credentia • Hyper-V enlightenments for Microsoft Windows VMs that include STIME SPINLOCK, TLBFLUSH, IPI **Note:** This is the default AMD CPU generation when no CPU generation name to run most guests (For Windows 11, see AMD Rome) and has migration compa
AMD Rome	This CPU generation exposes all CPU features from AMD Naples plus UMIP, PERFCTR_CORE, AMD-STIBP, IBPB, WBNOINVD, RDPID, XS **Note:** This CPU generation is the minimum AMD CPU generation supported b

PCIe Passthrough for Guest VMs

This section explains PCIe passthrough feature.

AHV supports Peripheral Component Interconnect Express (PCIe) passthrough for guest VMs to directly access and manage PCIe hardware devices connected to the host, bypassing the hypervisor layer. When you configure PCIe passthrough for a guest VM, the PCIe hardware devices appear to be physically attached to the guest operating system. This allows guest operating system drivers to use the device hardware directly from the host.

Note: Only v4 APIs is supported for PCIe passthrough feature.

Limitations

PCIe passthrough has the following limitations:

- Disaster Recovery is not supported.
- Live migration of VMs with a PCIe device attached is not supported.
- Hot-plug of a PCIe device is not supported.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1541

Assigning a PCIe Device to a Guest VM

You can assign a PCIe device to a guest VM using aCLI.

Before you begin

You must power off the guest VM before you assign the PCIe device. Perform a graceful shutdown from the operating system of the guest VM.

About this task

To assign the PCIe device to the guest VM on the AHV host, follow these steps:

Procedure

1. Log on to any Controller VM (CVM) in the cluster with SSH.

   ```
   $ ssh nutanix@cvm_ip_address
   ```

   Replace `cvm_ip_address` with the IP address of the CVM.

2. Obtain the group UUID of the PCIe device connected to the host in the cluster:

   ```
   nutanix@cvm$ acli host.get host_ip | grep "pcie_devices"
   ```

   Replace `host_ip` with the host IP address.

   Example:

   ```
   nutanix@cvm$ acli host.get 10.45.137.209 | grep "pcie_devices"
   ```

   Output similar to the following displays:

   ```
   pcie_devices {
               groups {
                 migratable: False
                 uuid: "11a0a5e5-6733-47c3-9a2d-8cd1c7d01e2c"
               }
     uuid: "11a0a5e5-6733-47c3-9a2d-8cd1c7d01e2c"
   }
   ```

3. Assign the PCIe device to the guest VM:

   ```
   nutanix@cvm$ acli vm.assign_pcie_device vm_name group_uuid=group_uuid
   ```

   Replace:

   `vm_name` with the name of the guest VM.

   `group_uuid` with the group UUID of the PCIe device.

   Example:

   ```
   nutanix@cvm$ acli vm.assign_pcie_device vm2
    group_uuid=11a0a5e5-6733-47c3-9a2d-8cd1c7d01e2c
   ```

   Output similar to the following displays:

   ```
   VmUpdate: complete
   ```

4. Power on the guest VM:

   ```
   nutanix@cvm$ acli vm.on vm_name
   ```

   Replace `vm_name` with the name of the guest VM.

Deassigning a PCIe Device from a Guest VM

You can deassign a PCIe device from a guest VM using aCLI.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1542

Before you begin

You must power off the guest VM before you deassign the PCIe device. Perform a graceful shutdown from the operating system of the guest VM.

About this task

To deassign the PCIe device attached to the guest VM on the AHV host, follow these steps:

Procedure

1. Log on to any Controller VM (CVM) in the cluster with SSH:

   ```
   $ ssh nutanix@cvm_ip_address
   ```

   Replace `cvm_ip_address` with the IP address of the CVM.

2. Obtain the config UUID of the PCIe device to be deassigned:

   ```
   nutanix@cvm$ acli vm.list_pcie_devices vm_name
   ```

   Replace `vm_name` with the name of the guest VM.

   Example:

   ```
   nutanix@cvm$ acli vm.list_pcie_devices vm2
   ```

   Output similar to the following displays:

   ```
   Group UUID                                Config UUID
   11a0a5e5-6733-47c3-9a2d-8cd1c7d01e2c      8588ec27-0082-4db5-ae0d-b0ecdb2aef26
   ```

3. Deassign the PCIe device from the guest VM:

   ```
   nutanix@cvm$ acli vm.deassign_pcie_device vm_name config_uuid=config_uuid
   ```

   Replace:

   `vm_name` with the name of the guest VM.

   `config_uuid` with the config UUID.

   Example:

   ```
   nutanix@cvm$ acli vm.deassign_pcie_device vm2 config_uuid=8603d9e4-1686-4178-
   b7ff-360668dddab7
   ```

   Output similar to the following displays:

   ```
   VmUpdate: complete
   ```

4. Power on the guest VM:

   ```
   nutanix@cvm$ acli vm.on vm_name
   ```

   Replace `vm_name` with the name of the guest VM.

Listing PCIe Devices Attached to a Guest VM

You can list the PCIe devices attached to a guest VM using aCLI.

About this task

To list PCIe devices attached to the guest VM on the AHV host, follow these steps:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1543

Procedure

1. Log on to any Controller VM (CVM) in the cluster with SSH:

   ```
   $ ssh nutanix@cvm_ip_address
   ```

   Replace *cvm_ip_address* with the IP address of CVM.

2. List the PCIe devices attached to the guest VM:

   ```
   nutanix@cvm$ acli vm.list_pcie_devices vm_name
   ```

   Replace *vm_name* with the name of the guest VM.

   Example:

   ```
   nutanix@cvm$ acli vm.list_pcie_devices vm2
   ```

   Output similar to the following displays:

   ```
   Group UUID                                Config UUID
   11a0a5e5-6733-47c3-9a2d-8cd1c7d01e2c      8588ec27-0082-4db5-ae0d-b0ecdb2aef26
   00000000-0000-0000-0000-000000000011      00000000-0000-0000-0000-000000000011
   ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1544

VM TEMPLATE MANAGEMENT

In Prism Central, you can create VM templates to manage the golden image of a VM. A VM template can be considered as a master copy of a virtual machine. It captures the virtual machine configuration and the contents of the VM including the guest operating system, and the applications installed on the VM. You can use this template to deploy multiple VMs across clusters.

> **Note:** You can create or manage a VM template only as an admin user or a user with admin privileges.

Limitations of VM Template Feature

The current implementation of the VM template feature has the following limitations:

- You cannot create a VM template if any of the following conditions is applicable at your site:
  - VM is not on AHV.
  - VM is an agent or a PC VM.
  - Any volume group is attached to the VM.
  - VM is undergoing vDisk migration.
  - VM has disks located on containers with replication factor 1.
  - VM is protected by PD-based DR.
- VM templates do not copy the following attributes from the source VMs:
  - Host affinity attributes
  - HA priority attributes
  - Nutanix Guest Tools (NGT) installation
  - Quality of service (QoS) configuration

  You must reconfigure the above-listed attributes at the deployed VMs.
- VM Template does not protect the underlying VM recovery point from deletion by a user having delete permission. VM Template deployment fails if you delete the associated VM recovery point.

Creating a VM Template

This section describes how to create a VM template in Prism Central.

About this task

To create a VM template, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar information in the *Prism Central Infrastructure Guide*.
   The system displays the **List** tab as default

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1545

3. In **List** tab, select the VM to create a VM template.

   Note: Before you select a VM to create a VM template, ensure that the VM is powered off.

4. In the **Actions** dropdown menu, select **Create VM Template**.

   You can also click **Create VM Template** in the **Summary** page of an individual VM. For information about how to access the **Summary** page of an individual VM, see VM Details View information in *Prism Central Infrastructure Guide*.

   The system displays the **Create template from VM** window.

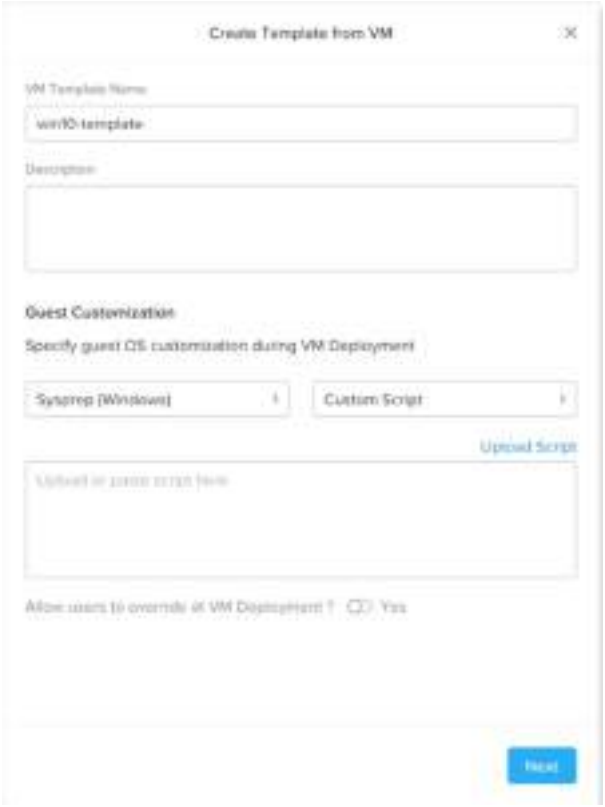


Figure 40: Create Template from VM window

5. In the **Create Template from VM** window, enter the following information:

   a. **Name** - Name of the VM Template.

   b. **Description** - Description for the VM template. Description is an optional field.

   c. For the **Guest Customization** fields, select the following options for guest operating system (OS) for the VMs that you deploy using this VM template:

      - In the **Script Type** field, select **Sysprep (Windows)** to customize the Windows OS, and **Cloud-init (Linux)** to customize the Linux OS.

        Note: If you select **No Customization** at the time of creating the template and allow the users to override the guest customization settings using **Allow users to override at VM Deployment?** toggle field, it

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1546

gives the maximum customization control to the users. In this case, the users can customize the script type and the configuration method.

- In the **Configuration Method** field, for each of these script types selected in **Script Type** field, select either upload a custom script or opt for a guided setup in the field.

  Note:

  - If you select **Custom Script**, you can either upload a script to customize the guest OS of the VMs, or you can copy-paste the script in the text box.
  - If you select **Guided Script** , enter the following information:
    - **Authentication Type**: Select one of the radio button to set the authentication type:
      - **Password**: Set a username and password for the user who uses this template to deploy the VM.
      - **SSH Key** [Cloudinit (Linux) only]: Set the SSH key for the user who use this template to deploy the VM.
    - **Locale**: Select the locale (language) from the dropdown list.
    - **Hostname**: Enter the hostname for the user who uses this template to deploy a VM
    - **License Key**: Enter the license key.

      Important: The information that you enter is used to customize the OS of the VMs that are deployed using this template.

Note: If you opt for **Guest Customization** setup with script (custom or guided script), ensure that the script is in a valid format. The system does not validate the guest customization scripts. In the script is not in valid format, the VM deployment might succeed but the guest customization script may not work as expected. You can observe the discrepancies (if any) only after the VM gets deployed.

d. Set the **Allow users to override at VM Deployment?** toggle field as per your requirement. This toggle field is used to enable or disable the override permission for guest customization settings.

- If this toggle field is:
  - *Enabled*: The system allows the users (who use this VM template to deploy VM) to modify the guest OS customization settings in VM template. The users can modify the settings only for the **Configuration Method** field. For example, the users can change the authentication information at the time of deploying a VM from VM template, or they can change from a guided setup to a custom script.
  - *Disabled*: The settings that are already provided in the VM template, can be used for VM deployment.

6. Click **Next**.

On the next page, you can review the template details.

The system prompts you to review the configuration details, resource details, network details, and management details.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1547

7. Click **Save** to save the inputs and create a VM template.

   The new template appears in the **Templates** page list.

   > **Note:** Once you create a VM template, the template metadata is available in Prism Central. The template data is stored as a VM recovery point and is co-located with the source VM. If you use the VM template to deploy a VM to another cluster, the recovery point is copied to the destination cluster before deployment.

Deploying VM from a Template

Before you begin

Ensure that the VM template is available. For information on how to create a VM template, see Creating a VM Template on page 250.

About this task

After you create a VM template, you can use the VM template to deploy any number of VMs across clusters.

To deploy a VM using a VM template, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute** > **Templates** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar information in *Prism Central Infrastructure Guide* .
3. Select the target VM template to deploy VMs using either of the following methods:

   - In the **Templates** page, select the target template checkbox, and click **Deploy VMs**. For more information about **Templates** page, see VM Template Summary View information in *Prism Central Infrastructure Guide*.
   - In the **Summary** page of an individual VM template, click **Deploy VMs**. For more information about **Summary** page of an individual VM template, see VM Template Details View information in *Prism Central Infrastructure Guide*.
   - In the **Versions** page of an individual VM template, select the target VM template version, and click **Deploy VMs**. For more information on **Versions** page of an individual VM template, see VM Template Details View information in *Prism Central Infrastructure Guide*.

     > **Note:** In the **Versions** page, you can select any active or non-active VM template version for VM deployment.

     > **Note:** By default, the active version of the VM template is used for VM deployment.

   The **Deploy VM from Template** window appears. By default, you see a **Quick Deploy** method. You can click**Advanced Deploy** to access the **Advanced Deploy** method in **Deploy VM from Template** window . In **Advanced Deploy** method, you can view and modify some VM properties and network settings.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1548

4. Deploy VM using either of the following deployment methods:

   - **Quick Deploy** method:

     The is an example showing the **Quick Deploy** method:

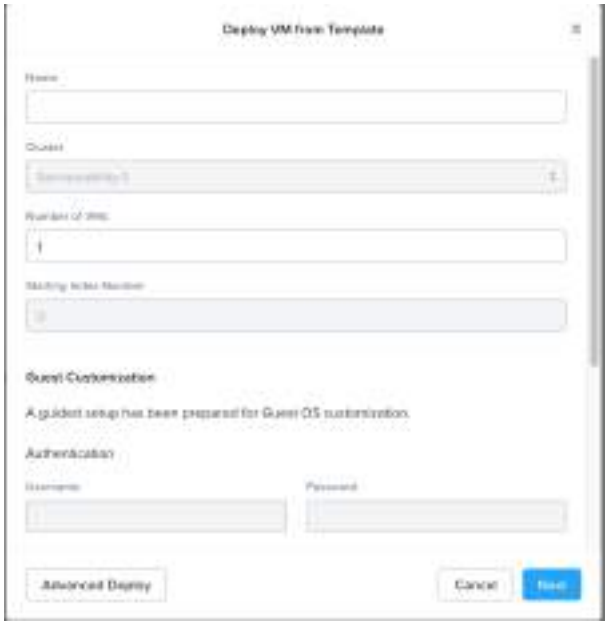


Figure 41: Deploy VM from VM Template using the Quick Deploy Method

1. Enter the following information:

   - **Name**: Enter a name for the VM.
   - **Cluster**: Select the cluster where you want to deploy the VM.
   - **Number of VMs**: Enter the number of VMs that you want to deploy.
   - **Starting Index Number**: Enter the starting index number for the VMs when you are deploying multiple VMs simultaneously. These index numbers are used in the VM names. For example, if you are deploying two VMs and specify the starting index number as 5, the VMs are named as *vm_name*-5 and *vm_name*-6.
   - **Guest Customization**: The template can have any one of the following options for guest OS customization:

     - **No Customization**
     - **Sysprep (Windows)**, or **Cloud-init (Linux)**. For **Sysprep (Windows)**, or **Cloud-init (Linux)**, you can choose to either upload a custom script or opt for a guided setup.

       Note: These fields are enabled for modification only if the VM template allows you to override its guest customization settings while deploying the VM. The **Allow users to override at VM Deployment?** toggle field is used to enable or disable the override for guest customization settings. For information on how to set this toggle field during VM template creation, see Creating

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1549

a VM Template on page 250. If the override permission for the guest OS customization is disabled, the settings that are already provided in the template can be used for VM deployment.

2. Click **Next** to verify the configuration details of the VMs to be deployed.
3. Click **Deploy** to deploy the VMs.

- **Advanced Deploy** method:

  The following is an example showing the **Advanced Deploy** method:

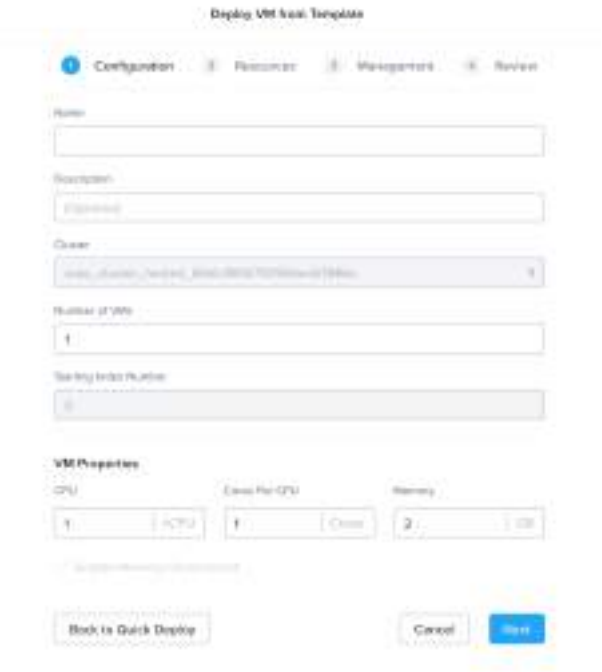


Figure 42: Deploy VM from VM Template using the Advanced Deploy Method

1. Enter the following information:

   - **Configuration**: Provide inputs for name and description (optional) of the VM, cluster where you want to deploy the VM, Number of VMs to be deployed, and starting index number (only if deploying multiple VMs). In this tab, you can also view and modify the VM properties such as CPU, core per CPU, and memory.
   - **Resources**: Review the configuration settings for the VM resources such as disks, networks, and boot configuration. Here, you can modify the network settings but cannot modify any other settings.
   - **Management**: The fields in this tab are enabled for modification only if the VM template allows you to override its guest customization settings while deploying the VM. The **Allow users to override at VM Deployment?** toggle field is used to enable or disable the override for guest customization settings. For information on how to set this toggle field during VM template creation, see Creating a

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1550

VM Template on page 250. If the override permission for the guest OS customization is disabled, the settings that are already provided in the template can be used for VM deployment.

If guest customization has been enabled, provide inputs for authentication type, username, password, locale, and Hostname.

> **Note:** Hostname of the VM is automatically generated based on the VM names that you provide. If you are deploying a single VM, you can override the automatic generation of the hostname by specifying a hostname. If you are deploying multiple VMs, you cannot override the automatic hostname generation.

- **Review**: Review the information displayed in this tab.

2. Click **Deploy** to deploy the VMs.

Managing a VM Template

About this task

After you create a VM template, you can perform the following actions to manage the VM Template:

- Update the guest OS of the source VM specified in the VM template
- Complete guest OS update
- Cancel guest OS update
- Update the configuration of the template to create a new VM template version
- Delete the VM template.

For information on how to create a VM template, see Creating a VM Template on page 250.

To manage a VM template, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute** > **Templates** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar information in *Prism Central Infrastructure Guide* .

Select the target VM template using either of the following methods:

- Select the target VM template checkbox in the **Templates** page. For more information on **Templates** page, see VM Template Summary View information in *Prism Central Infrastructure Guide*.
- Click the target template to view the **Summary** page of an individual VM template. For more information about **Summary** page of an individual VM template, see VM Template Details View information in *Prism Central Infrastructure Guide*.

3. Select the required action from the **Actions** dropdown menu:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1551

> **Note:** The available actions appear in bold and the unavailable actions are greyed out. The available actions depend on the current state of the template and user permissions.

The following actions are available in **Actions** drop down menu:

- **Update Guest OS**

  To update the guest OS in a VM Template, perform the following steps:

  1. Select the target VM template version on which the guest OS is to be updated in **Select a version to Update** window, and click **Proceed**.

     > **Note:** By default the active version of the VM Template is selected for VM Template update, however the system provides you an option to select the VM Template version on which the guest OS is to be updated.

  2. Review the information displayed in the **Update Guest OS** window, and click **Proceed**.

     At this stage, the system deploys a temporary VM from the selected VM template version, and provides you an option to access the VM. You can also access the new VM from VMs **List** tab. For information on VMs **List** tab, see VMs Summary View information in *Prism Central Infrastructure Guide*.

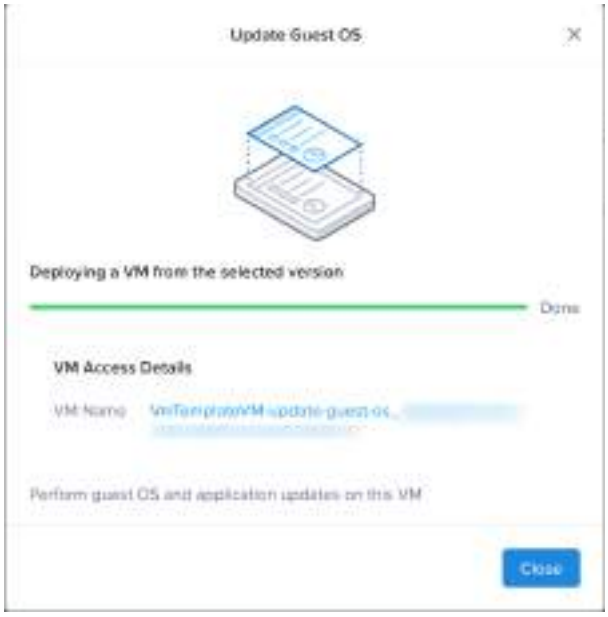


Figure 43: Update Guest OS

  3. Start the temporary VM, log on to the VM, and update the guest OS of the temporary VM. For information on how to update a VM, see Managing a VM through Prism Central (AHV) information in *Prism Central Infrastructure Guide*.
  4. Complete the guest OS update using the **Complete Guest OS Update** option from the **Actions** dropdown menu.

- **Complete Guest OS Update** to complete the process initiated for guest OS update. You must select this option only after successful update of the guest OS of the temporary VM. If you have opted for guest customization for

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1552

the deployed VMs, ensure to run Sysprep (for Windows) or Cloud-init (for Linux) before completing the guest OS update.

> **Note:** At this stage, the system prompts you to create a new version of the VM Template with updated guest OS. Specify the details for the new version, and click **Complete Update**.

The temporary VM automatically gets deleted after completion of the guest OS upgrade process.

- **Cancel Guest OS Update** to cancel the process initiated for guest OS update.

  The temporary VM automatically gets deleted after cancellation of the guest OS upgrade process.

- **Update Configuration** to modify the VM template configuration. In **Select a version to Update** window, select the VM template version that you want to modify, and create a version on top of it.

  Perform the following steps to update the VM template configuration in **Update Template Configuration** window:

Figure 44: Update Template Configuration

1. In the **Configuration** step, view the name of the base version that you want to update, change notes for that version, cluster name, VM properties (CPU, cores per CPU), and memory). In this section, you can modify only VM properties.
2. In the **Resources** step, view the information about disks, networks, and boot configuration. In this section, you can modify only network resources.
3. In the **Management** step, modify the guest customization settings.
4. In the **Review** step, review and modify the configuration settings that you are allowed to modify. You must provide a name and change notes for the new version. You can also choose to set this new version as active version.

   > **Note:** An active version is the version of the template gets deployed by default when you click **Deploy VMs** after VM template configuration update.

5. Click **Save** to save the settings and create a new VM template version.

- **Delete Template** to delete a template. The system prompts you to confirm the delete action. Click **OK** to delete the VM template.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1553

4. To only manage a VM template version:

   a. Select the VM template version from the **Versions** page. For information on how to access the **Versions** page of an individual VM template, see VM Template Details View information in *Prism Central Infrastructure Guide*.

   b. Select either of the following options from the **Actions** dropdown menu:

- **Set as Active** to make the selected VM template version as the active version.
- **Delete** to delete the selected VM template version.

> **Note:** You cannot delete the active version of a VM template.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1554

COPYRIGHT

Copyright 2025 Nutanix, Inc.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Nutanix and the Nutanix logo are registered trademarks of Nutanix, Inc. in the United States and/or other jurisdictions. All other brand and product names mentioned herein are for identification purposes only and may be trademarks of their respective holders.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1555

v5.9 | June 2024 | BP-2005

SOLUTIONS DOCUMENT

Data Protection and Disaster Recovery Best Practices

NUTANIX

Legal

© 2024 Nutanix, Inc. All rights reserved. Nutanix, the Enterprise Cloud Platform, the Nutanix logo and the other Nutanix products, features, and/or programs mentioned herein are registered trademarks or trademarks of Nutanix, Inc. in the United States and other countries. All other brand and product names mentioned herein are for identification purposes only and are the property of their respective holder(s), and Nutanix may not be associated with, or sponsored or endorsed by such holder(s). This document is provided for informational purposes only and is presented "as is" with no warranties of any kind, whether implied, statutory or otherwise.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

Contents

1. Executive Summary 6
Document Version History 7

2. Web-Scale Data Protection 9

3. Deployment Overview 11
Native Nutanix Snapshots 11
Two-Way Mirroring 11
Many-to-One 12
To the Cloud 13
Single-Node Backup 14
Disaster Recovery Orchestration 15

4. Local Backup with Snapshots 16
Crash-Consistent vs. Application-Consistent Snapshots 16

5. Protection Domains 20
Consistency Groups 20

6. Backup and Disaster Recovery on Remote Sites 22
Remote Site Setup 22
Scheduling Full Snapshots and Asynchronous Replication 25
Scheduling Lightweight Snapshots and NearSync 27
Cross-Hypervisor Disaster Recovery 28
Single-Node Backup Target 28
Cloud Connect 29

7. Disaster Recovery Orchestration 30
Required Infrastructure for Disaster Recovery Orchestration 30
Availability Zones 30
Protection Policies 31
Recovery Plans 33

8. Sizing Space 36
Full Local Snapshots 36
Asynchronous Replication 37
Lightweight Snapshots 37
NearSync 39

9. Bandwidth 40
Seeding 40

10. Failover: Migrate vs. Activate 42
Protection Domain Cleanup 43

11. Self-Service File Restore 44

12. Third-Party Backup Products 45
Backups with Replication 45

13. Conclusion 46

14. Appendix 47
General Best Practices 47
Nutanix Native VSS Snapshots 47
Hyper-V VSS Provider 47
Protection Domains 48
Consistency Groups 48
Disaster Recovery and Backup 48
Remote Sites 49
Remote Containers 49
Network Mapping 49
Scheduling 49
Cross-Hypervisor Disaster Recovery 50
Disaster Recovery Orchestration 50
Availability Zones 50
Protection Policies 50
Cross-Hypervisor Support with ESXi for Protection Policies 51
Recovery Plans 51
Network Mapping 51
Nutanix DRaaS Hypervisor Support 52

Nutanix DRaaS VM Configuration Restrictions..... 52
Single-Node Backup.....52
Cloud Connect.....52
Sizing..... 53
Bandwidth..... 53
File-Level Restore..... 53

About Nutanix.....55

List of Figures.....56

1. Executive Summary

The Nutanix Cloud Platform can deliver storage, compute, and virtualization services for any application. Designed for supporting multiple virtualized environments, including Nutanix AHV, VMware ESXi, and Microsoft Hyper-V, Nutanix invisible infrastructure provides many ways to achieve your recovery point objectives (RPOs).

Enterprises are increasingly vulnerable to data loss and downtime during disasters, as they rely on virtualized applications and infrastructure that their legacy data protection and disaster recovery solutions can no longer adequately support. This best practice guide provides the optimal configuration for achieving data protection using the native Nutanix disaster recovery capabilities and the disaster recovery orchestration features available both on-premises, in Nutanix DRaaS, and in public cloud providers like Amazon Web Services (AWS).

Whatever your use case, you can protect your applications with ease. Nutanix Prism facilitates management to configure the shortest recovery time objectives (RTOs) possible, so that you can build complex disaster recovery workflows at a moment's notice. With Prism Central, you can apply protection policies across all your managed clusters. Based on your RPO, you can activate recovery plans to validate, test, migrate, and fail over seamlessly. Recovery plans can protect availability zones both on-premises and hosted in Nutanix DRaaS.

As application requirements change and grow, Nutanix can adapt to business needs. Nutanix is uniquely positioned to protect and operate in environments with minimal administrative effort because of its web-scale architecture and commitment to enterprise cloud operations.

This document provides best practice guidance for implementing data protection solutions on Nutanix servers running AOS 6.5 and covers the following topics:

- Scalable metadata
- Backup
- Crash-consistent versus application-consistent snapshots

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1561

- Protection domains
- Protection policies
- Recovery plans
- Scheduling snapshots and asynchronous replication
- Sizing disk space for local snapshots and replication
- Scheduling lightweight snapshots (LWS) and NearSync replication
- Sizing disk space for LWS and NearSync replication
- Determining bandwidth requirements
- File-level restore

Document Version History

Version Number	Published	Notes
1.0	December 2014	Original publication.
2.0	March 2016	Updated best practices throughout.
2.1	June 2016	Updated the Backup and Disaster Recovery on Remote Sites section.
2.2	July 2016	Updated bandwidth sizing information.
2.3	December 2016	Updated for AOS 5.0.
2.4	May 2017	Updated information on sizing SSD space on a remote cluster.
3.0	December 2017	Updated for AOS 5.5.
3.1	September 2018	Updated the Nutanix overview and the Remote Site Setup section.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1562

Version Number	Published	Notes
4.0	December 2018	Updated for AOS 5.10 and Xi Leap.
4.1	February 2019	Updated the Sizing Space section and Leap product details.
4.2	August 2019	Updated for AOS 5.11.
4.3	October 2019	Updated for AOS 5.11.1 and Nutanix Files support for NearSync replication.
5.0	May 2020	Updated for AOS 5.17.
5.1	September 2020	Updated for AOS 5.18.
5.2	December 2020	Updated for AOS 5.19 and Leap multisite replication.
5.3	March 2021	Refreshed content.
5.4	February 2022	Updated the Third-Party Backup Products section.
5.5	May 2022	Updated product names and references to configuration maximums throughout.
5.6	August 2022	Updated the Third-Party Backup Products section.
5.7	October 2023	Removed the PowerShell Scripts section.
5.8	May 2024	Updated the Executive Summary section.
5.9	June 2024	Updated the Disaster Recovery Orchestration and Nutanix VSS Support with Nutanix Guest Tools sections.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1563

2. Web-Scale Data Protection

One of the key architectural differentiators for Nutanix is the ability to scale. Nutanix isn't bound by the same limitations as dual-controller architectures or federations relying on special hardware like NVRAM or custom ASICs for performance. When it comes to snapshots and disaster recovery, scaling metadata is a key part of delivering performance while ensuring availability and reliability. Each Nutanix node is responsible for a subset of the overall platform's metadata. All nodes in the cluster serve and manipulate metadata entirely through software, eliminating traditional bottlenecks.

Because each node has its own virtual storage controller and access to local metadata, replication scales with the system. Every node participates in replication to reduce hotspots throughout the cluster.

Nutanix uses two different forms of snapshots: full snapshots for asynchronous replication (when the RPO is 60 minutes or greater) and lightweight snapshots (LWS) for NearSync replication (when the RPO is between 1 minute and 15 minutes). Full snapshots keep system resource usage low when you use many snapshots over an extended period. The LWS feature reduces metadata management overhead and increases storage performance by decreasing the high number of storage I/O operations that long snapshot chains can cause.

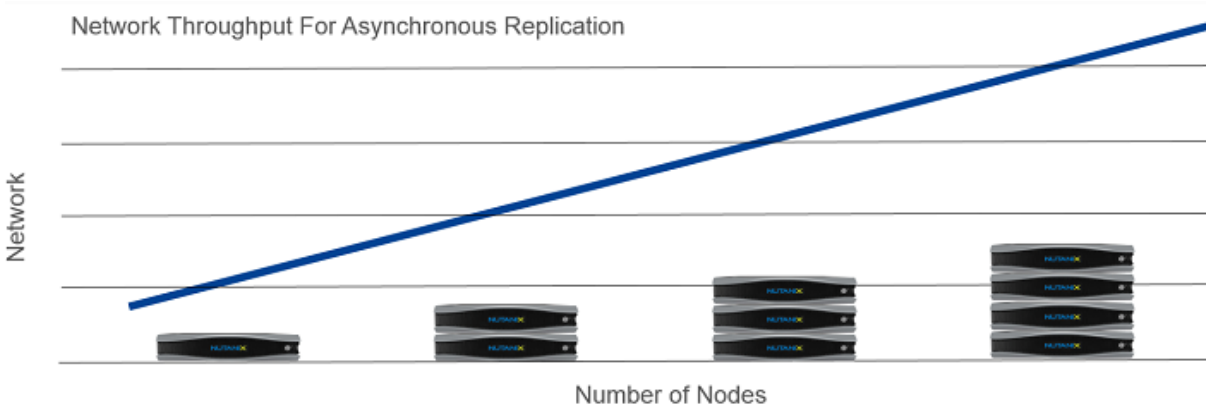


Figure 1: Scalable Replication

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1564

In asynchronous replication, every node can replicate four files, up to an aggregate of 100 MBps at one time. Thus, in a four-node configuration, the cluster can replicate 400 MBps or 3.2 Gbps. As you grow the cluster, the virtual storage controllers keep replication traffic distributed. In many-to-one deployments, as when remote branch offices communicate with a main datacenter, the main datacenter can use all its available resources to handle the increased replication load from the branch offices. When the main site is scalable and reliable, administrators don't have multiple replication targets to maintain, monitor, and manage. You can protect both VMs and volume groups with asynchronous replication.

NearSync offers unbound throughput. All writes go to SSD, so to avoid filling the performance tier, AOS automatically allocates 7 percent of it for NearSync. NearSync, which covers both VMs and volume groups, is supported for bidirectional replication between two clusters.

Nutanix also provides cross-hypervisor disaster recovery natively with asynchronous replication. Existing vSphere clusters can target AHV-based clusters as their disaster recovery and backup targets. With VM mobility, you can place your workloads on the platform that best meets their needs.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1565

3. Deployment Overview

Nutanix meets real-world requirements with native backup and replication infrastructure and management features that support a wide variety of enterprise topologies.

Native Nutanix Snapshots

Per-VM or per-volume group snapshots enable instant recovery. Depending on the workload and associated SLAs, you can tune the snapshot schedule and retention periods to meet RPOs. With the intuitive snapshot browser, you can perform restore and cloning operations instantly on the local cluster.

Two-Way Mirroring

The ability to mirror VM and volume group replication between multiple sites is necessary in environments where all sites must support active traffic. Consider a two-site example. Site B is the data protection target for selected workloads running on site A. At the same time, site A serves as the target for designated workloads running on site B. While asynchronous replication is supported for all workflows listed in this section, two-way mirroring is the only supported topology for NearSync.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1566

Figure 2: Two-Way Mirroring

Many-to-One

In many-to-one or hub-and-spoke architectures, you can replicate workloads running on sites A and B to a central site C. Centralizing replication to a single site can improve operational efficiency for geographically dispersed environments. Remote and branch office (ROBO) use cases are a classic many-to-one architecture.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1567

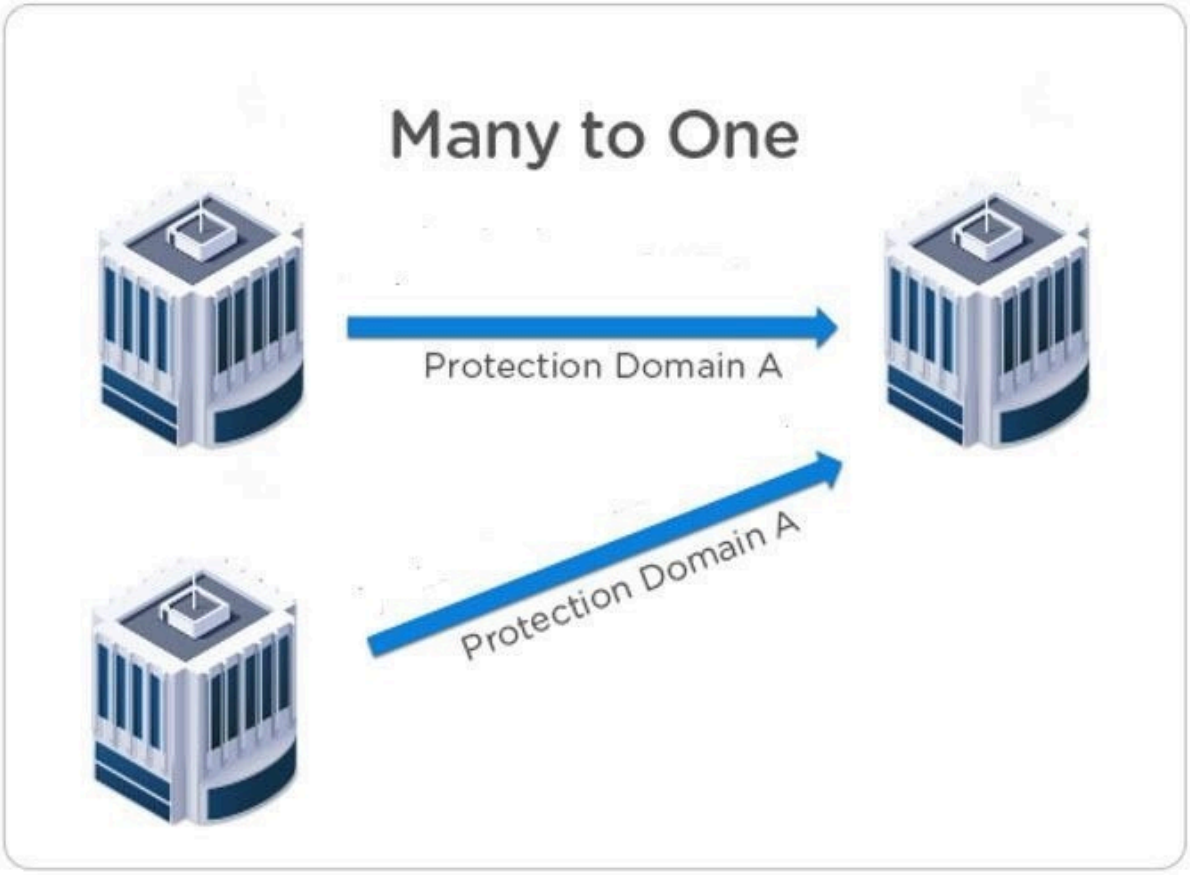


Figure 3: Many-to-One Architecture

To the Cloud

With Cloud Connect, you can use the public cloud as a destination for backing up your on-cluster VMs and volume groups. Currently, Nutanix supports Amazon Web Services (AWS) as the cloud destination. This option is particularly suitable if you don't have an offsite location for backups or are currently relying on tapes for storing backups offsite. Cloud Connect provides you with backup options for both Hyper-V and ESXi using Nutanix Prism. You can also deploy a Nutanix cluster in a public cloud provider like AWS, setting up protection domains and employing the same workflows you use with on-premises clusters.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1568

Figure 4: Public Cloud as a Backup Destination

Single-Node Backup

Nutanix has added support for single-node backup as a cost-efficient solution for providing full native backups. Using the same underlying disaster recovery technology, the single node can be either on-site or remote. Nutanix protects data on the node from single drive failure and provides native backup end to end. Single-node systems can also run VMs for testing or remote branch offices.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1569

Disaster Recovery Orchestration

With Prism Central, you can monitor and manage multiple clusters. Supported AOS versions provide protection policies and recovery plans in Prism Central, offering a way to orchestrate operations around migrations and unplanned failures. You can apply orchestration policies for ESXi and AHV from a central location, ensuring consistency across all your sites and clusters.

To manage these protection policies and recovery plans, Nutanix uses a construct called availability zones. When on-premises, an availability zone includes all the Nutanix clusters managed by one Prism Central instance. An availability zone can also represent a region in Nutanix DRaaS. For disaster recovery, availability zones exist in pairs—either on-premises to on-premises, on-premises to cloud using Nutanix Cloud Clusters, or on-premises to Nutanix DRaaS. Multiple Nutanix DRaaS subscription plans are available, so you don't have to pay the full cost of buying a secondary cluster up front, and you save the time it takes to manage and operate the infrastructure.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1570

4. Local Backup with Snapshots

Nutanix native snapshots provide production-level data protection without sacrificing performance. Nutanix uses a redirect-on-write algorithm to dramatically improve system efficiency for snapshots. Native snapshots operate at the VM level, and our crash-consistent snapshot implementation is the same across hypervisors. Implementation varies for application-consistent snapshots because of differences in the hypervisor layer. Nutanix can create local backups and recover data instantly to meet a wide range of data protection requirements.

Best practices:

- All VM files should sit on Nutanix storage. If you make non-Nutanix storage available to store files (VMDKs), the storage must have the same file path on both the source and destination clusters.
- Remove all external devices, including ISOs and floppy devices.

Crash-Consistent vs. Application-Consistent Snapshots

VM snapshots are by default crash-consistent, which means that the vDisks captured are consistent with a single point in time. The snapshot represents the on-disk data as if the VM crashed or the power cord was pulled from the server—it doesn't include anything that was in memory when the snapshot was taken. Today, most applications can recover well using crash-consistent snapshots.

Application-consistent snapshots capture the same data as crash-consistent snapshots, with the addition of all data in memory and all transactions in process. Because of their extra content, application-consistent snapshots are the most involved and take the longest to perform.

While most organizations find crash-consistent snapshots to be sufficient, Nutanix also supports application-consistent snapshots. The Nutanix application-consistent snapshot uses the Nutanix Volume Shadow Copy Service (VSS) to quiesce the file system for ESXi and AHV before taking the snapshot. You can configure which type of snapshot each protection domain maintains.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1571

Nutanix VSS Support with Nutanix Guest Tools

Nutanix Guest Tools (NGT) plays an important role in application-consistent snapshots. ESXi and AHV-based snapshots call the Nutanix VSS provider from the Nutanix Guest Agent, which is one component of NGT. VMware Tools talk to the guest VM's Nutanix VSS writers. Application-consistent snapshots quiesce all I/O, complete all open transactions, and flush the caches. Nutanix VSS freezes write I/O while the native Nutanix snapshot takes place so that all data and metadata are written consistently. After the snapshot takes place, Nutanix VSS resumes the system and allows queued writes to proceed. Application-consistent snapshots don't snapshot the OS memory during this process.

Requirements for Nutanix VSS snapshots:

- You must have NGT installed.
- An external cluster IP address must be configured.
- Guest VMs must be able to reach the external cluster IP on port 2074.
- The TCP port 23578 in the guest VM must be accessible if you want to use the Nutanix VSS service.
- Guest VMs must have an empty IDE CD-ROM for installing and configuring NGT.
- Guest VMs must use ESXi or AHV.
- Virtual disks must use the SCSI bus type.
- For NearSync support, you must have NGT version 1.3 installed.
- Nutanix VSS isn't supported with NearSync or if the VM has any delta disks (hypervisor snapshots).

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1572

- Nutanix VSS snapshots are only available for these supported versions:
  - Windows 7 and later
  - Windows Server 2008 R2 and later
  - CentOS 6.5 and 7.0
  - Red Hat Enterprise Linux (RHEL) 6.5 and 7.0
  - Oracle Linux 6.5 and 7.0
  - SUSE Linux Enterprise Server (SLES) 11 SP4 and 12
- Microsoft VSS must be running on the guest VM (Windows).
- The guest VM must support the use of Nutanix VSS writers.
- Nutanix VSS isn't supported for volume groups.
- You can't include volume groups in a protection domain configured for Metro Availability.
- You can't include volume groups in a protected VStore.
- You can't use Nutanix native snapshots to protect VMs that have VMware fault tolerance enabled.

For ESXi, if NGT isn't installed, the process fails back using VMware Tools. Because the VMware Tools method creates and deletes an ESXi-based snapshot whenever it creates a native Nutanix snapshot, it generates more I/O stress. To eliminate this stress, we strongly recommend installing NGT.

Best practices:

- Schedule application-consistent snapshots during off-peak hours. NGT takes less time to quiesce applications than VMware Tools, but application-consistent snapshots still take longer than crash-consistent snapshots.
- Increase cluster heartbeat settings when using Windows Server Failover Cluster (WSFC).

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1573

- To avoid accidental cluster failover when you perform a vMotion, follow VMware best practices to increase heartbeat probes:
  - Change the tolerance of missed heartbeats from the default of 5 to 10. Increase the number to 20 if your servers are on different subnets.
  - If you run Windows Server 2012, adjust the RouteHistoryLength to double the CrossSubnetThreshold value.

Microsoft failover settings adjusted for using Nutanix VSS:

```
(get-cluster).SameSubnetThreshold = 10
(get-cluster).CrossSubnetThreshold = 20
(get-cluster).RouteHistoryLength = 40
```

VSS on Hyper-V

Hyper-V on Nutanix supports VSS only through third-party backup applications, not snapshots. Because the Microsoft VSS framework requires a full share backup for every virtual disk in the share, Nutanix recommends limiting the number of VMs on any container using VSS backup.

Best practices:

- Create different containers for VMs that need VSS backup support. Don't exceed 50 VMs on each container.
- Create a separate large container for crash-consistent VMs.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1574

5. Protection Domains

A protection domain is a group of VMs or volume groups that you can either snapshot locally or replicate to one or more clusters when a remote site is configured. Prism Element uses protection domains when replicating between remote sites.

Best practices:

- Protection domain names must be unique across sites.
- VMware Site Recovery Manager and Metro Availability protection domains are limited to 3,200 files.
- No more than 10 VMs per protection domain with LWS.
- Group VMs with similar RPO requirements.
- NearSync can only have one schedule, so place NearSync VMs in their own protection domain.

For more information on protection domain limits, see the Nutanix Configuration Maximums page.

Consistency Groups

Administrators can create a consistency group for VMs and volume groups that are part of a protection domain and need to be snapshotted in a crash-consistent manner.

Best practices:

- Keep consistency groups as small as possible. Collect dependent applications or service VMs into a consistency group to ensure that they're recovered in a consistent state (for example, put a web server and database in the same consistency group).
- For all hypervisors, try to limit consistency groups to fewer than 10 VMs following these best practices. Although we tested consistency groups with up to 50 VMs, it's more efficient to have smaller consistency groups.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1575

- Each consistency group using application-consistent snapshots can contain only one VM.
- When you provide disaster recovery for VDI using VMware View Composer or Machine Creation Services (MCS), place each protected VM in its own consistency group (including the gold image) inside a single protection domain.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1576

6. Backup and Disaster Recovery on Remote Sites

With Nutanix you can set up remote sites, and you can choose to use those remote sites either for simple backup or for both backup and disaster recovery.

Remote sites are a logical construct. You must configure any AOS cluster—either physical or based in the cloud—as a remote site from the perspective of the source cluster before you use it as the destination for storing snapshots. Similarly, on this secondary cluster, you must configure the primary cluster as a remote site before snapshots from the secondary cluster start replicating to it.

Configuring the backup option on Nutanix allows you to use its remote site as a replication target. This option means you can back up data to this site and retrieve snapshots from it to restore locally, but failover protection (that is, running failover VMs directly from the remote site) isn't enabled. Backup supports using multiple hypervisors; as an example, an enterprise might have ESXi in the main datacenter but use Hyper-V at a remote location. With the backup option configured, the Hyper-V cluster could use storage on the ESXi cluster for backup. Using this method, Nutanix can also back up to AWS from Hyper-V or ESXi.

Configuring the disaster recovery option allows you to use the remote site both as a backup target and as a source for dynamic recovery. In this arrangement, failover VMs can run directly from the remote site. Nutanix provides cross-hypervisor disaster recovery between ESXi and AHV clusters. Currently, Hyper-V clusters can only provide disaster recovery to other Hyper-V-based clusters.

For data replication to succeed, configure forward (DNS A) and reverse (DNS PTR) DNS entries for each ESXi management host on the DNS servers used by the Nutanix cluster.

Remote Site Setup

You can customize several options when you set up a remote site. Protection domains inherit all remote site properties during replication.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1577

Address

Use the external cluster IP as the address for the remote site. The external cluster IP is highly available, as it creates a virtual IP address for all the virtual storage controllers. You can configure the external cluster IP in Nutanix Prism under cluster details.

Other recommendations:

- Try to keep both sites at the same AOS version. If both sites require compression, both must have the compression feature licensed and enabled.
- Open the following ports between both sides:
  - 2009 TCP
  - 2020 TCP
  - 9440 TCP
  - 53 UDP
- If you use the SSH tunnel, also open 22.
- Use the external cluster IP address for the source and destination. Cloud Connect uses a port between 3000—3099, but that setup occurs automatically.
- You must allow all CVM IPs to pass replication traffic between sites with the ports listed previously. To simplify firewall rules, you can use the proxy described in the following section.

Enable Proxy

The enable proxy option redirects all egress remote replication traffic through one node. This remote site proxy is different from the Prism proxy. When you enable the proxy, replication traffic goes to the remote site proxy, which then forwards it to other nodes in the cluster. This arrangement significantly reduces the number of firewall rules you need to set up and maintain.

Best practice: Use the proxy in conjunction with the external address

SSH Tunnel

An SSH tunnel is a point-to-point connection—one node in the primary cluster connects to a node in the remote cluster. By enabling proxy, we force replication traffic to go over

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1578

this node pair. You can use the SSH tunnel between Cloud Connect and physical Nutanix clusters when you can't set up a virtual private network (VPN) between the two clusters. We recommend using an SSH tunnel as a fail-back option rather than a VPN.

Best practices:

- To use an SSH tunnel, enable the proxy.
- Open port 22 between external cluster IPs.
- Only use SSH tunnel for testing—not production. Use a VPN between remote sites or a Virtual Private Cloud (VPC) with AWS.

Capabilities

The disaster recovery option requires that both sites either support cross-hypervisor disaster recovery or have the same hypervisor. Today, Nutanix supports only ESXi and AHV for cross-hypervisor disaster recovery with full snapshots. When using the backup option, the sites can use different hypervisors, but you can't restore VMs on the remote side. You also use the backup option when you back up to AWS and Azure.

Bandwidth Throttling

Max bandwidth is set to throttle traffic between sites when no network device can limit replication traffic. With the max bandwidth option, you can set different settings throughout the day and assign a max bandwidth policy when your sites are busy with production data. You can also disable the policy when they aren't as busy. Max bandwidth doesn't imply a maximum observed throughput.

When you talk with your networking teams, note that this setting is in megabytes per second, not megabits per second. NearSync doesn't currently honor maximum bandwidth thresholds.

Remote Container

VStore name mapping identifies the container on the remote cluster used as the replication target. When you establish the VStore mapping, we recommend that you create a new, separate remote container with no VMs running on it on the remote side. This configuration helps the hypervisor administrator recognize the failed-over VMs quickly and apply policies on the remote side easily in case of a failover.

Best practices:

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1579

- Create a new remote container as the target for the VStore mapping.
- If you're backing up many clusters to one destination cluster and the source containers have similar advanced settings, use only one destination container.
- Enable MapReduce compression if licensing permits.
- If you use vCenter Server to manage both the primary and remote sites, don't have storage containers with the same name on both sites.

If the aggregate incoming bandwidth required to maintain the current change rate is less than 500 Mbps, we recommend skipping the performance tier. This setting saves your flash for other workloads while also saving on SSD write endurance. To skip the performance tier, use the following command from the nCLI:

```
ncli ctr edit sequential-io-priority-order=DAS-SATA,SSD-SATA,SSD-PCIe
 name=<container-name>
```

You can reverse this command at any time.

Network Mapping

AOS supports network mapping for disaster recovery migrations moving to and from AHV. Whenever you delete or change the network attached to a VM specified in the network map, modify the network map accordingly.

Scheduling Full Snapshots and Asynchronous Replication

Set the snapshot schedule to be equal to your desired RPO. In practical terms, your RPO determines how much data you can afford to lose in the event of a failure. The failure might be due to a hardware malfunction, human error, or environmental issues. Taking a snapshot every 60 minutes for a server that changes infrequently or when you don't need a low RPO takes resources from more critical services.

You set your RPO from the local site. If you set a schedule to take a snapshot every hour, bandwidth and available space at the remote site determine if you can achieve the RPO. In constrained environments, limited bandwidth might cause the replication to take longer than the one-hour RPO, increasing the RPO. This document lists guidelines for sizing bandwidth and capacity to avoid this scenario.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1580

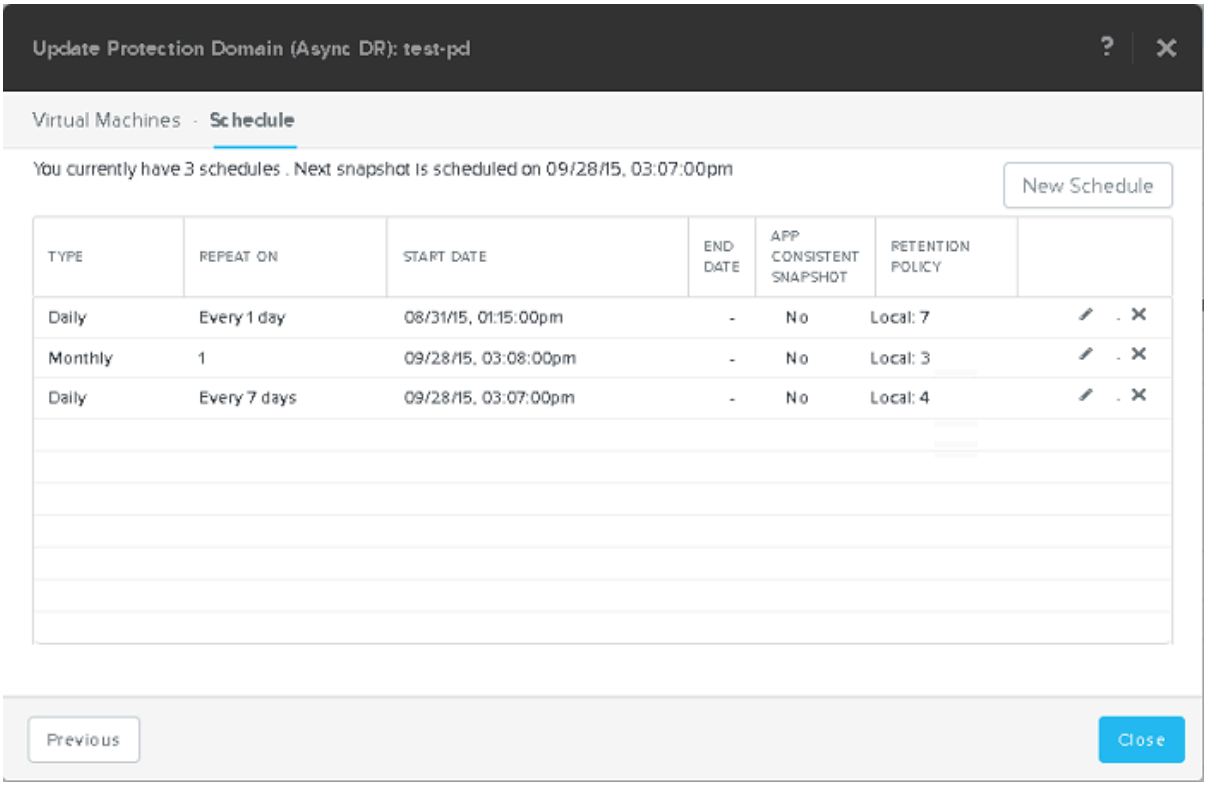


Figure 5: Multiple Schedules for a Production Domain

You can create multiple schedules for a protection domain using full snapshots, and you can have multiple protection domains. The previous figure shows seven daily snapshots, four weekly snapshots, and three monthly snapshots to cover a three-month retention policy. This policy manages metadata on the cluster more efficiently than a daily snapshot with a 180-day retention policy.

Best practices:

- Stagger replication schedules across protection domains. If you have a protection domain starting at the top of the hour, stagger the protection domains by half of the most common RPO. The goal is to spread out replication impact on performance and bandwidth.
- Configure snapshot schedules to retain the lowest number of snapshots while still meeting the retention policy, as shown in the previous figure.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1581

Remote snapshots implicitly expire based on how many snapshots exist and how frequently they are taken. For example, if you take daily snapshots and keep a maximum of five, the first snapshot expires on the sixth day. At that point, you can't recover from the first snapshot because the system deletes it automatically.

In case of a prolonged network outage, Nutanix always retains the last snapshot to ensure that you don't ever lose all the snapshots. You can modify the retention schedule from the nCLI by changing the `min-snap-retention-count` parameter. This value specifies the number of snapshots to retain, even if all the snapshots reach the expiry time. This setting works at the protection-domain level.

Scheduling Lightweight Snapshots and NearSync

Nutanix offers NearSync replication with a telescopic schedule (time-based retention). When you set the RPO between 1 and 15 minutes, you can save your snapshots for n number of weeks or months. Once you select NearSync, you can't add any more schedules.

The following table presents the default telescopic schedule to save recovery points for one month.

Table: Default Telescopic Schedule for One Month

Type	Frequency	Retention
Minute increments	Every minute	15 minutes
Hourly	Every hour	6 hours
Daily	Every 24 hours	7 days
Weekly	Every week	4 weeks
Monthly	Every month	1 month

For more information on the latest requirements and limitations, see Requirements of Data Protection with NearSync Replication.

Limit the number of VMs to 10 or fewer per protection domain. If you can, maintain one VM per protection domain to help you transition back to NearSync if you run out of lightweight snapshots (LWS) reserve storage.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1582

Cross-Hypervisor Disaster Recovery

Nutanix provides cross-hypervisor disaster recovery for migrating between ESXi and AHV clusters. The migration works with one click and uses the Prism data protection workflow. Once you've installed the mobility drivers through NGT, VMs can move freely between the hypervisors.

Best practices:

- Configure the CVM external IP address.
- Obtain the mobility driver from NGT.
- Don't migrate VMs:
  - With delta disks (hypervisor-based snapshots)
  - Using SATA disks
- Ensure that protected VMs have an empty IDE CD-ROM attached.
- Ensure that network mapping is complete.

Single-Node Backup Target

Nutanix offers the ability to use an NX-1155 or NX-1175 appliance as a single-node backup target for an existing Nutanix cluster. Because this target has different resources than the original cluster, its primary use case is to provide backup for a small set of VMs. This utility gives a fully integrated backup option to small and midsize businesses for remote and branch office (ROBO) protection.

Best practices:

- Limit all protection domains combined to fewer than 30 VMs.
- Limit backup retention to a three-month policy. We recommend a policy that includes seven daily, four weekly, and three monthly backups.
- Only map an NX-1155 or NX-1175 to one physical cluster.
- Set the snapshot schedule to at least six hours.
- Turn off deduplication.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1583

Cloud Connect

The CVM running in AWS and Azure has limited SSD space, so we recommend following these best practices when you size:

- Try to limit each protection domain to one VM to speed restore operations. This approach also saves money, as it limits the amount of data going across the WAN.
- The RPO must not be lower than four hours.
- Turn off deduplication.
- Try to use Cloud Connect to protect workloads that have an average change rate of less than 0.5 percent.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1584

7. Disaster Recovery Orchestration

The following best practices for disaster recovery orchestration cover both on-premises environments and Nutanix DRaaS. We've noted any differences between the two.

Required Infrastructure for Disaster Recovery Orchestration

- Deploy Prism Central.
  - › For on-premises environments, deploy two Prism Central instances or one Prism Central instance at a separate site for high availability.
  - › Nutanix Disaster Recovery for ROBO sites only requires one Prism Central, at the main site. When you replicate between two clusters managed from the same Prism Central instance, the minimum RPO is one hour or more and cross-hypervisor disaster recovery isn't supported.
- Deploy Prism Central on a subnet that doesn't fail over.
- Place the CVM and hypervisor IPs on a separate subnet from those used by VMs.
- The test network for on-premises disaster recovery orchestration requires a nonroutable VLAN.

Availability Zones

Paired availability zones synchronize the following disaster recovery configuration entities:

- Protection policies
- Recovery plans
- Categories used in protection policies and recovery plans

Issues (like network connectivity loss between paired availability zones) or user actions (such as unpairing availability zones, and then pairing those availability zones again) can

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1585

affect entity synchronization. Pairing previously unpaired availability zones triggers an automatic synchronization event.

If you don't update entities before you resolve a connectivity issue or pair the availability zones again, the synchronization behavior resumes. If you update entities in either or both availability zones before you resolve such issues or pair unpaired availability zones again, you can't synchronize the entities. In such a scenario, you can force the entities in one availability zone to synchronize with the paired availability zone. This forced synchronization overwrites entities at the paired availability zone.

Observe the following recommendations to avoid inconsistencies and the resulting synchronization issues:

- During network connectivity issues, don't update an entity at both availability zones in a pair. You can safely make updates at any one location. After the connectivity issue is resolved, force synchronization from the updated availability zone. Failure to adhere to this recommendation results in synchronization failures.
- You can safely create new entities in either or both availability zones if you don't assign the same name to entities in both availability zones. After you resolve the connectivity issue, force synchronization from the availability zone where you created the entities.
- If one of the availability zones becomes unavailable or if a service in the paired availability zone is down, force synchronization from the paired availability zone after you resolve the issue.

Protection Policies

A protection policy automates the creation and replication of snapshots. When you configure a protection policy for creating local snapshots, you specify the RPO, retention policy, and the entities to protect. To automate snapshot replication to a remote location, you can also specify the remote location. Nutanix Disaster Recovery uses entity-centric disaster recovery.

Requirements for using protection policies:

- A VM can only belong to a protection domain or a protection policy, not both.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1586

- If you don't use Nutanix AHV IPAM and need to retain your IP addresses, you must install NGT on the VMs you want protected.
- You can associate a VM with a maximum of two protection policies.
- When you protect a VM with more than one protection policy, only one of those policies can use NearSync or have Nutanix DRaaS as the target.

Best practices for using protection policies:

- Apply protection policies using categories.
- For VMs that haven't been replicated before, create a container with the same name on both sides. If the VM was in a protection domain before, it continues to use the same container.
- All protection policies that use NearSync must have fewer than 200 VMs.

Cross-Hypervisor Disaster Recovery

AOS supports cross-hypervisor disaster recovery for Nutanix DRaaS for ESXi on-premises. (Because Nutanix DRaaS already runs AHV, AHV on-premises just works.) Cross-hypervisor disaster recovery preserves the following elements of the ESXi configuration on failback when your on-premises environment is healthy again:

- Port group (based on network mapping)
- Virtual hardware version
- Network adapter types
- Disk adapter type
- VMware Tools state
- Amount of vCPU
- Number of cores per vCPU
- Static MAC address
- Disk provisioning (thick or thin)
- OS type

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1587

Cross-hypervisor disaster recovery has the following limitations:

- Doesn't preserve SCSI controllers (Nutanix uses LSI logic on failback)
- No support for UEFI boot
- Doesn't preserve vSphere High Availability (HA) and Distributed Resource Scheduler (DRS) settings
- No support for hypervisor-based snapshots, VMware VSS, or linked clones

Recovery Plans

A recovery plan orchestrates restoring protected VMs at a backup location. Recovery plans can either recover all specified VMs at once or, using what is essentially a runbook functionality, use power-on sequences with optionally configurable interstage delays to recover applications gracefully and in the required order. Recovery plans that restore applications in Nutanix DRaaS can also create the required networks during failover and can assign public-facing IP addresses to VMs.

The requirements for recovery plans are as follows:

- To enable disaster recovery orchestration, you must set up a Prism Element external data services IP.
- Prism Central must run on a Nutanix cluster with the external data services IP.

Nutanix DRaaS doesn't allow you to create a recovery plan if you meet either of the following conditions:

- The recovery network that you specify exists with the same name on multiple clusters.
- The networks have the same name but different IP address spaces.

> **Note:** If you add a VM to multiple recovery plans and perform failover simultaneously on those recovery plans, each recovery plan creates an instance of the VM at the recovery location. You must manually clean up the additional instances.

Create your recovery plans based on the following best practices:

- For on-premises availability zones, create a nonroutable network for testing failovers.
- Run the Validate workflow after you make changes to recovery plans.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1588

- After you run the Test workflow, run the Clean-Up workflow instead of manually deleting VMs.
- Keep asynchronous or NearSync replication VMs in separate recovery plans from synchronous replication VMs. Synchronous recovery plans don't support planned failover.

For more information on the configuration maximums for Nutanix Disaster Recovery in multiple scenarios, see Nutanix Configuration Maximums.

Virtual Networks in On-Premises Clusters

Virtual networks in on-premises Nutanix clusters are virtual subnets bound to a single VLAN. At physical locations, including the recovery location, administrators must create these virtual subnets manually, with separate virtual subnets created for production and test purposes. You must create these virtual subnets before you configure recovery plans.

When you configure a recovery plan, map the virtual subnets at the source location to the virtual subnets at the recovery location.

Virtual Networks in Nutanix DRaaS

Nutanix DRaaS features two built-in virtual networks: Production and Test. These virtual networks aren't analogous to the virtual subnets used in on-premises Nutanix clusters; they only provide two separate IP address spaces for production and testing so that activities performed in one do not affect the other. These separate Production and Test IP address spaces contain virtual subnets that are analogous to the virtual subnets in on-premises Nutanix clusters.

The Production virtual network contains subnets used for production workloads. These production workloads can be either workloads created and maintained in Nutanix DRaaS or workloads that have failed over from a paired physical location.

The Test virtual network contains the subnets to recover VMs to when you test failover from the virtual subnets at a paired physical location. When you configure a recovery plan, map the virtual subnets on your on-premises clusters to virtual subnets in the Production and Test networks in Nutanix DRaaS.

Best practices:

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1589

- Set up administrative distances on VLANs for subnets that completely fail over. If you don't set up administrative distances, shut down the VLAN on the source side after failover if the VPN connection is maintained between the two sites. If you're failing over to a new subnet, set up the subnet beforehand so that you can test the routing.
- The prefix length for network mappings must be the same at the source and the destination.
- If you don't use Nutanix IPAM, you must install NGT to maintain a static address.
- To maintain a static address for Linux VMs that don't use Nutanix IPAM, the VMs must have the NetworkManager command-line tool (nmcli) version 0.9.10.0 or later installed. Additionally, you must use NetworkManager to manage the network for the Linux VMs. To enable NetworkManager on a Linux VM, set the value of the `NM_CONTROLLED` field to `yes` in the interface configuration file (for example, in CentOS, the file is `/etc/sysconfig/network-scripts/ifcfg-eth0`). After you set this field, restart the network service on the VM.

For networking best practices specific to Nutanix DRaaS, see the Nutanix DRaaS Connectivity Tech Note.

Nutanix DRaaS Hypervisor Support

Nutanix DRaaS supports clusters running AHV or ESXi as the source.

Nutanix DRaaS VM Configuration Limitations

VMs with the following configurations can't start:

- VMs configured with a GPU resource.
- VMs configured with four vNUMA sockets.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1590

8. Sizing Space

This section provides storage sizing guidance for the following snapshot configurations:

- Full local snapshots
- Asynchonous replication
- Lightweight snapshots (LWS)
- NearSync replication

Full Local Snapshots

To size space for local snapshots, you need to account for the rate of change in your environment and how long you plan to keep your snapshots on the cluster. Reduced snapshot frequency might increase the rate of change because common blocks are more likely to change before the next snapshot.

As you lower the RPO for asynchronous replication, you might need to account for an increased rate of transformed garbage, which is space that was allocated for I/O optimization or space that was assigned but the metadata no longer refers to.

To find the space needed to meet your RPO, you can use the following formula:

```
snapshot reserve = (frequency of snapshots × change rate per frequency) +
(change rate per frequency × # of snapshots in a full curator scan × 0.1)
```

A full curator scan runs every six hours. You can compare the incremental differences between your backups to find the change rate. You can also take a conservative approach and start with a low snapshot frequency and a short expiry policy, then gauge the size difference between backups before consuming too much space.

To demonstrate using the local snapshot reserve formula, we assume that the change rate is 35 GB of data every six hours and that we keep ten snapshots:

```
snapshot reserve = (frequency of snapshots × change rate per frequency) +
(change rate per frequency × # of snapshots in a full curator scan × 0.1)
= (10 × 35,980 MiB) + (35,980 MiB × 1 × 0.1)
= 359,800 + (35,980 × 1 × 0.1)
= 359,800 + 3,598
= 363,398 MiB
```

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1591

```
= 363 GiB
```

Asynchronous Replication

Asynchronous replication uses the same process, but you must include the first full copy of the protection domain plus delta changes based on the set schedule.

Remote snapshot reserve formula:

```
snapshot reserve = (frequency of snapshots × change rate per frequency) +
(change rate per frequency × # of snapshots in a full curator scan × 0.2)
+ total size of the source protection domain
```

For the minimum amount of space needed at the remote side, 130 percent of the protection domain is a good average to work from.

If the remote target also runs a workload, incoming replication uses the performance tier. If you use a hybrid cluster, size for the additional hot data. You can also skip the performance tier by creating a separate container for incoming replication and following the steps in the Remote Container section.

Lightweight Snapshots

Sizing for LWS is similar to sizing for full snapshots in that you must account for change rate and retention time. During the LWS retention time, you don't have to size for transformed garbage space, but LWS does use additional SSD space that you must size for. By default, 7 percent of each node's SSD space forms the LWS reserve, which is an additional factor.

Duplicating the workload from the full snapshot example, let's change the RPO to one minute. LWS data exists for 75 minutes plus one extra snapshot based on the RPO value. Because the frequency rate in this scenario is high, it's very important to account for overwrites in the change rate. Because all data goes through the oplog, it's compressed; the type and amount of compression varies by workload. Using inline compression, we typically see a 2:1 compression rate.

Example Using 35 GB Change Rate Over Six Hours

If your change rate is 35 GB of data every six hours, add 5 GB to account for overwrites. 40 GB every six hours has a change rate of approximately 114 MB per minute. If the cluster is running with replication factor 2, you must account for the total physical space.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1592

LWS reserve:

```
= (frequency of snapshots × change rate per frequency) × oplog compression ×
 replication factor
= (75 × 114 MB per minute) × 0.50 × 2
= 8,550 MB
= 8.6 GB
```

If you run a 3460 hybrid system with two 1.9 TB SSDs, the following calculation shows your cluster LWS reserve:

```
= ((total SSD capacity per node – (CVM + metadata + oplog + cache overhead))
 × number of nodes) × LWS reserve percentage
= (3,539 GiB – (120 GiB + 30 GiB + 200 GiB + 40 GiB)) × 4 × 0.07
= 3,149 GB × 4 × 0.07
= 881.72 GiB
= ~945 GB
```

Apply the 7 percent of the SSD space used by the extent store after you account for the rest of the system. Because the LWS cluster reserve is 945 GB, this system has room for the workload and additional business-critical applications.

As mentioned in the Scheduling Lightweight Snapshots and NearSync section, a telescopic schedule has a total of six hourly, seven daily, four weekly, and one monthly snapshots. You only need to account for additional garbage space for the daily snapshots because of the higher frequency. Using the change rate above, you can calculate each separate schedule and add them all together. Because full snapshots occur less often than LWS, you don't have to be concerned with overwrites and can use the original 35 GB change rate for every six hours.

Example of a Telescopic NearSync Snapshot Schedule

```
Hourly change rate: 5,833 MB
Daily change rate: 140,000 MB
Weekly change rate: 980,000 MB
Monthly change rate: 3,920,000 MB

snapshot overall capacity reserve = (hourly schedule + daily schedule +
 weekly schedule + monthly schedule)

For the hourly schedule:
(frequency of snapshots × change rate per frequency) + (change rate per
 frequency × # of snapshots in a full curator scan × 0.1)

The remaining schedules:
= (frequency of snapshots × change rate per frequency)
snapshot overall capacity reserve = ((6 × 5,833)+(5,833 × 6 × 0.1)) + (7 ×
 140,000) + (4 × 980,000) + (2 × 3,920,000)
= 34,998 + 3,500 + 980,000 + 3,920,000 + 8,257,538
= 13,196,036 MB
= ~13 TB
```

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1593

For most small and medium businesses, a daily change of 140 GB is considered high. This NearSync example highlights the difference between keeping a lot of snapshots around and keeping only the 10 snapshots in the full snapshot example.

NearSync

NearSync uses the same process as the snapshot process outlined previously, but you must include the first full copy of the protection domain and delta changes based on the set schedule.

For the minimum amount of space needed at the remote site, start with 130 percent of the protection domain plus the required LWS reserve space.

Best practices:

- Use drives with the same or greater capacity at the remote site compared to those in your primary cluster to ensure enough LWS reserve space.
- Don't enable deduplication on the source container for NearSync.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1594

9. Bandwidth

You must have enough available bandwidth to keep up with the replication schedule. If you're still replicating when the next snapshot is scheduled, the current replication job finishes first. The newest outstanding snapshot then starts to get the newest data to the remote side first. To help replication run faster when you have limited bandwidth, you can seed data on a secondary cluster at the primary site before shipping that cluster to the remote site.

Seeding

To seed data for a new site:

1. Set up a secondary cluster with local IPs at the primary site.
2. Enable compression on the remote site in the production domain.
3. Set the initial retention time to 3 months.
4. Reconfigure the secondary cluster with remote IPs.
5. Turn off the secondary cluster.
6. Ship the secondary cluster to the remote site.
7. Turn on the remote cluster.
8. Update the remote site on the primary cluster to the new IP.

If you can't seed the protection domain at the local site, you can create the remote cluster as a normal install and turn on compression over the wire. Manually create a one-time replication with retention time set to three months. We recommend this retention time setting because of the extra time it takes to replicate the first data set across the wire.

To figure out how much throughput you need, you must know your RPO. If you set the RPO to one hour, you must be able to replicate the changes within that time.

Assuming you know your change rate based on incremental backups or local snapshots, you can calculate the bandwidth needed. The next example uses a change rate of 15 GB and an RPO of one hour. We don't use deduplication in the calculation, partly so the dedupe savings can serve as a buffer in the overall calculation and because the one-time cost for deduped data going over the wire has less impact once the data is present at the

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1595

remote site. We assume an average of 30 percent bandwidth savings for compression on the wire.

Bandwidth sizing:

```
Bandwidth needed = (RPO change rate × (1 – compression on wire savings %)) /
 RPO

Example:
(15 GB × (1 - 0.3)) / 3,600 sec
(15 GB × 0.7) / 3,600 sec
10.5 GB / 3,600 sec
(10.5 × 1,000 MB) / 3,600 sec (changing to MBps)
(10,500 MB) / 3,600 sec
10,500 MB / 3,600 = 2.92 MBps
Bandwidth needed = 23.33 Mbps
```

If you keep missing your replication schedule, either increase your bandwidth or your RPO. For more RPO flexibility, you can run different schedules on the same production domain; for example, have one daily replication schedule and create a separate schedule to take local snapshots every two hours.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1596

10. Failover: Migrate vs. Activate

Nutanix offers two options for handling VMs and volume groups during failover: migrate and activate.

Use the migrate option when you know that both the production site and the remote site are healthy. This option is only available on the active production site. Migrate shuts down the VM or volume group, takes another snapshot, and replicates the VM or volume group to the selected remote site.

The activate option for restoring a VM is only available on the remote site. When you select activate, the system uses the last snapshot on the remote side to bring up the VM, regardless of whether the active production site is healthy. You can't sync any outstanding changes to the VM from the production site.

If you activate a protection domain because the primary site is down but the primary site comes back up after the failover, you can have a split-brain scenario. To resolve this situation, deactivate the protection domain on the former primary site. The following command is hidden from the nCLI because it deletes the VMs, but it resolves the split while keeping the existing snapshots:

```
ncli> pd deactivate_and_destroy_vms name=<protection_Domain_Name>
```

You can test a VM at the remote site without breaking replication using the restore or clone functionality.

Use the local snapshot browser on the inactive production domain at the remote site, and choose the restore option to clone a VM to the datastore. Add a prefix to the VM's path.

Best practices:

- When you activate protection domains on the remote site, use intelligent placement for Hyper-V and DRS for ESXi clusters. Intelligent placement evenly spreads out the VMs on startup during a failover. AOS powers on VMs uniformly at start time.
- Install NGT on machines using volume groups.
- Configure the data services cluster IP on the remote cluster.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1597

Protection Domain Cleanup

Because inactive protection domains still consume space in existing snapshots, you should remove any unused protection domains to reclaim that space.

To remove a protection domain from a cluster, follow these steps:

1. Remove existing schedules.
2. Remove both local and remote snapshots.
3. Remove the VMs from the active protection domain.
4. Delete the protection domain.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1598

11. Self-Service File Restore

Self-service file restore is available for ESXi and AHV. The goal is to offer self-service file-level restore with minimal support from infrastructure administrators. Once you install NGT, you can open a web browser and go to `http://localhost:5000` to browse snapshots sorted by today, last week, last month, and user-defined criteria. Self-service works with both protection domains and Nutanix Disaster Recovery.

- Guest VMs must use:
  - Windows 2008, Windows 7, or later
  - Centos 6.5 or later and 7.0 or later
  - Red Hat 6.5 or later and 7.0 or later
  - OEL 6.5 or later
  - SLES 11 or later
- Install VMware Tools.
- Remove JRE 1.8 or later if installed with a previous release.
- Configure a cluster external IP address.
- Add the VM to a protection domain.
- Use the default disk.EnableUUID = true for the VM in advanced settings for ESXi.
- The VM must have an IDE-based CD-ROM configured for installation. On newer versions of ESXi, a SATA-based CD-ROM is added by default.
- Detach the mounted disk after you restore your files.

Limitation: For Linux VMs, logical volumes spanning multiple disks aren't supported.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1599

12. Third-Party Backup Products

Nutanix provides its own hypervisor-agnostic, changed-region tracking API that vendors can access using a REST API. Currently, Cohesity, Commvault, Druva, HYCU, and Rubrik provide backup support specifically for AHV. Nutanix systems can integrate with any backup vendor that supports vStorage APIs for Data Protection for ESXi. Nutanix also offers a VSS provider for Hyper-V backup software vendors. For more information on certified third-party solutions, see the Nutanix Elevate Technology Alliance Partner Program page.

Backups with Replication

Hypervisor-based snapshots left on the VM when you take a hardware-based snapshot might cause the recovery to fail. You must manually turn on the VM. For more information, see VMware KB 1025279.

Backup software interacting with AHV uses scoped production domains, also known as backup snapshots. When the backup software requests a snapshot of a VM that isn't protected under any user-created production domain, temporarily protect the VM by placing it in a scoped production domain. Issue a snapshot of this production domain, then remove the VM from the production domain. With backup snapshots, you can also back up VMs and use disaster recovery orchestration. The only possible issue is that while the snapshot operation on the scoped production domain is in progress, the user-initiated VM protection might fail in the regular production domain.

Best practices:

- Avoid using hypervisor-based snapshots.
- Try to schedule hypervisor snapshots or user-created, hardware-based snapshots at times outside of the backup window.

For optimization and scaling recommendations for third-party backup solutions, see the best practice guides on an enhanced disk-to-disk backup architecture on the Nutanix Support Portal.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1600

13. Conclusion

Nutanix offers granular data protection based on your required recovery point objectives across many different deployment models. As your application requirements change and your cluster grows, you can add and remove VMs from protection domains. Sizing capacity and bandwidth are key to achieving optimal data protection and maintaining cluster health. Snapshot frequency and the daily change rate affect the capacity and bandwidth needed between sites to meet the needs of the business.

With data protection features that are purpose-built, fully integrated, and completely software-defined, Nutanix provides the adaptability and flexibility for meeting your enterprise's backup and recovery needs.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1601

14. Appendix

The following sections provide high-level best practices for backup and disaster recovery on Nutanix.

General Best Practices

- Store all VM files on Nutanix storage. If non-Nutanix storage stores files externally, it should have the same file path on both sides.
- Remove all external devices, including ISOs or floppy devices.

Nutanix Native VSS Snapshots

- Configure an external cluster IP address.
- Guest VMs must be able to reach the external cluster IP on port 2074.
- Guest VMs must have an empty IDE CD-ROM for attaching NGT.
- Guest VMs must use ESXi or AHV.
- Virtual disks must use the SCSI bus type.
- VSS must be running in the guest VM.
- The guest VM needs to support the use of VSS writers.
- Schedule application-consistent snapshots during off-peak hours or ensure that additional I/O performance is available. If you take a VSS snapshot during peak usage, the delta disk from the hypervisor-based snapshot might become large. When you delete the hypervisor-based snapshot, collapsing it takes additional I/O; account for this additional I/O to avoid affecting performance.

Hyper-V VSS Provider

- VSS support is only for backup.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1602

- Create different containers for VMs that need VSS backup support. Limit the number of VMs on each container to 50.
- Create a separate large container for crash-consistent VMs.

Protection Domains

- Protection domain names must be unique across sites.
- Group VMs with similar RPO requirements.
- For current limits, see the Nutanix Configuration Maximums page.
- VMware Site Recovery Manager and Metro Availability protection domains are limited to 50 VMs.
- Linked clone VMs (typically nonpersistent View desktops) aren't supported with NearSync.
- Remove unused protection domains to reclaim space.
- If you must activate a protection domain rather than migrate it, deactivate the old primary protection domain when the site comes back up.

Consistency Groups

- Keep consistency groups as small as possible. Keep dependent applications or service VMs in one consistency group to ensure that they are recovered in a consistent state (for example, App and DB).
- Each consistency group using application-consistent snapshots can contain only one VM.

Disaster Recovery and Backup

- Ensure that you configure forward (DNS A) and reverse (DNS PTR) DNS entries for each ESXi management host on the DNS servers used by the Nutanix cluster.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1603

Remote Sites

- Use the external cluster IP as the address for the remote site.
- Use disaster recovery proxy to limit firewall rules.
- Use max bandwidth to limit replication traffic.
- When activating protection domains, use intelligent placement for Hyper-V and DRS for ESXi clusters on the remote site. Intelligent placement evenly spreads out the VMs at start time during a failover. AOS starts VMs uniformly at start time.
- If you use vCenter Server to manage both the primary and remote sites, don't use storage containers with the same name on both sites.

Remote Containers

- Create a new remote container as the target for the VStore mapping.
- When you back up many clusters to one destination cluster, use only one destination container if the source containers have similar advanced settings.
- Enable MapReduce compression if licensing permits.
- If the aggregate incoming bandwidth required to maintain the current change rate is less than 500 Mbps, we recommend skipping the performance tier to save flash capacity and increase device longevity.

Network Mapping

- Whenever you delete or change the network attached to a VM specified in the network map, modify the network map accordingly.

Scheduling

- To spread out replication impact on performance and bandwidth, stagger replication schedules across protection domains. If you have a protection domain starting at the top of the hour, stagger the protection domains by half of the most common RPO.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1604

- Configure snapshot schedules to retain the smallest number of snapshots while still meeting the retention policy.
- Metro and SRM-protected containers aren't supported.
- Deduplication on the source container isn't currently supported for NearSync.

Cross-Hypervisor Disaster Recovery

- Configure the CVM external IP address.
- Obtain the mobility driver from NGT.
- Don't migrate VMs with delta disks (hypervisor-based snapshots), using SATA disks, or using volume groups.
- Ensure that protected VMs have an empty IDE CD-ROM attached.
- Ensure that network mapping is complete.

Disaster Recovery Orchestration

- Deploy Prism Central to each on-premises site.
- Deploy Prism Central on a subnet that doesn't fail over.
- Place CVM and hypervisor IPs on a separate subnet from the subnets used by VMs.
- On-premises disaster recovery orchestration requires a nonroutable VLAN for the test network.

Availability Zones

- If one of the availability zones becomes unavailable or if a service in the paired availability zone is down, resolve the issue and then force synchronization from the paired availability zone.

Protection Policies

- A VM can only belong to a protection domain or a protection policy, not both.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1605

- If you don't use Nutanix AHV IPAM and need to retain your IP addresses, install NGT on the VMs to be protected.
- Use categories to apply protection policies.
- For Nutanix Disaster Recovery on-premises, create the same container name on both sides. If the container name doesn't match on both sides, data replicates by default to the SelfServiceContainer.

Cross-Hypervisor Support with ESXi for Protection Policies

- No support for UEFI boot
- Doesn't preserve vSphere HA and DRS settings
- No support for hypervisor-based snapshots, VMware VSS, or linked clones

---

Recovery Plans

- For on-premises availability zones, create a nonroutable network for testing failovers.
- Run the Validate workflow after making changes to recovery plans.
- After you run the Test workflow, run the Clean-Up workflow instead of manually deleting VMs.
- For the current limits, see Nutanix Configuration Maximums.

Network Mapping

- Set up administrative distances on VLANs for subnets that completely fail over. If you don't set up administrative distances, shut down the VLAN on the source side after failover if the VPN connection is maintained between the two sites. If you're failing over to a new subnet, set up the subnet beforehand so you can test the routing.
- The prefix length for network mappings at the source and the destination must be the same.
- If you don't use Nutanix IPAM, you must install the NGT software package to maintain a static address.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1606

- To maintain a static address for Linux VMs that don't use Nutanix IPAM, the VMs must have the NetworkManager command-line tool (nmcli) version 0.9.10.0 or later installed. Additionally, you must use NetworkManager to manage the network for the Linux VMs. To enable NetworkManager on a Linux VM, set the value of the NM_CONTROLLED field to `yes` in the interface configuration file (for example, in CentOS, the file is `/etc/sysconfig/network-scripts/ifcfg-eth0`). After you set the field, restart the network service on the VM.

Nutanix DRaaS Hypervisor Support

- Nutanix DRaaS only supports clusters running AHV.

Nutanix DRaaS VM Configuration Restrictions

- Can't power on VMs configured with a GPU resource.
- Can't power on VMs configured with four vNUMA sockets.

Single-Node Backup

- Limit all protection domains combined to fewer than 30 VMs.
- Limit backup retention to a three-month policy. We recommended seven daily, four weekly, and three monthly backups.
- Only map an NX-1155 to one physical cluster.
- Snapshot schedule must be at least six hours.
- Turn off deduplication.

Cloud Connect

- Try to limit each protection domain to one VM to speed up restores. This approach also saves money, as it limits the amount of data going across the WAN.
- The RPO shouldn't be lower than four hours.
- Turn off deduplication.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1607

- Try to use Cloud Connect to protect workloads that have an average change rate of less than 0.5 percent.

Sizing

- Size local and remote snapshot storage using the application's change rate.
- Remember to either size the performance tier for hybrid clusters to accommodate incoming data or bypass the performance tier and write directly to disk.

Bandwidth

- Seed locally for replication if WAN bandwidth is limited.
- Set a high initial retention time for the first replication when you seed.

File-Level Restore

- Guest VMs must use:
  - Windows 2008, Windows 7, or later
  - Centos 6.5 or later and 7.0 or later
  - Red Hat 6.5 or later and 7.0 or later
  - OEL 6.5 or later
  - SLES 11 or later
- Install VMware tools.
- Install JRE 1.8 or later.
- Configure a cluster external IP address.
- Add the VM to a protection domain.
- Use the default `disk.EnableUUID = true` for the VM in advanced settings.
- The VM must have a CD-ROM configured.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1608

- Detach the mounted disk after restoring your files.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1609

About Nutanix

Nutanix offers a single platform to run all your apps and data across multiple clouds while simplifying operations and reducing complexity. Trusted by companies worldwide, Nutanix powers hybrid multicloud environments efficiently and cost effectively. This enables companies to focus on successful business outcomes and new innovations. Learn more at Nutanix.com.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1610

List of Figures

Figure 1: Scalable Replication..... 9

Figure 2: Two-Way Mirroring..... 12

Figure 3: Many-to-One Architecture..... 13

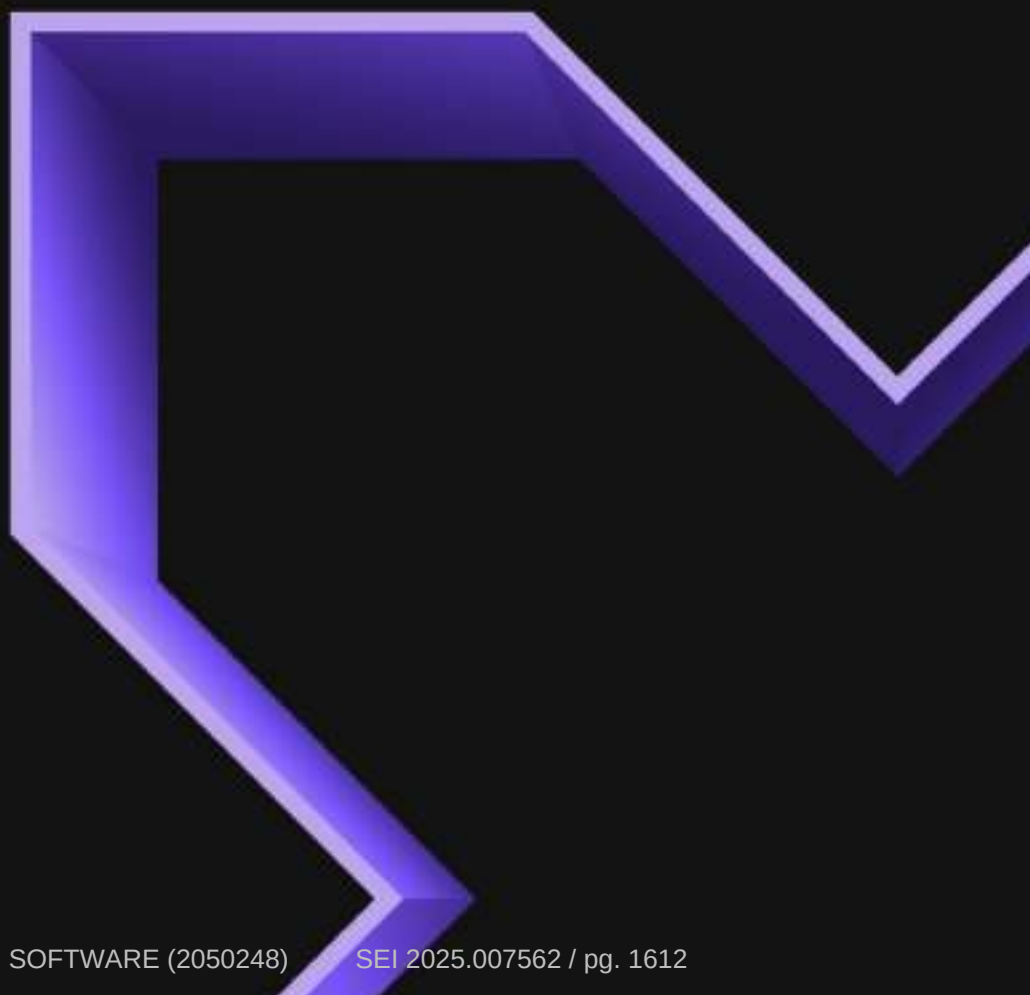
Figure 4: Public Cloud as a Backup Destination..... 14

Figure 5: Multiple Schedules for a Production Domain..... 26

v4.1 | December 2024 | BP-2009

SOLUTIONS DOCUMENT

Metro Availability Best Practices



NUTANIX

Legal

© 2024 Nutanix, Inc. All rights reserved. Nutanix, the Enterprise Cloud Platform, the Nutanix logo and the other Nutanix products, features, and/or programs mentioned herein are registered trademarks or trademarks of Nutanix, Inc. in the United States and other countries. All other brand and product names mentioned herein are for identification purposes only and are the property of their respective holder(s), and Nutanix may not be associated with, or sponsored or endorsed by such holder(s). This document is provided for informational purposes only and is presented "as is" with no warranties of any kind, whether implied, statutory or otherwise.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

Contents

1. Executive Summary..... 5

2. Metro Availability Overview..... 7
- Active Containers..... 9
- Standby Containers..... 10
- Metro Availability Witness..... 12
- Metro Availability Replication States..... 13

3. VMware Component Overview..... 18
- VMware High Availability Cluster..... 18
- VMware Distributed Resource Scheduler..... 20
- VMware vMotion..... 21
- VMware vCenter Server..... 22

4. Operational Scenarios..... 24
- Establishing Metro Availability..... 24
- Planned Failover..... 25
- Network Outage Between the Nutanix Clusters..... 27
- Site Failure..... 31
- Site Recovery..... 33
- Metro Availability Witness-Specific Workflows..... 37
- Operational Scenarios Summary..... 40
- Asynchronous Snapshot Workflows..... 42

5. Metro Availability Best Practices Checklist..... 50
- Requirements..... 50
- Interoperability..... 50
- Limitations..... 51
- Nutanix Recommendations..... 52
- VMware Recommendations..... 53

6. Metro Availability Detailed Best Practices: Nutanix Cloud Platform..... 55
- Acropolis Upgrade..... 55

Networking Performance and Availability..... 55
Cluster Hardware Configuration and Sizing..... 56
Virtual Machine Locality..... 56

7. Metro Availability Detailed Best Practices: VMware.....58
VMware High Availability Cluster.....58
vCenter Server Availability.....59
VMware Distributed Resource Scheduler Affinity Rules.....59

8. Utilities and Alerting.....61
REST API..... 61
nCLI Commands..... 61
PowerShell Commands.....62
Nutanix Cluster Check..... 63
Alerts.....63

9. Conclusion.....65

About Nutanix.....66

List of Figures.....67

1. Executive Summary

IT departments regularly face demanding service-level agreements (SLAs) that require building resilience into all aspects of the datacenter. While traditional solutions provide redundancy at the hardware layer, administrators must still manage downtime due to infrastructure failures, site maintenance, or natural disasters.

Many existing solutions are expensive, complex, and built on legacy principles and infrastructure. As a result, many application workloads aren't protected—or are underprotected—and are vulnerable to outages. To help address these concerns, Nutanix developed a continuous availability solution called Metro Availability. Metro Availability creates a global file system namespace across Nutanix clusters and uses synchronous replication. Combining the Nutanix hyperconverged infrastructure with a continuous availability solution limits downtime and preserves all data, even during a complete site failure. Further, Metro Availability enables workload mobility for disaster avoidance or planned maintenance scenarios.

With Metro Availability, you can extend hypervisor clustering technologies across datacenters. This stretched-cluster configuration minimizes downtime during unplanned outages. Metro Availability also supports migrating virtual machines (VMs) across sites, using technologies such as vMotion, which results in zero downtime while transitioning workloads between datacenters.

With Metro Availability, Nutanix delivers an entire spectrum of solutions to provide the data and application protection you need to fulfill your SLAs and meet your recovery point and recovery time objectives (RPOs and RTOs). Nutanix built safeguards into the platform for everything from minor events, such as individual VM deletion, to major ones, including unplanned datacenter failure. You can set up and manage your solution from Nutanix Prism, a consumer-grade management experience for handling disaster recovery and high availability.

This document presents an overview of Nutanix and the Metro Availability for VMware vSphere feature, and we describe deployment considerations and general best practices around Metro Availability functionality in a VMware vSphere environment.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1616

This document addresses key items for enabling successful design, implementation, and transition to operation.

Table: Document Version History

Version Number	Published	Notes
1.0	February 2015	Original publication.
2.0	April 2016	Updated for AOS 4.6.
3.0	January 2017	Updated for AOS 5.0.
3.1	March 2018	Updated platform overview.
3.2	May 2018	Updated Nutanix overview and deduplication recommendations.
3.3	September 2018	Updated container sizing and network configuration guidance.
3.4	August 2019	Updated for AOS 5.11.
3.5	June 2020	Updated for AOS 5.15 and AOS 5.17.
3.6	March 2021	Updated information on VM Component Protection (VMCP) and witness-specific workflows.
3.7	April 2022	Refreshed content.
4.0	October 2023	Updated nCLI syntax, clarified cross-hypervisor disaster recovery limitations, and added detailed best practices specific to the Nutanix Cloud Platform and VMware.
4.1	December 2024	Minor text updates throughout.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1617

2. Metro Availability Overview

Metro Availability for VMware vSphere is part of a suite of data protection features offered on the Nutanix platform. As a continuous availability solution, Metro Availability for VMware vSphere provides a global file system namespace across a container that's stretched between Nutanix clusters. Synchronous storage replication supports the stretched container across independent Nutanix clusters, using the protection domain and remote site constructs. The platform replicates all VMs and files stored in that container synchronously to another Nutanix cluster.

Each protection domain maps to one container. You can create multiple protection domains to enable different policies, including bidirectional replication, where each Nutanix cluster replicates synchronously to one or more clusters. When enabled for Metro Availability, containers exist in two primary states: active and standby. As shown in the following figure, active containers replicate data synchronously to standby containers.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1618

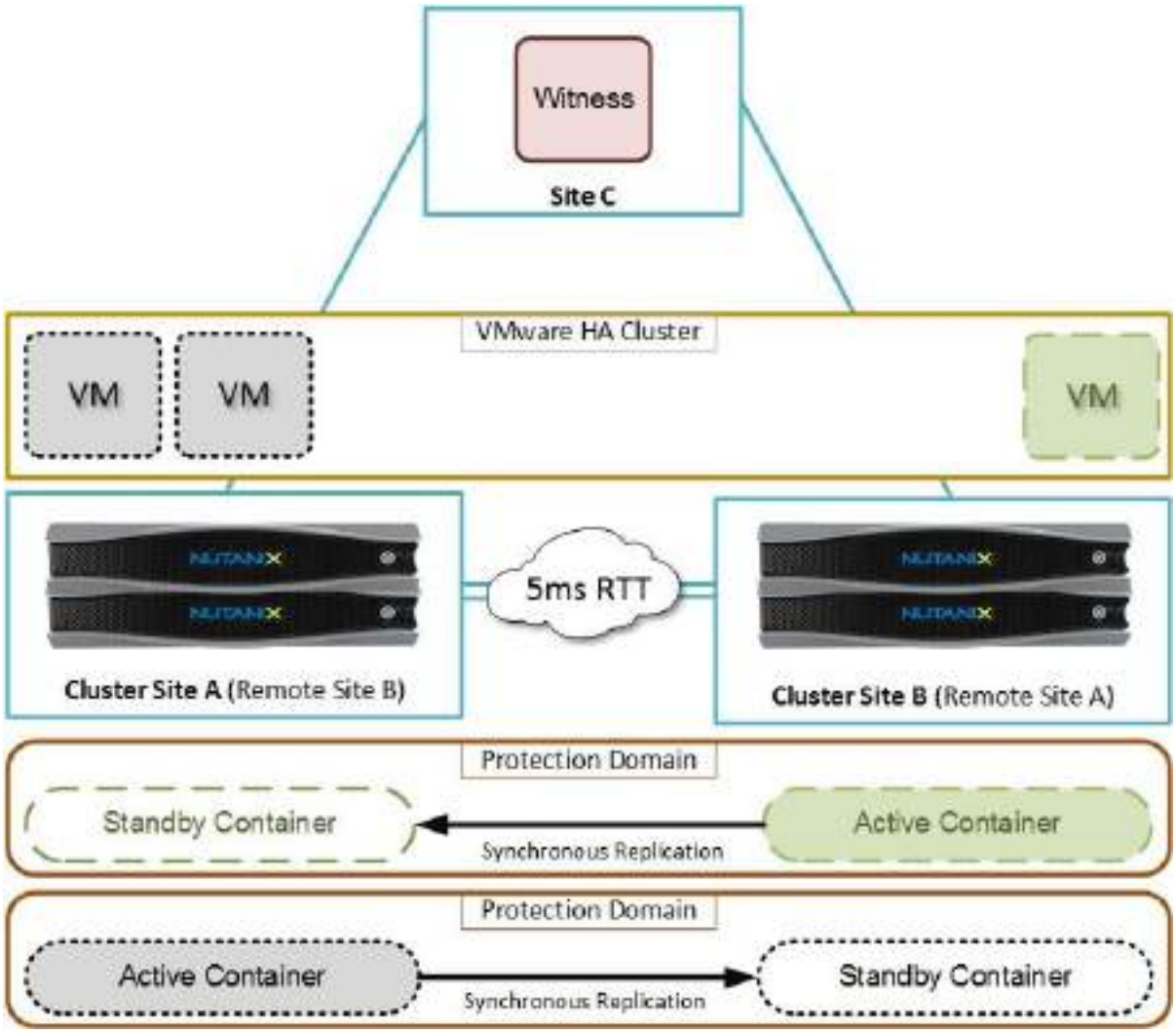


Figure 1: Metro Availability Overview

You can create a protection domain by specifying an active container on the local cluster and a standby container with the same name on the remote cluster. The active and standby containers mount to their respective hypervisor hosts using the same datastore name, which effectively spans the datastore across both clusters and sites. With a datastore stretched across both Nutanix clusters, you can create a single hypervisor cluster and use common clustering features, like VMware vMotion and VMware High Availability (VMware HA), to manage the environment. Hosts presenting standby containers can run VMs targeted for the standby container; however, standby containers

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1619

aren't available for direct VM traffic. The system forwards all I/O targeted for a standby container to the active site.

Nutanix supports Metro Availability in conjunction with other data management features, including compression, deduplication, and tiering. By enabling compression for the synchronous replication traffic between the Nutanix clusters, you reduce the total bandwidth required to maintain the synchronous relationship.

Active Containers

Active containers are fully read and write and process all VM I/O operations. Local read operations for a VM running against an active container function like non-Metro Availability environments. All local write operations, including both random and sequential writes, go through the oplog of the Controller Virtual Machine (CVM) with Metro Availability enabled. When local writes occur, data replicates locally based on the container's replication factor. In parallel, the system sends remote writes to the oplog of a CVM in the cluster maintaining the standby container. The standby container's replication factor determines the number of writes required to complete the remote write operation against the peer cluster. After all replication factor writes are processed for both the active and standby containers, the VM receives an acknowledgment that the write is complete. The following diagram depicts this process.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1620

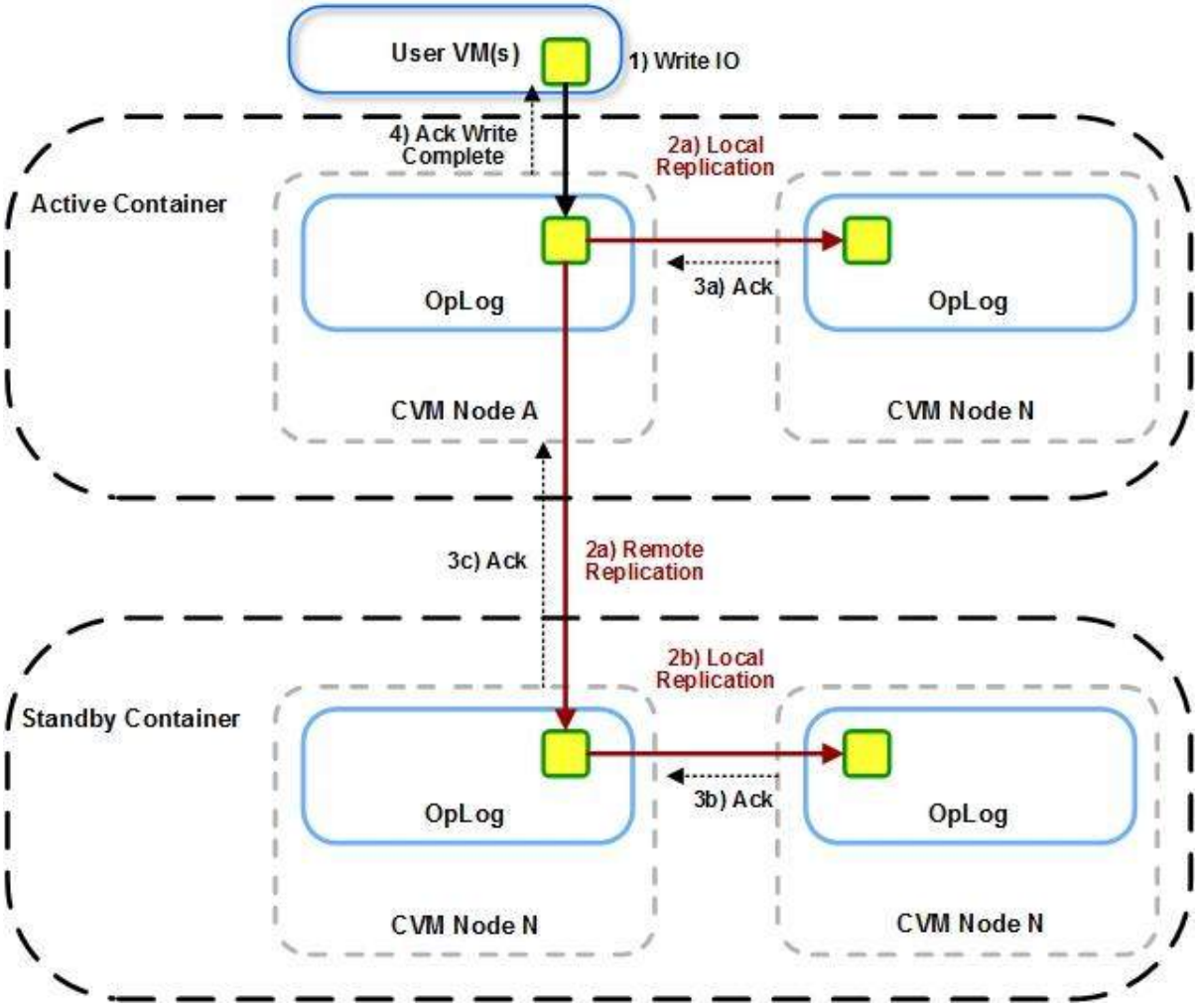


Figure 2: VM Write to an Active Container with Replication Factor 2 at Both Sites

Standby Containers

Standby containers receive synchronous write updates from the active container. Standby containers mount to the appropriate hypervisor instances in the Nutanix cluster, so you can run VMs locally to the hypervisor nodes that own the container and datastore. While the standby container appears available, it does not process VM I/O directly. The system forwards all VM read or write I/O targeted for a standby container to a CVM in the cluster that owns the active container before returning data or acknowledgment to the VM. The following figures depict the behavior of these remote read-and-write operations.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1621

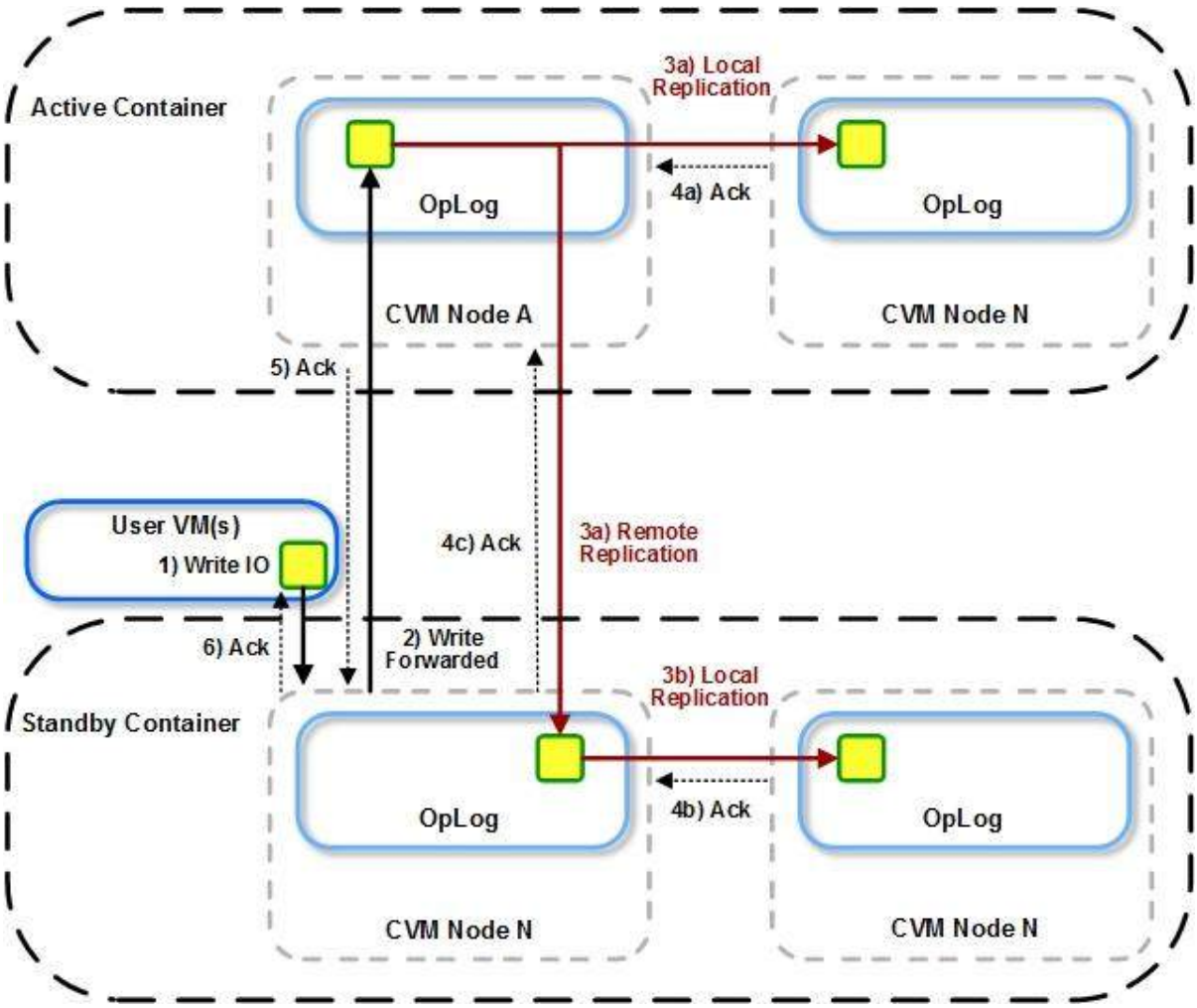


Figure 3: VM Write to a Standby Container with Replication Factor 2 at Both Sites

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1622

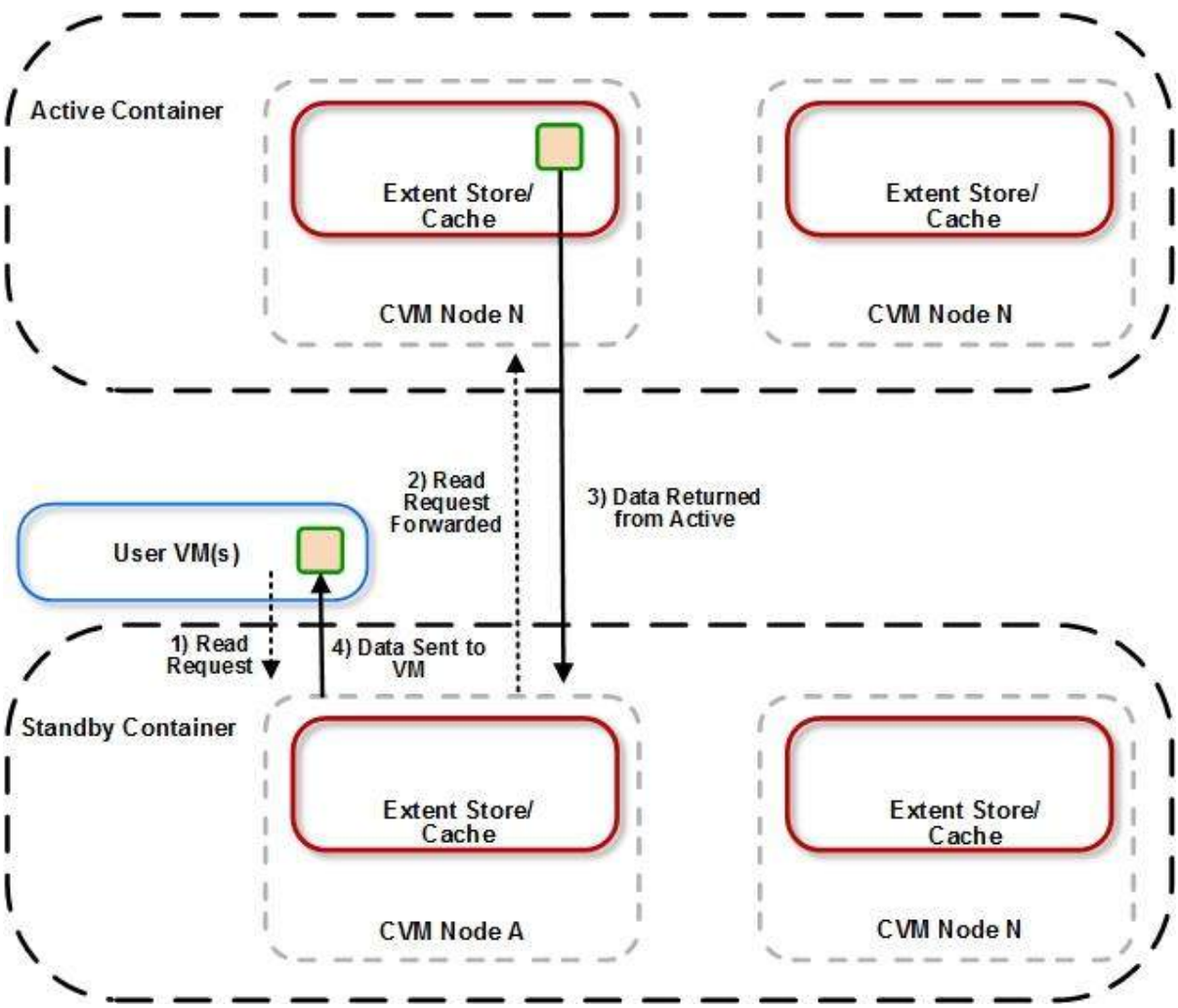


Figure 4: VM Read from a Standby Container

Metro Availability Witness

The Metro Availability witness allows Nutanix clusters to automate storage and replication state management, including promoting standby protection domains, so VMs can automatically fail over during site failures. The witness is a VM you can install in both Nutanix and non-Nutanix environments. It resides in a site and failure domain separate from the Nutanix clusters forming the Metro Availability relationship, enabling failover decisions that avoid conditions that can lead to a split-brain scenario where storage is active on both sites.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1623

Nutanix clusters register with the witness, and each protection domain represents a unique relationship. This design permits multiple sets of clusters to register with one witness and supports both active and standby protection domains. To use the witness-based functionality, the Nutanix clusters must run a supported version of AOS. The following sections provide additional information about this feature.

Metro Availability Replication States

When you first enable Metro Availability, a full copy of the data residing in the active container replicates between the clusters. Nutanix uses a snapshot for this initial full copy and maintains it as a reference point. The relationship is in a synchronizing state until the copy completes. Any writes that occur following the initial snapshot replicate synchronously. After it's fully synchronized, the protection domain enters an enabled state, which indicates that the standby container is consistent.

Failure Handling

A network failure between Nutanix clusters in a Metro Availability relationship first halts any writes against the active container, and the replication state reports `remote unreachable`. A standby container becomes unavailable and inactive to the hypervisor host while the active container is unreachable. The failure handling setting offers options for disabling Metro Availability to allow writes to continue against the active container: manual, automatic resume, or witness.

With failure handling set to manual, VM writes don't resume until network connectivity is restored between the clusters or an administrator manually disables Metro Availability. Use this option in environments that require strict, continuous synchronous replication between sites. If network connectivity is restored, the replication state immediately returns to enabled, and synchronous replication continues between the clusters; otherwise, writes are held indefinitely. If an administrator manually disables replication, the system reports a disabled state and writes resume, but they only propagate to the active container. Following a manual disable operation, replication to the standby container does not resume until network connectivity is restored and the administrator manually enables it again.

With failure handling set to automatic resume, the replication state immediately returns to enabled if network connectivity is restored within the time-out specified in the automatic replication break setting. Writes continue to replicate synchronously between the

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1624

clusters. The default automatic replication break time-out is 10 seconds. If the time-out period expires, the system automatically disables Metro Availability and writes resume, but they only propagate to the active container. Using this option, temporary network outages between sites don't impact applications running against the active container. Following the automatic replication break, replication to the standby container doesn't resume until network connectivity is restored and the administrator manually enables it again.

The Nutanix availability witness provides an automatic mechanism for disabling Metro Availability for the primary protection domain and promoting the standby protection domain. With failure handling set to witness, when network connectivity between the Nutanix clusters is interrupted, both sites attempt to obtain a lock against the witness VM for each protection domain. A cluster attempts to obtain the witness lock against primary protection domains after 10 seconds and against standby protection domains after 120 seconds. If the primary protection domain obtains the lock, the system automatically disables Metro Availability and writes resume, but they only propagate to the active container. If the primary protection domain fails to obtain the lock, all I/O is held for its respective container until network connectivity is restored or an administrator disables the protection domain. If the standby protection domain obtains the lock, the system automatically promotes it to active. If the standby protection domain fails to obtain the lock, it becomes unavailable and inactive to the hypervisor host until network connectivity is restored or an administrator manually performs the promotion. The Operational Scenarios section contains more details regarding automatic failure handling when using the witness.

After you set the failure handling option during the protection domain creation process, you can modify it from the Nutanix command-line interface (nCLI) or the Nutanix Prism UI. The Utilities and Alerting section provides an example of how to modify this setting using the nCLI.

Resume Replication

When replication is disabled, either manually by an administrator or automatically based on the failure handling setting, you can issue a command from the original active cluster to resume replication after network connectivity is restored. The system creates a snapshot that references the last snapshot taken. While enabled, Metro Availability takes a snapshot every six hours to use as a reference point. The data that represents the differences between the current and the last reference snapshot then replicates to the

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1625

standby container. The amount of data replicated might be more than the incremental amount of change since the network or site outage and can represent all data if the containers were empty at the time of the last reference snapshot.

You can also resume replication against the standby cluster to carry out planned failovers or to reestablish Metro Availability following an unplanned event. The replication direction depends on which cluster you choose, and the cluster you resume replication from becomes the active site and the source for replication. For example, if you choose the standby cluster to enable Metro Availability after a failover, replication for the container is essentially reversed: the standby becomes the active container, and the original active container becomes the standby.

The following flowcharts provide an overview of the replication states from the perspective of the active protection domain in the following figure and the standby protection domain in the subsequent figure. Note that these flowcharts don't include details about deleting a protection domain, which is an additional option and affects states. The Operational Scenarios section contains additional information on which steps to perform in each event.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1626

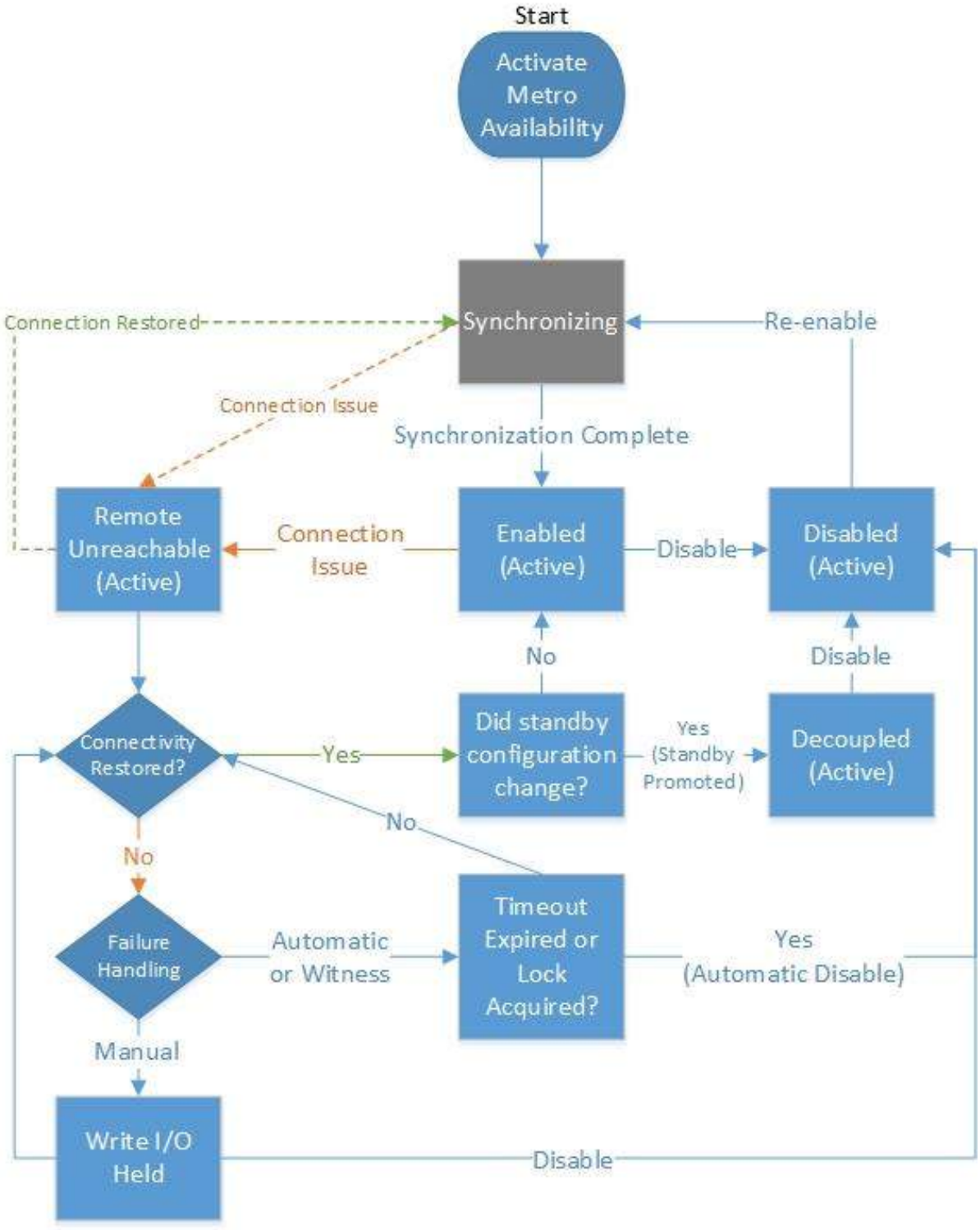


Figure 5: Active Protection Domain Flowchart

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1627

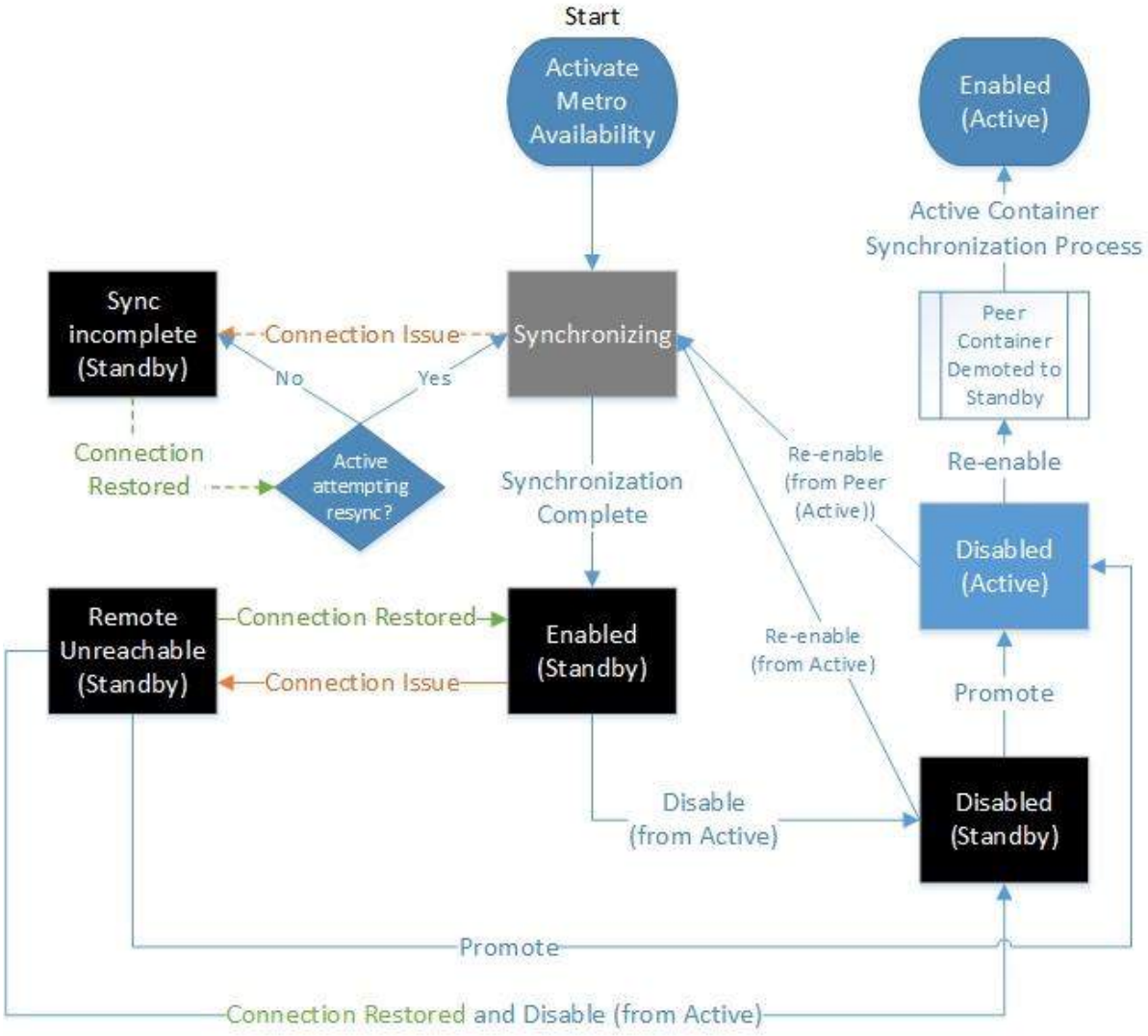


Figure 6: Standby Protection Domain Flowchart

© 2024 Nutanix, Inc. All rights reserved

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1628

3. VMware Component Overview

To deploy and operate a Metro Availability–based stretched cluster successfully, you must understand the following VMware components.

VMware High Availability Cluster

One of the goals of Metro Availability is to simplify VM recovery management. Because Metro Availability presents a stretched datastore between two Nutanix clusters, you can form a single VMware cluster. With that single stretched VMware cluster, you can use VMware HA to provide speed and automation to VM recovery.

Each host in a VMware HA cluster operates as a leader host or a worker host. A cluster contains one leader host, with all other hosts operating as workers. The leader performs several functions, including monitoring worker hosts, monitoring the power state of protected VMs, keeping an inventory of cluster hosts and protected VMs, and communicating cluster health state to the vCenter Server.

When a server fails, the VMware HA leader automates restarting the affected VMs onto other servers in the cluster. By default, VMware HA attempts to restart VMs five times over roughly a 30-minute time span. When you use it in combination with the VMware Distributed Resource Scheduler (DRS) affinity rules, you can configure VMware HA to target nodes in the cluster onto which specific VMs must restart. Combined with VMware HA, VMware DRS controls which servers and, by extension, which Nutanix cluster own a set of VMs.

VMware High Availability Host Isolation

VMware HA uses a process called host isolation to respond to the loss of network connectivity between nodes in a cluster. Host isolation occurs when hosts are running but can neither communicate with other hosts nor ping the configured isolation addresses. Additionally, VMware HA uses datastore heartbeating to help determine the nature of the host failure. If a host stops issuing heartbeats to the configured datastores, the system considers it failed, and it restarts its VMs on other hosts in the cluster.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1629

When the isolated host remains online, you can use one of several options to manage its VM states:

- **Disabled** or **leave powered on** (the name of the option depends on the vSphere version): This default response leaves the VMs running on an isolated host.
- **Power off**: This option turns off all VMs on the isolated host; a hard stop.
- **Shut down**: This option turns off all VMs on the isolated host, assuming VMware tools are installed. If a shutdown isn't successful, the system issues a command to turn off the VMs within five minutes.

VMware High Availability Compatibility List or Matrix

VMware HA monitors which hosts in a cluster contain the required resources (such as network port group or datastore) for restarting VMs. This feature is sometimes called the VMware HA compatibility list or compatibility matrix. VMware HA only attempts to restart VMs against hosts in the cluster that contain the required network and storage resources.

When you use Metro Availability and a network partition or site failure occurs, standby containers go into an inactive state. This inactive state prevents VMware HA from attempting to restart VMs against the standby containers. VMware HA continues to check the state of the containers every minute to update the compatibility list. When the standby containers are promoted, they become locally read and write capable and no longer report as inactive. VMware HA updates its compatibility list and then attempts to restart the VMs against the now-active container, which triggers VMware HA retry counts and retry intervals.

VMware High Availability Admission Control

Admission control ensures that the VMware cluster contains sufficient resources to support VM resource reservations. In the context of Metro Availability, you can use admission control in coordination with VMware HA to ensure that enough resources exist between the two Nutanix clusters to allow VMs to restart in the event of a site failure. Admission control helps guarantee that all VMs can restart against a single Nutanix cluster in the remote site.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1630

VMware Distributed Resource Scheduler

VMware DRS helps balance resource usage across nodes in a cluster. VMware DRS monitors the CPU and memory resources for all hosts in the cluster and can recommend or automatically run VM migrations for load balancing. In Metro Availability configurations, you can avoid automatically moving VMs to nodes in a cluster that own a datastore in a standby state by creating and using VMware DRS affinity rules to ensure that they don't move to specific servers for load balancing or VMware HA restart purposes.

Distributed Resource Scheduler Affinity Rules

VMware DRS affinity rules control the placement of VMs on hosts in a cluster. DRS supports affinity or antiaffinity between groups of VMs and hosts or between individual VMs. Affinity between VMs prompts DRS to attempt to keep the specified VMs running on the same hosts. Antiaffinity for VMs prompts DRS to attempt to keep VMs running on different hosts.

Affinity between a group of VMs and a group of hosts allows DRS to place members of a VM DRS group on members of a host DRS group. DRS enforces affinity based on *must run on* or *should run on* rules. Must run on rules force VMs to always reside on a member of a specific host group. Should run on rules attempt to place VMs on members of the specified host DRS group, but certain conditions, including host failure, can override them.

Antiaffinity between a group of VMs and a group of hosts relies on *must not run on* and *should not run on* rules. Must not run on rules prevent VMs from ever running on members of a specified host group. Should not run on rules attempt to prevent VMs from running on members of a specified host group, but certain conditions, including host failure, can override them.

Metro Availability offers flexibility when deciding whether to use must or should affinity or antiaffinity rules. Using should rules can help automate restarting VMs across Nutanix clusters during a site failure. To avoid automated restarts across Nutanix clusters, use must rules instead.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1631

VMware vMotion

VMware vMotion migrates VMs between physical servers for performance optimization or hardware maintenance without disruption. With Metro Availability, you can live-migrate a VM between a Nutanix cluster with an active container and a Nutanix cluster with the corresponding standby container. Metro Availability with vMotion can help relieve memory or CPU pressure against ESXi hosts in the active cluster without disruption. You can also use it to prepare for site maintenance or disaster avoidance. While running against the standby container, the VM's I/O redirects to the active site, as described in the Standby Containers section. If you need to service VM I/O locally following a vMotion, you must promote the standby container. The Operational Scenarios section offers more detail concerning the use of vMotion with Metro Availability. The following figure shows a representation of how Metro Availability operates with vMotion.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1632

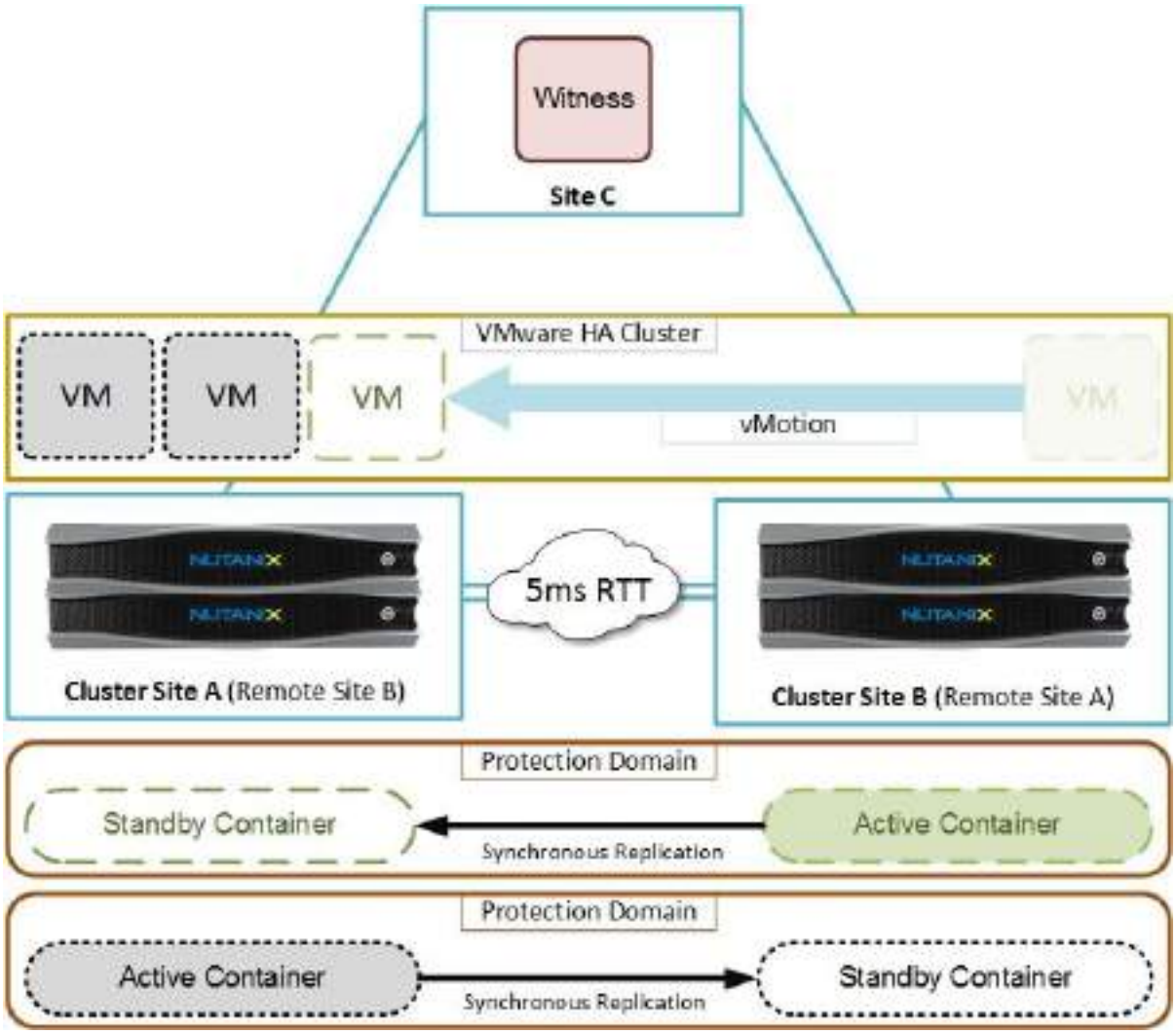


Figure 7: Metro Availability Overview with vMotion

VMware vCenter Server

VMware vCenter Server offers centralized management for VMware environments. With VMware vCenter, you can create clusters, use vMotion, and configure VMware HA and VMware DRS. Metro Availability typically involves a single VMware cluster, and a single vCenter Server instance manages that cluster. You must ensure that the vCenter Server is highly available in stretched-cluster environments. While VMware HA isn't dependent

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1633

on the vCenter Server after it turns on, operations such as vMotion and DRS rules aren't available when the vCenter Server is offline.

For an ideal Metro Availability configuration, place the vCenter Server into a fault domain (generally a third site) separate from the active and standby Nutanix clusters. With this structure, you can manage the environment if either the active or standby site fails.

Alternatively, place the vCenter Server in a container that's used for Metro Availability and replicated to the standby site. In such a configuration, you can protect and recover the vCenter Server with VMware HA or as a part of disaster recovery procedures between the Nutanix clusters.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1634

4. Operational Scenarios

Metro Availability provides several methods for managing replication states, including the Prism Element UI, REST API, nCLI, and PowerShell. The following sections outline nondisruptive planned workload migration, manual unplanned failover, and automated unplanned failover. For more information on how to manage Metro Availability from Nutanix Prism, see the Prism Web Console Guide.

Establishing Metro Availability

The initial configuration of Metro Availability involves creating remote sites and containers in both Nutanix clusters. The containers created in each Nutanix cluster mount to their respective ESXi hosts. The containers must have identical names between the clusters, and the round-trip time latency between the remote sites can't exceed 5 ms. You can then create protection domains for each container targeted for replication.

For scenarios including the Metro Availability witness, you must install the witness in a failure domain separate from the Nutanix clusters, and then register the witness with the clusters participating in the Metro Availability relationship.

An administrator can form a single VMware cluster that contains all the nodes from both Nutanix clusters. You can configure VMware HA and VMware DRS rules to manage VM placement policies. We recommend keeping VMs running locally to active containers. You can use VMware DRS affinity rules to ensure that VMs run against cluster nodes that own the active containers. Should run on rules keep VMs running on a specific group of hosts but also allow failover if a site fails. You can use must run on rules to prevent VMs from restarting on different cluster nodes in the event of a site failure.

We provide specific steps for creating containers, remote sites, and Metro Availability protection domains in the Prism Web Console Guide. The following list summarizes the general steps:

1. (Optional) Install the witness VM.
2. (Optional) Register the witness VM with each cluster.
3. Create containers with matching names in both clusters.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1635

4. Create remote sites in both clusters.
5. Create protection domains for the appropriate containers.
6. In vCenter, create a single VMware HA cluster.
7. Configure VMware HA and DRS affinity rules as appropriate.

Planned Failover

Planned failover involves moving VM operations between sites for disaster recovery testing, planned maintenance, and disaster avoidance. In general, complete a planned failover with Metro Availability through vMotion or a cold migration of VMs. When using vMotion, you can migrate VMs nondisruptively between Nutanix clusters. This capability includes nondisruptively promoting standby containers and enabling replication again.

As a part of the overall procedure, you can enable replication again after the promotion of the containers or not at all for certain test scenarios. Resuming Metro Availability from the standby site acts as a reversal of the replication relationship. The process marks the original active container as standby and overwrites its contents with any new writes.

Enabling replication again after a promotion provides the shortest window for resuming the synchronous relationship. Waiting to enable replication again allows you to validate VM operations prior to marking the previous active container as standby. Additionally, if the scenario is to test VM failover and not persist the data in the standby site, you can skip enabling replication from the standby site.

Planned Failover with vMotion

Using vMotion to move VMs to the standby site provides nondisruptive workload migration during planned failovers. Operationally, using vMotion takes more time than a cold migration, as the VM memory state must be transferred across sites.

Planned failover requires a force-promote of the targeted standby container. The force-promote allows a standby container to become active and enables reads and writes to occur against the local cluster. All VMs running against a container must migrate to the secondary cluster prior to promoting the standby container. The force-promote is nondisruptive to VMs running in the standby container. When you force-promote a standby container, the current active container goes into a decoupled state, making the datastore read-only.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1636

Following promotion, if failure handling is configured for manual or automatic resume, you must disable the formerly active site. After the disable operation, resuming Metro Availability from the standby site reverses the replication relationship. With supported AOS versions, witness failure handling doesn't require you to disable the formerly active site. While the formerly active site is decoupled, you can resume it directly from the promoted standby site. The original active container is marked as standby, and any new writes that occur overwrite its contents.

The following list outlines the planned failover process with vMotion when you configure the failure handling setting for manual or automatic resume mode:

1. Update VMware DRS affinity rules.
2. Migrate all VMs from the active site to the standby site with vMotion.
3. (Optional) Take a snapshot from the active site (Site A).
4. Force-promote the standby containers (Site B).
5. Turn off Metro Availability from Site A.
6. Enable replication from Site B.

If you use asynchronous snapshots in combination with Metro Availability, you might need to suspend those schedules prior to issuing a disable command:

```
ncli pd suspend-schedules name=<PDName>
```

Be sure to resume any suspended schedules when you're done:

```
ncli pd resume-schedules name=<PDName>
```

The following list outlines the planned failover process with vMotion when you configure the failure handling setting for witness mode:

1. Update VMware DRS affinity rules.
2. Migrate all VMs from the active site to the standby site with vMotion.
3. (Optional) Take a snapshot from the active site (Site A).
4. Force-promote the standby containers (Site B).
5. Enable replication from Site B.

Manage any asynchronous snapshot schedules as previously noted.

Planned Failover with Cold Migration

Cold migration provides the fastest operational time for performing a planned failover because it cuts out the time that vMotion takes. VMs, however, incur downtime, because

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1637

cold migration from the active to the standby site is an offline operation. The following list outlines the planned failover process with cold migration:

1. Turn off VMs running against active containers.
2. Update VMware DRS affinity rules.
3. Cold migrate all VMs from the active site to the standby site.
4. (Optional) Take a snapshot from the active site (Site A).
5. Promote the standby containers (Site B).
6. Turn off Metro Availability from Site A.
7. Turn the VMs on in Site B.
8. Enable replication from Site B.

With supported AOS versions and witness failure handling, you don't need to perform the disable operation during a planned failover.

Network Outage Between the Nutanix Clusters

When considering the converged networking architecture of the Nutanix platform, a loss of communication between sites generally causes a communication failure between the VMware hosts and the Nutanix clusters. When you lose VMware host communication, the cluster is partitioned into two sites. VMware HA undergoes an election process for the site that lost communication with the VMware HA leader. Both sites have a VMware HA leader and the ability to restart VMs they perceive to fail.

During the network outage, Metro Availability replication becomes degraded (remote unreachable), and the standby datastores become unavailable and enter an inactive state. The lack of site communication also causes datastore heartbeating to fail for partitioned servers from the perspective of the active datastores. When both host communication and datastore heartbeating fail, the leader VMware HA agent attempts to restart VMs.

Before attempting to restart failed VMs, VMware HA ensures that the cluster contains resources available to support the VMs, such as network port groups and datastores. When standby datastores are in an inactive state, VMware HA can't attempt to restart VMs against those containers. VMware HA retry counters don't apply because the servers are no longer on the VMware HA compatibility list. Thus, VMware HA continually

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1638

looks to update its compatibility list so it can restart the VMs after the standby containers become available again.

Any VM running against a standby container when this kind of network outage occurs loses access to its datastore, which is one of the reasons we recommend running VMs locally to their active containers. You can restart these failed VMs on the opposite site, against the active container, as a part of the VMware HA failure detection and VM restart process.

While VMware HA doesn't require VMware vCenter to be available to restart VMs, certain management operations, such as modifying VMware HA or VMware DRS settings (including affinity rules), are affected when the vCenter Server is unavailable. Depending on the location of the vCenter Server instance, you might have limited options for managing the cluster in a degraded state.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1639

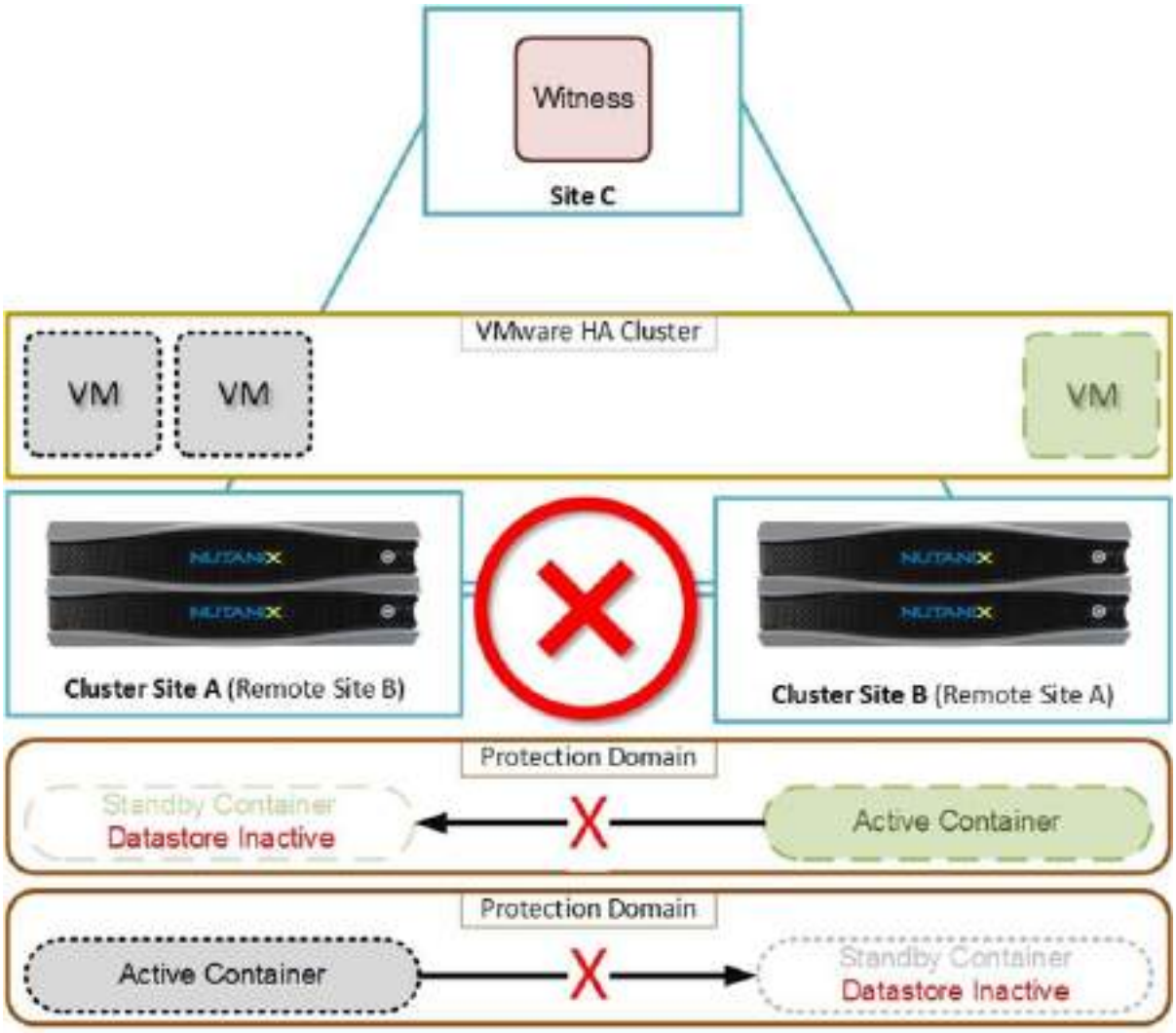


Figure 8: Network Failure Between Nutanix Clusters

VMs running on active containers continue to operate, but the network failure might affect them, depending on the Metro Availability failure handling setting and the duration of the outage.

Network Failure Handling: Manual Mode

With failure handling set to manual, VM writes to the active container don't resume until network connectivity is restored between the clusters or an administrator manually disables Metro Availability. The benefit of this setting is that it enables strict synchronous

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1640

replication between the sites. The downside is that applications in the VMs can time out when writes are held.

Network Failure Handling: Automatic Resume Mode

With failure handling set to automatic resume mode, if network connectivity is restored within the time-out period (10 seconds by default), the replication state immediately returns to enabled and writes continue to replicate synchronously between the clusters. If the time-out period expires, Metro Availability is disabled automatically and writes resume, but they only propagate to the active container. When Metro Availability is disabled, replication to the standby container doesn't occur until both network connectivity is restored and you manually enable it again. The following list summarizes the general process during a network disruption between sites:

1. Hold writes to active containers.
2. Disable Metro Availability from the active sites.
3. Resume writes to active containers.
4. When network connectivity resumes, enable Metro Availability from the active sites.

Network Failure Handling: Witness Mode

With failure handling set to witness, if network connectivity is restored within the time-out period (10 seconds by default), the replication state immediately returns to enabled, and writes continue to replicate synchronously between the clusters. If the time-out period expires, the cluster that owns the active protection domain attempts to acquire the witness lock. If the active protection domain successfully acquires the lock, Metro Availability is disabled automatically and writes resume, but they only propagate to the active container.

During this time, the cluster that owns the standby protection domain also detects the network interruption. After 120 seconds (by default), it attempts to obtain the witness lock. Because the active site already acquired the lock, the standby site fails to obtain it and becomes inactive.

When witness coordination automatically disables Metro Availability, replication to the standby container stops until network connectivity is restored and you manually enable it again.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1641

Site Failure

The surviving site perceives site failure similarly to a complete network outage. Both communications and datastore heartbeating fail, and the VMware HA agent reports a `host failed` state. If required, VMware HA reelects a high availability leader that attempts to restart VMs that are offline because of the site outage.

Metro Availability replication enters a degraded state (remote unreachable), and the standby datastores become unavailable and enter an inactive state. The inactive state prevents VMware HA from attempting to restart VMs against those containers. VMware HA retry counters don't apply because the servers are no longer on the VMware HA compatibility list. As a result, VMware HA continually looks to update its compatibility list so it can restart the VMs when the standby containers become available again.

When the remote site fails, you can promote any standby containers in the surviving site. After they're promoted, the containers become active again to the VMware HA cluster. VMware HA updates its compatibility list and starts VMs that reside in that container. VMware HA automatically overrides VMware DRS should run on affinity rules, and VMs governed by those rules can restart in the surviving site. Must run on affinity rules are enforced, and you must update them so VMs covered by those rules can restart in the surviving site.

Any VM running against a standby container when this kind of network outage occurs loses access to its datastore (one of the reasons we recommend running VMs locally to their active containers). Because the opposite site failed, these VMs can only resume when the standby container is promoted.

While VMware HA doesn't require VMware vCenter to be available to restart VMs, certain management operations, such as the modification of VMware HA or DRS settings (including affinity rules), are affected when the vCenter Server is unavailable. Depending on the location of the vCenter Server instance, options for managing the cluster in a degraded state might be limited.

VMs running against active containers continue to operate, but the site failure might affect them if the Metro Availability failure handling setting is set to manual.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1642

Site Failure Handling: Automatic Resume Mode

With failure handling set to automatic resume mode, site loss causes the break replication time-out to expire in the remaining cluster. Metro Availability is disabled automatically for active protection domains and writes resume against those containers. Containers in standby protection domains become inactive, and you must manually promote them to allow VMs to restart. You must also manually update any VMware DRS rules as required, either to allow VM restart if using must rules or to prevent migration attempts if the failed site and cluster return to service. The following steps summarize the general process during a failure at Site A:

1. Hold writes to active containers (Site B).
2. Disable Metro Availability for active containers (Site B).
3. Resume writes to active containers.
4. Promote standby containers (Site B).

   The VMware HA restart process continues for the DRS should rules.
5. Ensure that vCenter Server is available.
6. Update DRS must rules as required.

   The VMware HA restart process proceeds for the modified must rules.
7. (Optional) To prevent VM movement to the remote cluster, update VMware HA or DRS rules.

Site Failure Handling: Witness Mode

With failure handling set to witness mode, the surviving cluster obtains the witness lock for the active and standby protection domains. Active protection domains are disabled automatically, which allows VM I/O to resume to those containers. Standby protection domains are automatically promoted, making those containers active for I/O. VMware HA then automatically restarts VMs. You must manually update any VMware DRS rules as required to allow VM restart if using must rules or prevent migration attempts if the failed site and cluster return to service.

Site Failure Handling: Witness Mode, Storage Only

A storage-only outage is defined as a condition where the ESXi hosts are running but lose connectivity to the storage. Because the hosts are running, a high availability event isn't triggered. In the event of a storage-only outage on the active site, the witness

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1643

promotes the storage on the standby site. This action puts the storage on the active site in a read-only state because the protection domain is decoupled.

Metro Availability (with a witness) relies on a VMware HA event to start the VMs on the standby site. VM Component Protection (VMCP) helps protect vSphere environments from storage connectivity loss. When a host loses a storage device, VMCP marks it in one of the following states:

- Permanent Device Loss (PDL): A device is marked as permanently lost if the storage array responds with a SCSI sense code marking the device as unavailable.
- All-Paths-Down (APD): If the PDL SCSI code isn't returned from a device, that device is marked as APD. The ESXi host continues to send I/O requests until the host receives a response.

Metro Availability uses VMCP APD implementation to handle storage-only failures. In case of storage-only failure on the primary site, Metro Availability detects the APD condition and automatically fails over the VMs on the affected site to the secondary site after the storage is promoted on the secondary site. In this scenario, the storage on the primary (affected) site is unavailable for reads or writes.

You must enable APD on the ESXi hosts for automatic VM failover to work in this storage-only failure scenario. For more information on configuring VMCP, see the Configuring a Protection Domain (Metro Availability) section of the Data Protection and Recovery with Prism Element guide.

Site Recovery

Site recovery involves returning the environment to its original state by recovering the cluster and resuming replication between the sites. The exact process depends on whether you are recovering an existing configuration or forming a new cluster pairing.

Original Cluster Pairing

In some site failure scenarios, like power loss, you can recover the original cluster and restart the Metro Availability environment using the previous remote site and cluster pairings. The procedures outlined in this section assume you recovered the original cluster in the failed site with the original configuration and data that was available at

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1644

the time of the failure. This procedure also assumes that you promoted all standby containers in the surviving site as described in the Site Failure section.

When you recover a cluster following an outage, Metro Availability validates the state of the protection domain to see if the remote site version diverged. When a standby container is promoted while the active container and cluster are offline, the protection domain on the recovered cluster can report as disabled or decoupled on recovery. An active container reports as disabled if the failure handling setting, when set to automatic, triggers a disable command before cluster failure. If the relationship was not automatically disabled prior to failure, the cluster reports a decoupled state. When the Metro relationship reports as disabled, the container can read and write to the VMware cluster. When the Metro relationship reports as decoupled, the container is in a read-only state.

The Metro Availability witness helps ensure that protection domains in failed sites are unavailable upon recovery. Protection domains come back online in either the standby or decoupled state, preventing VM operation in that cluster.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1645

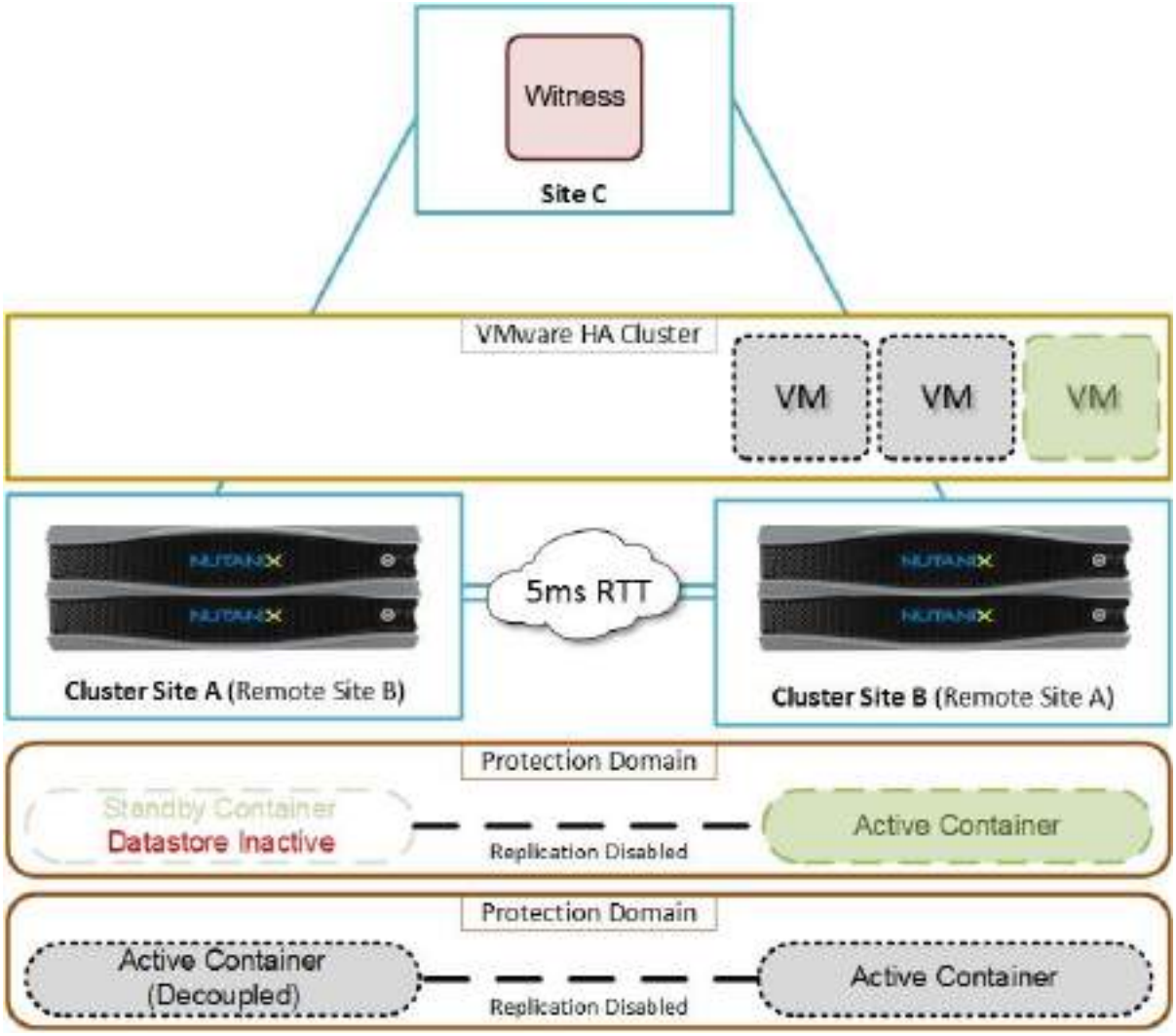


Figure 9: Initial Cluster State Following Site Recovery with Existing Configuration

Prior to recovering a cluster in a Metro Availability relationship that is offline, ensure that VMware DRS settings, including affinity rules, don't cause unwanted VM movement. If you recover a site and cluster, it's possible for legacy DRS settings to attempt to move VMs to unwanted hosts that contain stale data. To prevent this unwanted movement, set DRS to manual or update rules to enforce must not run on requirements temporarily while replication resumes.

To restart Metro Availability after you recover a site, you must disable active protection domains in the recovered cluster if you use manual or automatic resume mode failure

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1646

handling. You can then enable Metro Availability again. When using AOS and witness failure handling, you don't need to disable the active protection domains in the recovered cluster to enable them again from the promoted site. Ensure that you issue the resume operation from the appropriate Nutanix cluster: The site becomes the sole active copy and source of replication. For the example in the previous figure, the resume command comes from Site B. The following steps summarize the general process for site recovery:

1. Update VMware DRS affinity rules to prevent movement to Site A.
2. Recover the cluster from the failed site (Site A).
3. (Optional) Disable any active protection domains at Site A.

   This step is not required with a witness.
4. Enable Metro Availability (Site B).
5. (Optional) To allow movement to Site A, update VMware DRS rules.
6. Wait for synchronization to complete.
7. (Optional) Follow the planned failover process for VMs required at Site A.

If you're using asynchronous snapshots in combination with Metro Availability, you might need to suspend those schedules before you issue a disable command:

```
ncli pd suspend-schedules name=<PDName>
```

Be sure to resume any suspended schedules when finished:

```
ncli pd resume-schedules name=<PDName>
```

New Cluster Pairing

When you completely lose a remote cluster, you need to form a new remote site and protection domain relationship. The steps for this process resemble those for creating a new Metro Availability configuration. Before you enable the new relationship, remove the previous Nutanix cluster nodes from the VMware cluster in vCenter and delete any protection domains and remote sites. After you configure the new cluster intended for Metro Availability, you can establish the new pairing. Use this same process to relocate a Metro Availability relationship between new sites and clusters for migration.

We recommend the following process for moving Metro Availability to a new cluster pairing:

1. Update the VMware DRS rules and groups associated with the nodes that you plan to remove.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1647

2. Remove the nodes from the VMware cluster in vCenter.
3. Delete the protection domains from the existing cluster.
4. Delete the remote sites from the existing cluster.
5. Create containers with matching names on the new cluster.
6. Create remote sites between the new and existing clusters.
7. Create protection domains for the appropriate containers on the existing cluster.
8. Add the new nodes to the VMware cluster in vCenter.
9. Update the DRS rules and groups.

Metro Availability Witness-Specific Workflows

The previous section detailed workflows that are similar whether failure handling is set to manual, automatic resume, or witness. In the following section, we outline a few additional scenarios that are witness-specific.

Witness Failure

In the context of the Metro Availability relationship, the witness is passive; it isn't required for cluster availability or replication when Metro Availability is in a healthy state. A witness can fail, or sites can lose communication with the witness, and Metro Availability replication continues without interruption. Similarly, if a failed witness returns to operation, you don't need to take any additional steps to recover the environment.

The witness-only queries lock status and determine whether to allow an automatic disable or promotion operation for protection domains when communication between the Nutanix clusters fails. If the witness is unavailable, the automatic decision-making fails, affecting VM availability in much the same way as manual failure handling.

If the witness is permanently lost, you must associate the protection domains with a new witness or control protection domain states as needed. With a healthy Metro Availability relationship, you can update the failure handling of the protection domain from witness to another option, such as automatic resume or manual.

Primary Site and Witness Loss

Although very unlikely, it's possible to lose both a primary site and access to the witness. This scenario prevents automatic disabling and promotion of protection domains in the remaining cluster because witness communication is unavailable. You can, however, still

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1648

manage protection domains in the remaining cluster to allow VMs to continue operation. Metro Availability allows you to locally update protection domains to remove witness failure handling. A local failure handling update disassociates protection domains in that cluster from the existing witness, allowing you to manually disable active protection domains and promote standby protection domains. Use the nCLI to perform the local failure handling:

```
ncli pd update-failure-handling name=<PDName> failure-handling=Automatic
 local-only=true
```

Only perform a local failure handling update operation following site loss if you expect the existing witness to be unavailable for an extended period. The following procedure outlines the recovery process in Site B when both Site A and the witness site fail:

1. Update VMware VMware DRS affinity rules.
2. Locally update protection domains to remove witness failure handling.
3. Turn off the active protection domains.
4. Restart the VMs in the active protection domains as needed.
5. Promote the standby protection domains.

   VMware HA recovers the VMs in promoted protection domains.

Primary Site Complete Network Loss

If the primary site completely loses connectivity, a Nutanix cluster can still run in that site but can no longer communicate with its peer Metro Availability cluster or the witness. From the perspective of the opposite site, this situation appears as a complete site loss. In this scenario, using our previous Site A, Site B, and Site C examples, the following process occurs:

1. Site A attempts to contact the witness and fails.
2. All active and standby containers in the Site A cluster become unavailable for I/O.

   Running VMs stop responding.
3. Site B successfully attempts to contact the witness and obtain the lock.
4. In Site B, active protection domains are disabled and standby protection domains are promoted to active, allowing VMs to recover through high availability.

The following diagram captures the resulting state.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1649

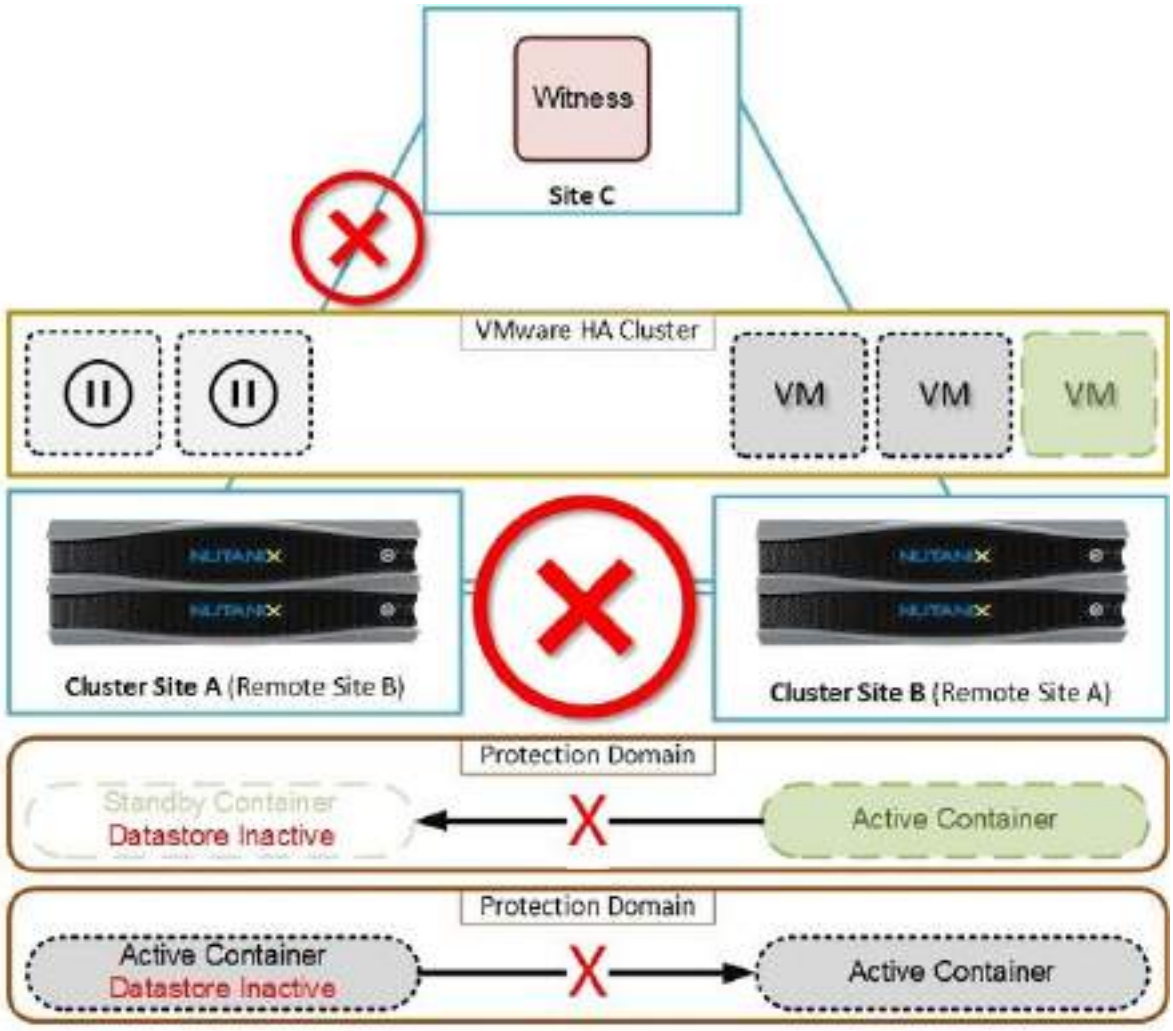


Figure 10: Primary Site Complete Network Loss

Recovering from Complete Network Loss in the Primary Site

If network connectivity is restored, turn off any VMs hanging against the cluster in Site A to recover the Metro Availability relationship. A normal off operation in this state generally doesn't work while the datastore is inactive, but you can use a few options to turn off these unresponsive VMs, including resetting the hosts, disabling the protection domain (making the container active so a normal off operation can proceed), or stopping the active VM process with ESXCLI. After you turn off the VMs, the vSphere cluster

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1650

automatically unregisters them to resolve the conflict. The remaining process for recovering from a complete network loss is similar to recovering from a site loss:

1. Update VMware DRS affinity rules to prevent movement to Site A.
2. Shut down the VMs in Site A.
3. (Optional) Disable any active protection domains in Site A.
4. Enable Metro Availability again in Site B.
5. (Optional) Update DRS rules to allow movement to Site A.
6. Wait for synchronization to complete.
7. (Optional) Follow the process outlined in the Planned Failover section for required VMs in Site A.

Rolling Failure

A rolling failure entails communication loss first between Site A and Site B followed by the complete loss of Site A. During the initial failure between Site A and Site B, the cluster that owns the active protection domain attempts to acquire the witness lock. If the active protection domain successfully acquires the lock, Metro Availability turns off automatically and I/O resumes.

During this time, the cluster that owns the standby protection domain also detects the network interruption and, after 120 seconds (by default), attempts to obtain the witness lock. Because the lock was already acquired by the active site, the standby site fails to obtain it, and the standby container becomes inactive.

The rolling failure continues and Site A is then lost. Because Site B was initially unable to obtain the witness lock, the standby protection domains remain in an inactive state, unable to serve VMs. You must locally update failure handling of any standby protection domains to promote them to active. After you promote these domains, VMs can restart using the high-availability recovery process. Perform the local failure handling update as described in the Primary Site and Witness Loss section.

Operational Scenarios Summary

The following table provides an overview of possible scenarios based on the failure handling setting. The table assumes a basic starting configuration in which Site A contains only active protection domains and Site B contains only standby protection domains.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1651

Table: Failure Scenario Summary

Failure Scenario	Witness Mode	Automatic Resume Mode	Manual Mode
Site A outage or complete network failure in Site A	Automatic protection domain promotion in Site B. VMs automatically restart in Site B.	You must promote protection domains in Site B for VMs to restart.	You must promote protection domains in Site B for VMs to restart.
Site B outage or complete network failure in Site B	VMs continue to run on Site A following an automatic disable of protection domains.	VMs continue to run on Site A following an automatic disable of protection domains.	VMs are paused, and you must disable protection domains in Site A.
Connection loss between Site A and Site B	VMs continue to run on Site A following an automatic disable of protection domains.	VMs continue to run on Site A following an automatic disable of protection domains.	VMs are paused, and you must disable protection domains in Site A.
Witness failure	No impact while the Metro Availability relationship is healthy.	N/A	N/A
Connection loss between witness and Site A	No impact while the Metro Availability relationship is healthy.	N/A	N/A
Connection loss between witness and Site B	No impact while the Metro Availability relationship is healthy.	N/A	N/A
Connection loss between witness and both Site A and Site B	No impact while the Metro Availability relationship is healthy.	N/A	N/A
Connection loss between Site A and Site B and between witness and Site A	VMs on Site A are paused. Automatic protection domain promotion in Site B. VMs automatically restart in Site B.	VMs continue to run on Site A following an automatic disable of protection domains.	VMs are paused, and you must disable protection domains in Site A.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1652

Failure Scenario	Witness Mode	Automatic Resume Mode	Manual Mode
Connection loss between all sites, including the witness (Site A recovery)	VMs on Site A are paused. You must update failure handling in Site A and disable protection domains to resume VMs.	VMs continue to run on Site A following an automatic disable of protection domains.	VMs are paused, and you must disable protection domains in Site A.
Connection loss between all sites, including the witness (Site B recovery)	You must update failure handling in Site B and promote protection domains in Site B for VMs to restart.	You must promote protection domains in Site B for VMs to restart.	You must promote protection domains in Site B for VMs to restart.
Rolling failure: Metro Availability failure followed by Site A failure	You must update failure handling in Site B and promote protection domains in Site B for VMs to restart.	You must promote protection domains in Site B for VMs to restart.	You must promote protection domains in Site B for VMs to restart.
Storage-only outage on Site A	The witness promotes the storage on Site B. The storage on Site A becomes inaccessible. If you enabled VMCP for APD, VMs fail over to Site B.	All VMs pause until you fix the storage outage or manually promote the storage on Site B. After you promote storage on Site B, manually migrate VMs by generating a VMware HA event.	All VMs pause until you fix the storage outage or manually promote the storage on Site B. After you promote storage on Site B, manually migrate VMs by generating a VMware HA event.

Asynchronous Snapshot Workflows

Nutanix supports the use of local and remote snapshots in combination with Metro Availability. You can schedule snapshots between the clusters used for Metro Availability and to a third cluster outside of the Metro Availability relationship (VMware ESXi only), as shown in the following figure.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1653

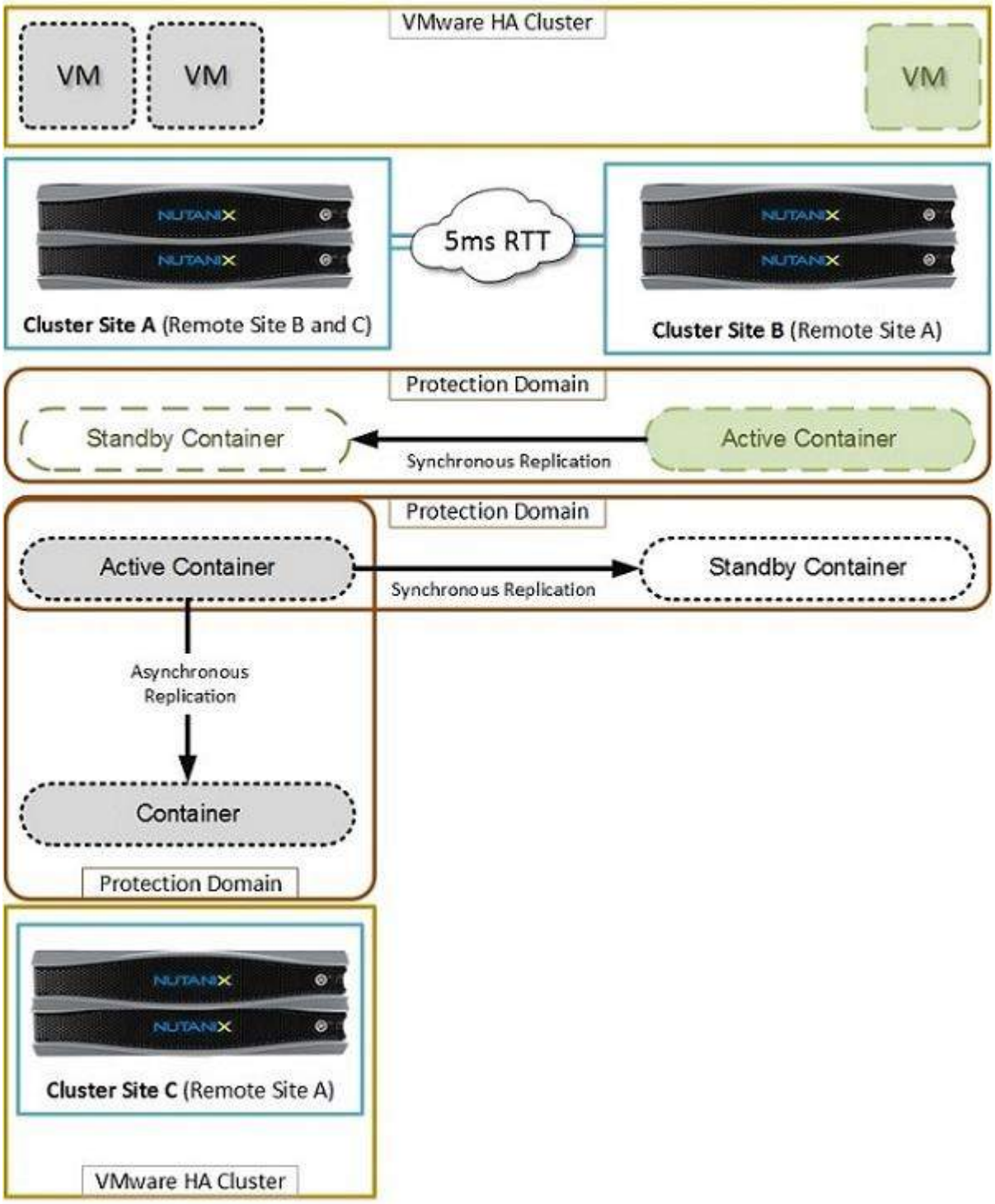


Figure 11: Metro Availability Three-Site Configuration

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1654

Snapshots for Metro Availability–enabled protection domains occur at the container level, which means that each snapshot operation captures all files in the container. By default, the system takes a snapshot every four hours to create a checkpoint used for incremental resynchronization if the Metro relationship becomes disabled. The default snapshot interval with AOS is six hours.

Snapshot Scheduling

You can take snapshots intended for backup and restoration manually or configure them in a schedule. Configure a schedule against the cluster that contains the Metro Availability protection domain in the active state. You can use Nutanix Prism to establish schedules that create local snapshots in both the source and target Metro Availability clusters. Optionally, you can select a third remote site to retain snapshots outside of the Metro Availability relationship.

Snapshot Restore

Snapshots are restored in the active Metro Availability protection domain or in three-site scenarios against the asynchronous protection domain. You cannot restore snapshots in the cluster that hosts the standby Metro Availability protection domain. A snapshot contains all files in the protection domain. Because the restoration process recovers all files, use a redirected restore. A redirected restore recovers the files to a subdirectory in a container, preventing you from overwriting any active files. Perform restores from the nCLI using the following steps:

1. Obtain the snapshot ID.

   For example, to obtain the snapshot ID for a protection domain called `metropd` (using a bash shell), run the following command: `ncli pd ls-snaps name=metropd | grep "Id|Create Time"`.

2. Restore the snapshot with redirection.

   - Example: `ncli pd restore-snapshot name=metropd snap-id=15113205 path-prefix=/temp`
   - If you omit the `path-prefix` parameter, the redirection command automatically creates a folder named `Nutanix-Clone`. Following a restore using the previous example, a `/temp` directory is available in the `metropd` datastore on the ESXi cluster. You can copy any folders and files required for recovery to other locations if necessary.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1655

3. Register the restored VMs by adding the configuration files to inventory.
4. (Optional) If you restore snapshots and register the VMs to a new location, ensure that the VMDK paths for the VMs point to the path specified during the restore operation.
5. Delete all remaining folders and files that were not needed as a part of the restore.

Planned Third Site Failover

In three-site configurations, you can migrate the entire protection domain to the asynchronous remote site (VMware ESXi only). Move the VMs to the third site using the following steps:

1. (Optional) To shorten migration time, perform an incremental replication.
   - Example: `pd add-one-time-snapshot name=metropd remote-sites=SiteC retention-time=86400`
   - Retention time is in seconds.
2. Shut down the VMs.
3. (Optional) Unregister the VMs.
4. Disable Metro Availability.
5. Migrate the protection domain to the remote site using the nCLI from the active Metro Availability cluster: `ncli pd migrate name=metropd remote-site=SiteC`.
6. Register the VMs in the third site.

Planned Third Site Failback

Perform a planned migration from the third site (VMware ESXi only) back to the active Metro Availability site using the following steps:

1. (Optional) To shorten migration time, perform an incremental replication.
   - Example: `pd add-one-time-snapshot name=metropd remote-sites=SiteC retention-time=86400`
   - Retention time is in seconds.
2. Shut down the VMs in the third site.
3. (Optional) Unregister the VMs in the third site.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1656

4. Migrate the protection domain to the active Metro cluster by running the following nCLI command from the third site cluster: `ncli pd migrate name=metropd remote-site=SiteA`.
5. Perform one of the following actions to manage VM registration and power state:
   - If the VMs remained registered during the planned failover, start them in the active Metro Availability cluster.

     You might be prompted to confirm whether the VM was copied or moved. Selecting **moved** maintains the same UUID for the VM.

   - If the VMs were unregistered during the planned failover, register and start them in the active Metro Availability cluster.

     You might need to enable Metro Availability again so both sides of the relationship have the same view of the datastore.

To complete the process, enable Metro Availability again if you didn't already do so in Step 5.

Unplanned Third-Site Failover

Performing an unplanned failover to the third site (VMware ESXi only) is the worst-case scenario. You can accomplish this task using the following steps:

1. Activate the asynchronous protection domain in the third-site cluster.

   Example: `ncli pd activate name=metropd`
2. Register the VMs in the third site.

Planned Third-Site Failback Following an Unplanned Failover: Original Cluster

The following procedure moves VMs back to an existing Metro Availability configuration following an unplanned failover to the third site:

1. Turn off the VMs in the Metro Availability site.
2. (Optional) Unregister the VMs in the Metro Availability site.
3. Ensure that Metro Availability is disabled.
4. Deactivate the active Metro Availability protection domain.

   Example: `ncli pd deactivate-and-destroy-vms name=metropd`

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1657

5. (Optional) Synchronize changes.
   - Example: `pd add-one-time-snapshot name=metropd remote-sites=SiteA retention-time=86400`
   - Retention time is in seconds.
   - Because Metro Availability clusters are offline, synchronizing changes can shorten migration time.
6. Turn off the VMs in the third site.
7. (Optional) Unregister the VMs in the third site.
8. Migrate the protection domain to the active Metro Availability cluster by running the following nCLI command from the third-site cluster: `ncli pd migrate name=metropd remote-site=SiteA`.
9. Perform one of the following actions to manage VM registration and power state:
   - If VMs remained registered during the planned failover, start them in the active Metro Availability cluster.

     You might be prompted to confirm whether the VM was copied or moved. Selecting **moved** maintains the same UUID for the VM.
   - If the VMs were unregistered during the planned failover, register and start them in the active Metro Availability cluster.

     You might need to enable Metro Availability again so that both sides of the relationship have the same view of the datastore.

To complete the process, enable Metro Availability again if you didn't already do so in Step 9.

Planned Third-Site Failback Following an Unplanned Failover: New Cluster

The following procedure moves back to a new Metro Availability configuration following an unplanned failover to the third site:

1. Recreate the Remote Sites and Metro Availability relationship in the new clusters.

   Be sure to use the same container name and protection domain name as in the third site.
2. Disable Metro Availability.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1658

3. Deactivate the active Metro Availability protection domain.

   Example: `ncli pd deactivate-and-destroy-vms name=metropd`
4. (Optional) To shorten migration time, perform the initial full replication.
   - Example: `pd add-one-time-snapshot name=metropd remote-sites=SiteA retention-time=86400`
   - Retention time is in seconds.
   - Although this step is optional, we recommend that you perform the initial full replication.
5. Shut down the VMs in the third site.
6. (Optional) Unregister the VMs in the third site.
7. Migrate the protection domain to the active Metro Availability cluster by running the following nCLI command from the third-site cluster: `ncli pd migrate name=metropd remote-site=SiteA`.
8. Enable Metro Availability.
9. Register the VMs and start them in the active Metro Availability cluster.

Site Recovery Manager Third-Site Support

The Nutanix Storage Replication Adapter (SRA) for Site Recovery Manager (SRM) supports replication, test, and failover automation between the active Metro Availability cluster and an asynchronous third site. The Storage Replication Adapter for Site Recovery Manager Administration Guide outlines the required configuration and operational steps with the following considerations:

- You don't need to issue a vStore protect command in any site.
- You must configure a vStore mapping between the cluster with the active protection domain and the cluster at the third site. Don't configure a vStore mapping between the cluster with the standby protection domain and the third site.
- To continue third-site replication on failover, add the vStore mapping after promoting a standby protection domain to active and remove the mapping from the previous active side. Reconfigure the protection domain replication schedules.
- SRM test workflows are supported while Metro Availability is enabled.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1659

- SRM planned recovery workflows require that you disable Metro Availability. These workflows include the following scenarios:
  - Failover between the active Metro Availability cluster and the third-site cluster
  - Replication from the third-site cluster to the active Metro Availability cluster
  - Failback from the third-site cluster to the active Metro Availability cluster
- Ensure that you enable Metro Availability again after the failback operations.

We recommend performing SRM recovery workflows without promoting the standby Metro Availability cluster.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1660

5. Metro Availability Best Practices Checklist

This section summarizes the Metro Availability best practices in the following categories:

- Requirements
- Interoperability
- Limitations
- Nutanix recommendations
- VMware recommendations

Requirements

- Use a 5 ms round-trip time latency maximum between active and standby Nutanix clusters.

  The system validates this setting during Metro Availability protection domains configuration.

- Active and standby container names must be identical between clusters.

  The system validates this setting during Metro Availability protection domains configuration.

- Datastore names must be the same as the container name.
- Ensure that all virtual disks associated with a VM reside on a container that is enabled for Metro Availability.

Interoperability

- The NX-2000 series isn't supported.
- You can create local and remote snapshots between the Metro Availability–enabled containers. You can configure a third Nutanix cluster to be the target for remote asynchronous replication.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1661

- Cluster configuration:
  - Cluster models can be different between active and standby sites.
  - vMotion might require Enhanced vMotion Compatibility (EVC).
  - Cluster resource sizes can be different.
  - Redundancy factor can be different.
- Container-specific settings, such as compression and replication factor, can be different.
- Don't enable a proxy on remote sites that you use with a Metro Availability protection domain.
- When linked clones are in a Metro Availability container, the gold image must reside in the same container.

Limitations

- Prior to AOS 5.17, Metro Availability performed a snapshot every four hours, which is supported in nodes with up to 80 TB HDD tiers. With AOS 5.17 and later versions, the default snapshot interval is six hours, which enables support for nodes with up to 120 TB HDD tiers. If you use a version before 5.17, you can modify the default snapshot schedule if needed to support denser nodes.
- Before you enable Metro Availability on a container with VMs in an asynchronous disaster recovery protection domain, delete the asynchronous disaster recovery protection domain or remove the VMs associated with the Metro Availability container from the protection domain.
- Latency on vDisks might increase during the synchronization between two clusters.
- If you disable Metro Availability, I/O from the standby site can't be forwarded to the primary site. Commands run on the hypervisors on the standby site might take additional time to run because the hypervisors can't access the underlying storage.
- Restoring snapshots of a Metro Availability protection domain with overwrite isn't supported.
- Symbolic links and hard links aren't supported.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1662

- You can't host VMs on the secondary cluster during the Metro Availability enable operation for the same container.
- You can't host VMs on the primary cluster during promotion of the secondary site for the same container.

Nutanix Recommendations

- Use redundant remote replication links between clusters.
- Maintain similar performance characteristics between the clusters used for Metro Availability:
  - Similar number of nodes
  - Similar server memory configuration
  - Similarly sized oplog
  - Similar drive count for oplog draining to the extent store
- Maintain adequate bandwidth to support peak write workloads.
- Run VMs locally to the active container where their data resides.
- Place no more than 3,600 files into a Metro Availability–enabled container. For more information, see the Alerts section.
- Use the Nutanix Metro Availability witness where the AOS version is 5.0 or later.
- Create no more than 50 protection domains in a Metro Availability cluster pair configured for witness failure handling.
- Use 200 ms round-trip latency or less between the witness and the Nutanix clusters participating in Metro Availability.
- Use Nutanix alerts to monitor Metro Availability replication health.
- Enable remote site compression in bandwidth-limited environments.
- Manually take a snapshot of the protection domain before you disable Metro Availability to ensure the most efficient synchronization when you reenable Metro Availability.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1663

VMware Recommendations

- Most Metro Availability configurations assume a layer 2 network across the two sites, but layer 2 isn't a requirement.
  - › Layer 3 is sufficient to enable Metro Availability, VMware vMotion, and VMware HA restart capabilities. For example, the Nutanix nodes in site 1 can be on network 192.168.10.0/24, while the Nutanix nodes in site 2 can be on 172.16.10.0/24.
  - › Layer 2 helps enable seamless network failover for VMs with static assignments.
- Make the VMware network port group names identical between the VMware hosts in each Nutanix cluster.
- Use a single ESXi cluster spanning the two Nutanix clusters in each site.
- Use a single vCenter Server instance to manage the VMware clusters between sites.
  - › Ideally, maintain the vCenter Server in a third site to allow cluster management regardless of site failure.
  - › Metro Availability can also protect and replicate the vCenter Server if a third site isn't available.
- Configure DRS affinity rules such that VMs aren't migrated to hosts on the cluster that owns the standby container.
  - › Use should affinity rules to allow automated VM restart on nodes that own the standby datastore.
  - › Use must affinity rules to avoid automated VM restarts against the standby datastore.
  - › Manually modify must rules to allow VMs to restart against blocked hosts. Modifying rules assumes the availability of the vCenter Server.
- Configure VM restart priorities as appropriate for the applications running in the environment.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1664

- Configure VMware HA with the following settings:
  - Change the VM restart priority of all CVMs to **disabled**.
  - Change the host isolation response of all CVMs to **leave powered on** or **disabled**, depending on the version of vSphere you are using.
  - Modify user VMs as appropriate. The general recommendation for user VMs is to choose **shutdown**.
  - Change the VM monitoring setting for all CVMs to **disabled**.
- Configure datastore monitoring:
  - Choose **Select only from my preferred datastores** and select the datastores used for Metro Availability.
  - If the VMware cluster contains only one datastore, add the advanced option: `das.ignoreInsufficientHbDatastore=true`.
- Configure VMware HA admission control based on the cluster configuration.
  - Assuming a balanced configuration, one option is to set **Percentage of cluster resources reserved as failover spare capacity** to 50 percent or lower. This setting ensures that enough resources exist in a single Nutanix cluster to support both sites.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1665

6. Metro Availability Detailed Best Practices: Nutanix Cloud Platform

This section builds on the Metro Availability Best Practices Checklist section and offers Nutanix-specific guidance.

Acropolis Upgrade

Nutanix supports upgrading Metro Availability–enabled clusters online without pausing steady-state or resynchronizing replication traffic. We recommend upgrading one cluster in the Metro Availability relationship at a time. After you upgrade the first cluster, the second cluster can follow.

Networking Performance and Availability

Because Metro Availability is a synchronous replication solution, VM write performance typically falls below that observed in standalone environments. The level of performance impact depends on the round-trip latency that exists between the two Nutanix clusters and the total bandwidth available for performing the replication between sites.

Metro Availability is qualified and supported in environments that have up to 5 ms round-trip latency time between the Nutanix clusters. Bandwidth requirements depend on the total concurrent write workload of the active containers used with Metro Availability. If you choose to run VMs against standby containers, the total read workload for those VMs also impacts the total bandwidth requirement.

We recommend enabling compression for the synchronous remote write operations to reduce the total bandwidth required to maintain the synchronous relationship. Compression can also reduce the bandwidth required to perform synchronizations when establishing new protection domains or during other operational procedures.

For performance and redundancy, we recommend using at least two network circuits between the Nutanix clusters and a layer 2 network between the sites to stretch the

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1666

subnets between the two clusters. A stretched subnet allows seamless VM failover when using VMware HA and the existing IP addresses for each VM.

Cluster Hardware Configuration and Sizing

Metro Availability is a flexible solution that doesn't require identical hardware between the two Nutanix clusters. While Metro Availability doesn't enforce exact configurations, the best practice is to ensure a balanced configuration between the two sites. In the context of an active-passive cluster, where VMs only run in one cluster at a time, a balanced configuration ensures that replication performs consistently, wherever the VMs reside. A balanced configuration also makes the same CPU, memory, and storage resources available in both sites, so VM performance is consistent when running in either cluster. Additionally, a slower standby cluster (with a smaller oplog or fewer drives for oplog draining compared to the active site) can adversely affect the write performance of VMs writing to the active container.

A balanced configuration simplifies resource constraint management, including VMware HA admission control configuration. Further, when both clusters offer the same available space between their respective storage pools, free-space monitoring and maintenance are easier. Ideally, a balanced configuration means that containers between both sites hold the same capacity optimization settings so that space consumption is similar between the two clusters.

For environments in which VMs run in both sites and replicate between the two clusters, in addition to maintaining a balanced configuration, we recommend sizing to ensure that all VMs can run in a single site and cluster. This sizing approach means that each of the Nutanix clusters participating in the Metro Availability relationship contains the CPU, memory, SSD, and HDD resources to run all replicated VMs satisfactorily. Otherwise, during site maintenance or failure events that require a single cluster to support the whole environment, performance degrades, and the cluster might operate at higher oversubscription ratios than desired.

Virtual Machine Locality

The platform achieves its best performance when running VMs locally to their respective active containers. When VMs run locally, read performance is similar to non–Metro

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1667

Availability environments, and writes, as previously mentioned, are impacted by a single round trip between the Nutanix clusters.

If a VM runs against a standby container, writes are forwarded to the active container, and additional round-trip latencies occur for the operation. The active site also services reads against the standby container, which causes an additional round trip to service I/O. After it's completed, reads aren’t cached in CVMs hosting the standby container, so any rereads must retrieve the data from the active site again. Because of this additional performance overhead, we recommend running VMs locally to the active containers.

In addition to performance considerations, if a temporary network outage between sites occurs, datastores in VMs running against standby containers can become inactive and unavailable, which causes them to fail and go offline. This possibility further reinforces our recommendation to run VMs locally against their active containers.

Upon deployment, you can automate adding VMs to specific DRS groups using the vSphere API or tools such as the vSphere PowerCLI.

When considering the potential for temporary network outages, we recommend configuring the VM availability setting to automatically disable replication. Otherwise, extended network outages between sites cause running VMs to fail against their active containers. Use a shorter time-out prior to the automatic disable than any application time-outs for the services running in the replicated VMs.

Metro Availability replication to the standby site does not maintain VM-specific data locality to a particular node in the standby cluster. When failing over a VM to the standby cluster and promoting the standby container, any node in that cluster can service local reads. Over time, data becomes resident on the node that owns the running VM. Therefore, you don't need to target a specific node for a VM to use on failover to a promoted standby cluster.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1668

7. Metro Availability Detailed Best Practices: VMware

This section builds on the Metro Availability Best Practices Checklist section and offers VMware-specific guidance.

VMware High Availability Cluster

We recommend configuring a single VMware HA cluster across two Nutanix clusters for use with Metro Availability. One reason to use a stretched-cluster configuration is the operational speed of recovery during unplanned events. The speed at which VMware HA can restart VMs upon container promotion generally outpaces solutions that require you to register and restart VMs across two different VMware clusters.

You can use a separate VMware cluster for each individual Nutanix cluster in combination with the synchronous replication capabilities of Metro Availability. Such a configuration is possible and is officially supported, but it's outside of the scope of this document.

Restart Priorities

You can configure VM restart priorities to control the order in which VMware HA restarts VMs. Setting these priorities can help correctly restart multitiered applications that run across multiple VMs. It’s important to understand that the restart priority is based on turning on the VM and isn't linked to application availability in the VM. Because of this basis, it's possible for lower-priority VMs to be operational before higher-priority VMs.

Isolation Response

The isolation response setting for a Metro Availability environment is only relevant when individual nodes fail, not when a cluster is partitioned. When a cluster is partitioned (as with a network outage between the sites), the nodes local to a site can communicate with each other and respond to VMware HA election traffic. In this case, host isolation doesn't occur.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1669

Host isolation does occur when an individual node fails because of a network outage for that node, and management traffic, including response to either election traffic or the VMware HA leader, also fails. Datastore heartbeating is likely to fail as well, considering the converged networking of the Nutanix platform. Because of this behavior, we generally recommend configuring the isolation response to **shutdown** for any user VMs running on that server. Always set Nutanix CVMs to **leave powered on** or **disabled**, depending on the version of vSphere you use.

Datastore Heartbeating

We recommend configuring datastore heartbeating against containers that mount to all nodes in a VMware HA cluster. When using Metro Availability, configure datastore heartbeating for the stretched containers enabled for replication. Because the single VMware HA leader in the cluster might be operating in either site, you can validate a perceived host failure in the opposite site against the replicated container configured for datastore heartbeating. The additional remote replication traffic caused by enabling datastore heartbeating is minimal and generally not a performance concern.

---

vCenter Server Availability

When using a single VMware HA cluster as recommended, you only need one vCenter Server instance. The vCenter Server is integral to managing the VMware HA cluster; therefore, its placement and availability are of the utmost importance. We recommend making the vCenter Server available in a failure domain separate from the Metro Availability clusters. A separate failure domain generally means a third site with separate connectivity to the two sites that represent the stretched cluster. This design allows the vCenter Server to remain online and be available immediately if either site fails.

If a third site isn't available, you can host the vCenter Server in the Metro Availability environment and replicate it between the sites. You can configure the vCenter Server with should affinity rules to allow automated restart if the site fails.

VMware Distributed Resource Scheduler Affinity Rules

As detailed in the Virtual Machine Locality section, target VMs to run locally against active containers. VMware DRS affinity rules can enforce this requirement. We recommend using should run on rules to keep VMs local to active containers, while also

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1670

allowing VMs to fail over automatically to the standby site in the event of a larger failure. Using should run on rules automates failover and restart after you promote standby containers, so these processes don't depend on vCenter Server availability.

You can use must run on rules, but you need to modify them before you can restart VMs in a site-failure scenario. vCenter Server availability affects your ability to modify the DRS rules, so take it into account when designing the solution.

Update DRS affinity rules in the event of a site failure, either immediately following the failure or before you recover an existing environment. Updating the affinity rules ensures that VMs don't move to a cluster unexpectedly during site recovery procedures to reestablish replication.

The Operational Scenarios and VMware DRS sections contain additional information regarding DRS affinity rules.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1671

8. Utilities and Alerting

This section describes how the following cluster management utilities work with Metro Availability:

- Nutanix REST API
- nCLI and PowerShell commands
- Nutanix Cluster Check
- Nutanix Prism alerts

REST API

The Nutanix REST API allows you to create scripts that run system administration commands against the Nutanix cluster. With the API, you can use HTTP requests to obtain information about the cluster and make changes to the configuration. API commands return JSON-formatted output.

The REST API Explorer section of Nutanix Prism contains a complete list of REST API functions and parameters, including those related to managing Metro Availability.

nCLI Commands

You can download the nCLI from Nutanix Prism and use it to manage the Nutanix cluster. The following list contains the commands relevant to Metro Availability:

- protection-domain | pd
- list | ls
- list-replication-status | ls-repl-status
- create | add
- remove | rm
- metro-avail-enable (includes resume option)

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1672

- metro-avail-disable
- promote-to-active
- update-break-replication-timeout
- update-failure-handling

Example: `ncli pd set-auto-replication-break name=<pd_name> wait-period=15`

We recommend setting `wait-period` to 10 seconds in configurations with four or more nodes

PowerShell Commands

You can download PowerShell commands (referred to as Cmdlets Installer) from Nutanix Prism and use them to manage the Nutanix cluster. The following list contains the commands relevant to Metro Availability:

- Get-NTNXProtectionDomain

  Example:

```
$myPD=Get-NTNXProtectionDomain -name DSHB_PD
$myPD.metroAvail | ft -AutoSize

role   remoteSite container status  timeout
----   ---------- --------- ------  -------
Active POC01b     DSHB      Enabled      10
```

- Promote-NTNXProtectionDomainStretchCluster
- Start-NTNXProtectionDomainStretchCluster

  Maps to enable; includes resume option

- Stop-NTNXProtectionDomainStretchCluster

  Maps to disable

- Update-NTNXProtectionDomainStretchTimeout
- Update-NTNXStretchFailureHandling

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1673

Nutanix Cluster Check

You can perform the following checks when running Nutanix Cluster Check on a Metro Availability–enabled cluster:

- Health_check > Data_protection_checks > Remote_site_checks > Remote_site_connectivity_check

  Checks that the remote sites are reachable.

- Health check > stretch_cluster_checks > backup_snapshots_on_metro_secondary_check

  Checks for snapshots on Metro Availability secondary containers that are candidates for deletion and space reclamation.

- Health check > stretch_cluster_checks > data_locality_check

  Checks whether VMs are operating against data locally.

- Health check > stretch_cluster_checks > secondary_metro_pd_in_sync_check

  Checks whether the secondary protection domain site is synchronized with the primary.

- Health check > stretch_cluster_checks > stale_state_of_secondary_check

  Checks whether the secondary site configuration is stale.

- Health check > stretch_cluster_checks > unsupported_vm_config_check

  Checks to ensure that all VM files are on the same stretched container.

Alerts

Metro Availability might generate the following Nutanix Prism alerts:

Information

If a resume operation requires full resynchronization

Warning

When latency between sites is more than 5 ms for 10 seconds

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1674

When the number of entities in a Metro Availability–protected container exceeds 3,600

When the total number of entities in live containers and associated remote snapshots exceeds 50,000

Metro Availability snapshots automatically fail when a container reaches this threshold. Exceeding 3,600 entities, including snapshots, also prevents you from enabling Metro Availability. Existing synchronous replication continues.

Critical

When a protection domain is in a remote unreachable state

When a protection domain is in a decoupled state

When a protection domain fails to automatically disable

Licensing

If the Ultimate license isn't enabled

Metro Availability requires the Ultimate software edition. If it isn't enabled, you see a license warning while configuring Metro Availability and in the Prism UI after configuration.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1675

9. Conclusion

Metro Availability represents two industry firsts for hyperconverged platforms: the first continuous availability solution and the first synchronous storage replication solution. Managing Metro Availability is simple, intuitive, and built directly into the Nutanix software. The simplified management and operation of Metro Availability stand out compared to the more complex solutions offered with legacy three-tier storage architectures.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1676

About Nutanix

Nutanix offers a single platform to run all your apps and data across multiple clouds while simplifying operations and reducing complexity. Trusted by companies worldwide, Nutanix powers hybrid multicloud environments efficiently and cost effectively. This enables companies to focus on successful business outcomes and new innovations. Learn more at Nutanix.com.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1677

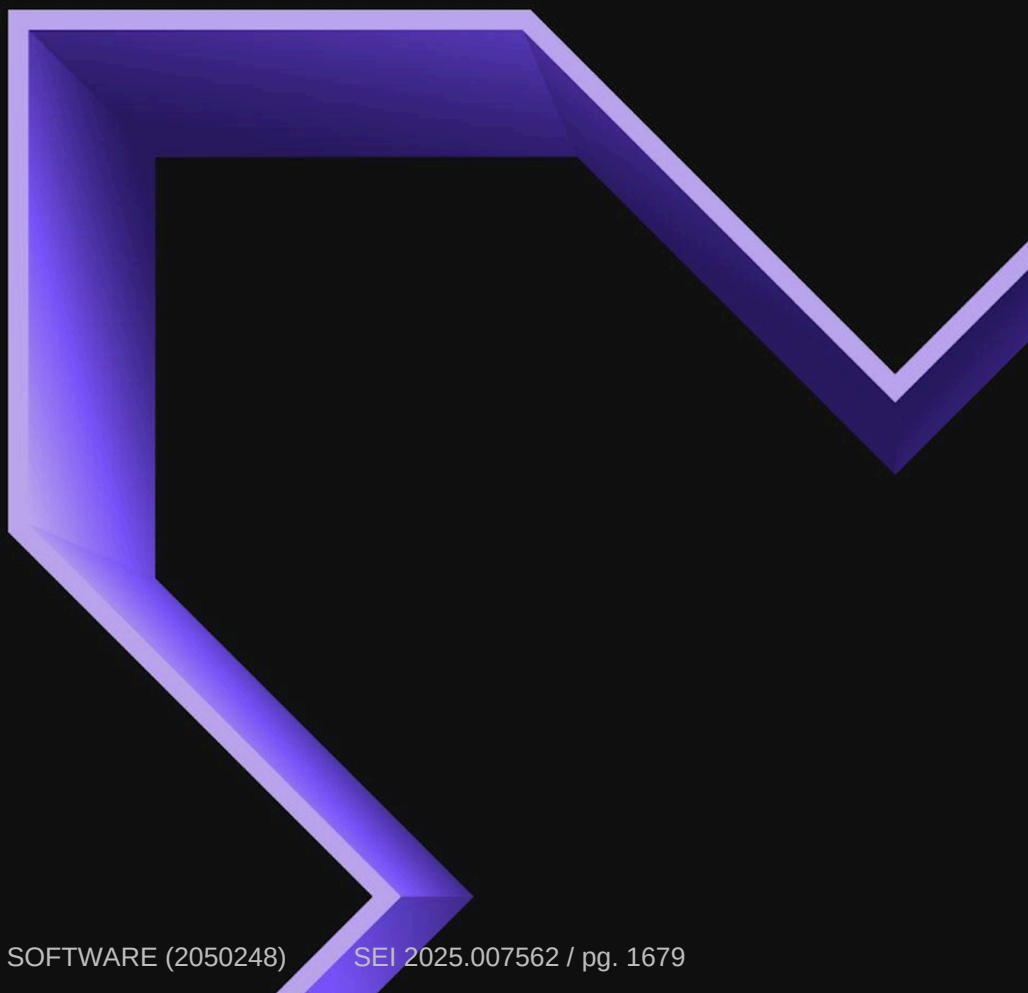
List of Figures

Figure 1: Metro Availability Overview....8
Figure 2: VM Write to an Active Container with Replication Factor 2 at Both Sites....10
Figure 3: VM Write to a Standby Container with Replication Factor 2 at Both Sites....11
Figure 4: VM Read from a Standby Container....12
Figure 5: Active Protection Domain Flowchart....16
Figure 6: Standby Protection Domain Flowchart....17
Figure 7: Metro Availability Overview with vMotion....22
Figure 8: Network Failure Between Nutanix Clusters....29
Figure 9: Initial Cluster State Following Site Recovery with Existing Configuration....35
Figure 10: Primary Site Complete Network Loss....39
Figure 11: Metro Availability Three-Site Configuration....43

v3.0 | January 2025 | BP-2050

SOLUTIONS DOCUMENT

Physical Networking Best Practices



NUTANIX

Legal

© 2025 Nutanix, Inc. All rights reserved. Nutanix, the Enterprise Cloud Platform, the Nutanix logo and the other Nutanix products, features, and/or programs mentioned herein are registered trademarks or trademarks of Nutanix, Inc. in the United States and other countries. All other brand and product names mentioned herein are for identification purposes only and are the property of their respective holder(s), and Nutanix may not be associated with, or sponsored or endorsed by such holder(s). This document is provided for informational purposes only and is presented "as is" with no warranties of any kind, whether implied, statutory or otherwise.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

Contents

1. Executive Summary....4

2. Choosing a Physical Switch....7

3. Network Design Requirements and Recommendations....10

Maximum of Three Switch Hops....10
Same Switch Fabric....10
Wide Area Network Links....11
Multicast....11
VLANs....11
Firewall Best Practices....12
Stretched Layer 2 Networking....13
Rack Awareness and Block Awareness....13
Oversubscription....14
Host Connections....14
Remote Direct Memory Access....16
Breakout Cables....17

4. Nutanix-Recommended Network Designs....18

Leaf-Spine Network Design....18
Core-Aggregation-Access Design....20
Multisite Designs....22

5. Conclusion....24

6. Appendix....25

Physical Networking Best Practices Checklist....25
References....26

About Nutanix....28

List of Figures....29

1. Executive Summary

Nutanix uses modern datacenter network technology to provide a highly available virtualization, compute, and storage platform. The network is a key component in ensuring high performance and availability, and successful Nutanix deployments combine the right physical switches with the right network designs. At the same time, certain physical switches and network designs can lead to poor performance or poor availability, and this guide can help you avoid those risks.

Well-designed networks are central to Nutanix Cloud Platform resilience and performance. A Nutanix cluster can tolerate multiple simultaneous failures because it maintains a set replication factor and offers features like block and rack awareness. However, this level of resilience requires a highly available, redundant network between the cluster's nodes. Protecting the cluster's read and write storage capabilities also requires highly available connectivity between nodes. Even with intelligent data placement strategies, if network connectivity between more than the allowed number of nodes breaks down, VMs on the cluster might experience write failures and enter read-only mode.

To optimize I/O speed, Nutanix clusters send each write to another dynamically selected node in the cluster. As a result, a fully populated cluster sends storage replication traffic in a full mesh, using network bandwidth between all Nutanix nodes. Because storage write latency directly correlates to the network latency between Nutanix nodes, any network latency increase adds to storage write latency.

This best practice guide is part of the Nutanix Solutions Library. We intend it for network and virtualization administrators and architects responsible for designing networks for a Nutanix environment. Readers of this document should already be familiar with top-of-rack networking concepts for datacenter environments and basic hypervisor networking.

This document covers the following topics:

- Choosing physical switches

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1682

- Network design requirements and recommendations:
  - Switch fabric scale
  - VLANs
  - Stretched networks and WANs
  - Oversubscription
  - Rack awareness and block awareness
- Recommended network designs:
  - Leaf-spine
  - Core-aggregation-access (multitier)
  - Multisite designs

Table: Document Version History

Version Number	Published	Notes
1.0	March 2019	Original publication.
2.0	November 2019	QoS and VLAN updates.
2.1	March 2020	Updated the Nutanix Enterprise Cloud Overview and Choosing a Physical Switch sections.
2.2	January 2021	Updated the Choosing a Physical Switch section.
2.3	May 2021	Added spanning tree warning.
2.4	April 2022	Added proxy ARP warning.
2.5	February 2023	Added VLAN scope and flood guidance. Other minor text updates.
2.6	March 2023	Clarified proxy ARP warning.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1683

Version Number	Published	Notes
2.7	April 2024	Updated the Stretched Layer 2 Networking section and added the Remote Direct Memory Access and Multicast sections.
2.8	May 2024	Updated the Choosing a Physical Switch and Maximum of Three Switch Hops sections.
2.9	October 2024	Added the Firewall Best Practices section.
3.0	January 2025	Added the Breakout Cables section.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1684

2. Choosing a Physical Switch

For Nutanix environments, use datacenter switches designed for transmitting large amounts of server and storage traffic at low latency. Don't use switches meant for deployment at the campus access layer. Campus access switches might have 10 Gbps ports like datacenter switches, but they aren't usually made to transport a large amount of bidirectional storage replication traffic.

The deployment size and purpose also influence physical switch choice. Datacenter switches with large buffers are critical in a large AOS cluster that grows beyond eight nodes or hosts storage-intensive applications. In smaller clusters or ROBO deployments that have fewer than eight nodes or don't host write-intensive applications, the switch might not experience buffer contention and you can relax these switch restrictions.

Datacenter switches have the following characteristics:

- Line rate: Ensures that all ports can simultaneously achieve advertised throughput
- Low latency: Minimizes port-to-port latency, measured in microseconds or nanoseconds
- Large per-port buffers: Handle speed mismatch from uplinks without dropping frames
- Nonblocking, with low or no oversubscription: Reduces the chance of drops during peak traffic periods
- 10 Gbps or faster links for Nutanix Controller VM (CVM) traffic

  Only use 1 Gbps links either for additional user VM traffic or when 10 Gbps or faster connections are not available, such as in a ROBO deployment. Limit Nutanix clusters using 1 Gbps links to eight nodes.

The switch manufacturer's datasheets, specifications, and white papers can help identify these characteristics. For example, a common datacenter switch datasheet might show a per-port buffer of 1 MB, while an access layer or fabric extension device has a per-port buffer of around 150 KB. During periods of high traffic or when using links with a speed mismatch (such as 40 Gbps uplinks to 10 Gbps edge ports), a smaller buffer can lead to frame drops, increasing storage latency. While some network designs can achieve high

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1685

throughput and low latency with very small switch buffers, these designs are generally very expensive or specialized environments, such as high-frequency stock trading, that aren't part of a common datacenter network.

The following list isn't exhaustive, but it gives some examples of model lines that meet the requirements for high-performance or large clusters:

- Arista 7050X3, 7160, 7170, 7280: larger buffer models
- Aruba CX 8325 and CX 8360
- Cisco Nexus 9000, 7000, and 5000
- Dell S5200-ON
- HPE FM3810, FM3132Q
- Juniper QFX5100, QFX5200, QFX10K
- Lenovo NE2580O
- NVIDIA Mellanox SN2410, SN2100, and SN2010
- Ruckus ICX 7850 (any variant)

Models similar to the ones listed are also great choices. We recommend using switches like these for large or high-performing clusters, but you can use them for smaller clusters and ROBO as well.

The following are examples of switches that don't meet the high-performance datacenter switch requirements but are acceptable for ROBO clusters and clusters with low performance requirements or fewer than eight nodes. Avoid using these switches for the data path of large or high-performing clusters:

- Arista 7050 and 7150s: smaller buffer models
- Cisco Nexus 3000: smaller buffer model
- Cisco Catalyst 9300 and 9500: campus access switch
- Cisco Catalyst 3850: stackable multigigabit switch
- HPE FM2072
- Ruckus ICX 7550-48F

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1686

The following are examples of switches that are never acceptable for any Nutanix data path connection but are acceptable for out-of-band management:

- Cisco Nexus 2000 (Fabric Extender): highly oversubscribed with small per-port buffers
- 10 Gbps expansion cards in a 1 Gbps access switch: provide uplink bandwidth for the switch, not server connectivity
- Ruckus ICX 7150 models
- Ruckus ICX 8200-24FX

Each Nutanix node also has an out-of-band connection for IPMI, iLO, iDRAC, or similar management. Because out-of-band connections don't have the latency or throughput requirements of VM networking or storage connections, they can use any access layer switch.

> **Note:** Nutanix recommends an out-of-band management switch network separate from the primary network for high availability.

Nutanix maintains close partnerships with several networking vendors. For more information on the network integration and automation capabilities available with Nutanix, review our list of partners in the Networking and Security section of our Technology Alliances page.

Regardless of the switch vendor you choose, follow the general recommendations in this document. For vendor-specific configuration recommendations, see the References section in the Appendix.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1687

3. Network Design Requirements and Recommendations

The following sections contain specific requirements and recommendations for Nutanix network design.

Maximum of Three Switch Hops

Nutanix nodes send storage replication traffic to each other in a distributed fashion over the top-of-rack network. One Nutanix node can therefore send replication traffic to any other Nutanix node in the cluster. Use a network that provides low and predictable latency for this traffic. Nutanix recommends no more than three switches between any two Nutanix nodes in the same cluster. A leaf-spine topology satisfies this recommendation and is a popular choice.

Deployments like the super-spine topology are extensions of the leaf-spine topology in high-performance datacenter networks. If enough bandwidth exists between pods in the super spine to support intracluster traffic and latency is low and consistent across pods, you can deploy a Nutanix cluster across different pods in the same super-spine topology, even though it has more than three switch hops.

Same Switch Fabric

A switch fabric is either a single leaf-spine topology or all switches connected to the same switch aggregation layer. The Nutanix VLAN shares a common broadcast domain in the fabric. Connect all Nutanix nodes that form a cluster to the same switch fabric. Don't stretch a single Nutanix cluster across multiple, disconnected switch fabrics.

Every Nutanix node in a cluster must be in the same layer 2 (L2) broadcast domain and share the same IP subnet.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1688

Wide Area Network Links

A wide area network (WAN) or metro link connects different physical sites over a distance. As an extension of the switch fabric requirement, don't place Nutanix nodes in the same cluster if they're separated by a WAN. When Nutanix nodes are separated by a WAN, create multiple clusters and use disaster recovery replication between sites.

Multicast

AHV treats multicast traffic without IGMP the same as broadcast traffic and forwards it to all end hosts in the VLAN. This process increases the AHV host CPU usage because the multicast packets must be replicated to all attached virtual network interfaces (vNICs) in the VLAN, which can negatively impact cluster operations if the multicast traffic load is high. To handle multicast traffic more efficiently, Nutanix recommends using IGMP snooping in the top-of-rack switches and the Nutanix AHV virtual switches. IGMP snooping tracks the active multicast listeners by listening for IGMP packets and only forwarding the multicast traffic to the end hosts that are interested in it.

To be as effective as possible, configure IGMP at the physical layer and on the AHV hosts:

- To configure IGMP in the physical switches, check with your networking vendor.
- To configure IGMP in the Nutanix virtual switch, see the IGMP Snooping section in the AHV Administration Guide.

Nutanix also recommends VLAN pruning in the physical switches according to the physical switch vendor's best practices. This practice reduces the number of active VLANs to the minimum number required by each host, decreasing unnecessary traffic.

VLANs

To protect the Nutanix CVM and hypervisor traffic, place them together in their own dedicated VLAN, separate from other VM traffic. Don't place the CVM and hypervisor hosts in a VLAN shared with other VMs.

Nutanix recommends that you configure the CVM and hypervisor host VLAN as the native, or untagged, VLAN on the connected switch ports. This native VLAN

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1689

configuration allows easy node addition and cluster expansion while placing traffic in a VLAN when it enters the switch. By default, new Nutanix nodes send and receive untagged traffic. If you use a tagged VLAN for the CVM and hypervisor hosts instead, you must configure that VLAN while you provision the new node, before you add that node to the Nutanix cluster.

Within the Nutanix VLAN, nodes use IPv6 neighbor discovery protocol and IPv6 UDP broadcast messages. To simplify cluster expansion, disable multicast and broadcast flood optimizations that block unsolicited discovery messages in the Nutanix VLAN. Consult your network team before making these changes, as multicast and broadcast flood optimizations can limit potentially harmful traffic. If these protocols are blocked, you can add nodes manually from the command line.

Use tagged VLANs for all guest VM traffic and add the required guest VM VLANs to all connected switch ports for hosts in the Nutanix cluster. Limit VLANs for guest VM traffic to the smallest number of physical switches and switch ports possible to reduce broadcast network traffic load. If you no longer need a VLAN, remove it. Removing unnecessary VLANs helps prevent accidental flooding or excessive broadcast and multicast traffic.

Nutanix AHV network automation streamlines VLAN provisioning for guest VMs. For a list of partners that support network automation, visit the Technology Alliances site and filter on networking and security.

Disable proxy Address Resolution Protocol (ARP) in the Nutanix VLAN before configuring network segmentation and other AHV virtual switch operations. Several Nutanix processes use ARP as a method to detect whether a connection or endpoint is active before proceeding. Proxy ARP replies to all ARP requests and invalidates the results of these checks, causing unexpected failures for operations such as virtual switch updates and other tasks.

Firewall Best Practices

Protect the Nutanix management network with a stateful firewall, and only allow access from known management endpoints.

For more information on the ports required to manage a Nutanix system, see the Ports and Protocols guide.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1690

Stretched Layer 2 Networking

Datacenters have traditionally shared a VLAN with an L2 broadcast domain between different racks. Modern designs sometimes terminate this L2 boundary at the top of the rack so that each rack is a separate L2 domain and a different IP subnet. Because all nodes in a Nutanix cluster must share the same L2 broadcast domain, this approach presents a challenge.

This scenario—stretching an L2 network between two racks in the same datacenter—is the only case when using a stretched L2 network over a layer 3 (L3) network is acceptable for storage traffic within a Nutanix cluster, because the Nutanix cluster is still in the same switch fabric or aggregation layer.

> **Note:** Placing the nodes that make up a Nutanix cluster in multiple datacenters or availability zones connected by stretched L2 networks, or in datacenters that have a remote link between the two locations isn't supported.

When you need compute and storage at multiple sites, use separate Nutanix clusters at each physical location. Use replication tools such as asynchronous disaster recovery, NearSync, and Metro Availability to share data between Nutanix clusters at different sites. These recommendations apply even if the two availability zones share close proximity or highly available network paths. Set up each site as a cluster boundary to protect against network, power, or other failures. The boundary can be a building, a firewall, or even different racks in the datacenter, depending on your availability requirements.

Flow Virtual Networking and Subnet Extension

With Flow Virtual Networking, you can use a Virtual Private Cloud (VPC) to extend the L2 network for user VMs across an L3 boundary. VPCs allow a subnet to exist on multiple Nutanix clusters, even if the clusters are in different L3 subnets. You can't use VPCs to extend the subnet used for Nutanix CVMs.

Rack Awareness and Block Awareness

Block awareness and rack awareness provide smart placement of Nutanix cluster services, metadata, and VM data to help maintain data availability even if you lose an

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1691

entire block or rack. The same network requirements for low latency and high throughput between servers in the same cluster still apply when you use block and rack awareness.

> **Note:** Don't use features like block or rack awareness to stretch a Nutanix cluster between different physical sites.

Oversubscription

Oversubscription occurs when an intermediate network device or link doesn't have enough capacity to allow line rate communication between the systems connected to it. For example, if a single 10 Gbps link connects two switches and four hosts connect to each switch at 10 Gbps, the connecting link is oversubscribed. Oversubscription is often expressed as a ratio—in this case 4:1, as the environment might attempt to transmit 40 Gbps between the switches with only 10 Gbps available. Achieving a 1:1 ratio isn't always feasible, but keep the ratio as small as possible based on budget and available capacity.

In a typical deployment where Nutanix nodes connect to redundant top-of-rack switches, storage replication traffic between CVMs traverses multiple devices. To avoid packet loss caused by link oversubscription, ensure that the switch uplinks consist of multiple interfaces operating at a faster speed than the Nutanix host interfaces. For example, for nodes connected at 10 Gbps, we recommend that the interswitch connection consist of multiple 10 Gbps or faster links.

Host Connections

Connect Nutanix hosts to redundant top-of-rack switches. Use the active-active configuration available in the hypervisor when possible. With vSphere, follow the VMware vSphere Networking best practices, using **Route based on Originating Virtual Port** or **Route based on Physical NIC Load**. With AHV, follow the Nutanix AHV Networking best practices, using either the default active-backup configuration or LACP with balance-tcp.

On switch ports that face Nutanix hosts, designate the interfaces as spanning tree edge ports to minimize port downtime and prevent triggering spanning tree topology changes.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1692

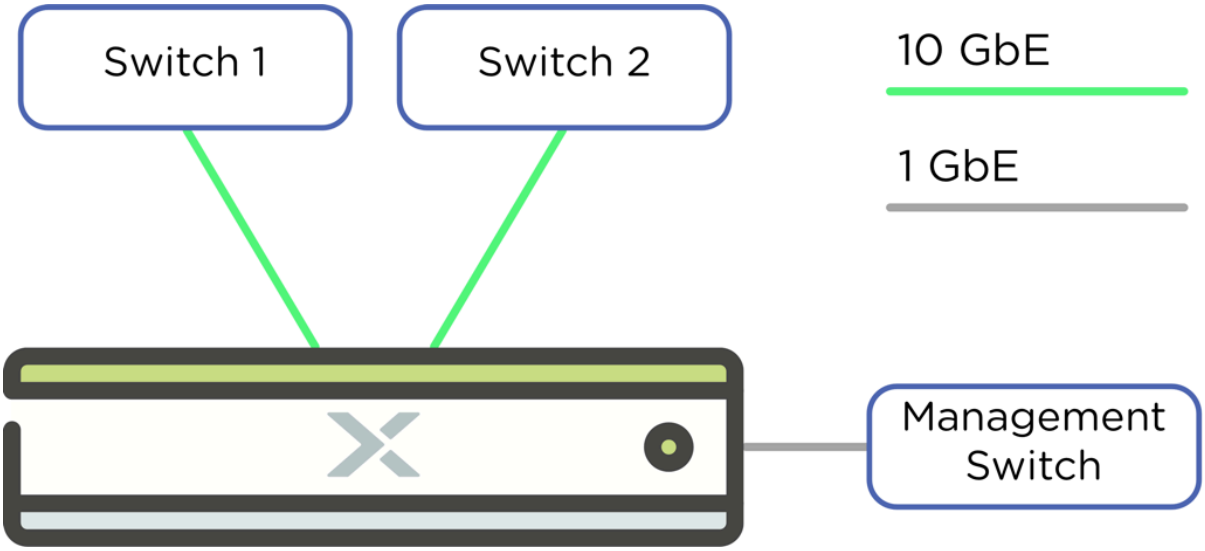


Figure 1: Host Network Connections

Quality of Service

When the network experiences traffic contention, quality of service (QoS) prioritizes traffic and reserves network resources for certain classes of traffic. QoS can mark important traffic with priority values or enable network switches to derive the traffic's class based on fields inside the traffic. After you define traffic classes, each network device can reserve resources for certain classes or decide which classes to prioritize and which to drop.

With a fabric that eliminates contention for storage traffic, you don't need a QoS configuration. Nutanix doesn't recommend configuring any top-of-rack QoS for storage traffic. Instead, configure a nonblocking, low-latency switch fabric with no oversubscription between Nutanix nodes.

As a precaution, use traffic policing on the physical switch ports to prevent excessive unicast, broadcast, or multicast flooding. The details of this configuration, sometimes called optimized multicast flood, differ between switch vendors, but it uses a pattern that matches all multicast and broadcast traffic. This configuration prevents excessive traffic from outside the Nutanix cluster from overwhelming the switch ports connecting the Nutanix cluster.

Nutanix doesn't recommend that you customize any QoS markings on traffic sourced from the CVM or the hypervisor host. If guest VMs pass frames with L2 class of service

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1693

or L3 differentiated services code point markers on them, these values pass from the hypervisor to the physical switch.

Nutanix AHV doesn't support enforcement for QoS prioritization or reservations. To guarantee available bandwidth for guest VMs in AHV, create an additional virtual switch using a dedicated set of physical adapters. For more information, see the Nutanix AHV Networking best practice guide.

For Network I/O Control (NIOC) recommendations with Nutanix on ESXi, see the Nutanix on VMware vSphere Networking best practice guide. If you need QoS at the hypervisor level, Nutanix recommends using shares without hard limits, so QoS with NIOC only applies when the network experiences contention.

Spanning Tree

In traditional networks, using the spanning tree protocol prevents network loops and enforces a loop-free network switch topology. Not all networks use the spanning tree protocol, but if yours does, treat the switch ports facing Nutanix hosts as server or host ports, sometimes referred to as edge ports. A Nutanix server acts like an end host, not a switch. Nutanix recommends either disabling the spanning tree protocol on the ports facing Nutanix servers or configuring the Nutanix-facing ports with features such as type edge or portfast so that these ports skip the normal spanning tree phases and immediately forward traffic.

> **Note:** Configure switch ports facing Nutanix servers as portfast or type edge. Failure to do so might cause service interruption while switch ports transition through the listening and learning phases, dropping all production traffic for up to 30 seconds during spanning tree topology changes.

Remote Direct Memory Access

Storage replication traffic between Nutanix nodes is transported over TCP/IP by default. For high-performance and low-latency environments, Nutanix supports Remote Direct Memory Access (RDMA) to bypass the TCP/IP stack and send storage replication traffic over a dedicated set of physical adapters between hosts in the same cluster. If the RDMA link fails, traffic falls back to the TCP/IP link.

High availability for the RDMA port and NIC using a second RDMA port and NIC isn't currently supported. If the RDMA port and NIC fail, traffic fails back to the TCP/IP link.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1694

RDMA also usually requires specific support from network switch vendors, typically called lossless ethernet or data center bridging (DCB) or priority-based flow control (PFC) depending on the switch vendor. Consult the switch vendor documentation for specific guidance on how to set up the relevant RDMA-compatible network. Map the PFC identifier value used in the network to the PFC value configured in the Nutanix Prism web interface. The most common value is 3, but you can configure the value. The value in the physical switch must match the value in the Nutanix interface.

AOS versions after 6.7 support Zero-Touch RDMA over Converged Ethernet (ZTR), which doesn't require the special switch configuration described previously because the NICs negotiate directly with each other. ZTR requires compatible Mellanox NICs; for a list of compatible NICs, see NIC Compatibility Matrix for RDMA Features.

In AOS versions after 6.6, you can use RDMA manageability to set up RDMA on NICs in brownfield scenarios after you deploy the cluster. Before AOS 6.6, you could only set up RDMA port passthrough during Foundation.

For more information on RDMA, see RDMA over Converged Ethernet (RoCE).

Breakout Cables

Ensure that the hypervisor host interfaces are connected to different top-of-rack switches when using breakout cables. For example, avoid connecting the same host to switch ports 1/1/1 and 1/1/4 accidentally, as this configuration doesn't provide switch redundancy.

Only certain vendors support breakout cables. When using breakout cables, you must connect the higher-bandwidth side to the switch. No Nutanix platform supports using breakout cables to split a single host interface into multiple upstream switch connections. Always confirm that the cables that you intend to use are supported by the switch manufacturer and the NIC manufacturer. See the relevant manufacturer documentation for your use case.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1695

4. Nutanix-Recommended Network Designs

The following sections contain the network designs recommended by Nutanix.

Leaf-Spine Network Design

The leaf-spine network design is popular in new datacenter deployments because it's easy to deploy and easy to scale after deployment. A leaf-spine topology requires at least two spine switches and two leaf switches. Every leaf connects to every spine using uplink ports. The spine switches have no connections between them in the conventional leaf-spine design; neither do the leaf switches.

Use uplinks that are faster than the edge ports to reduce uplink oversubscription. To increase uplink capacity, add spine switches or uplink ports as needed.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1696

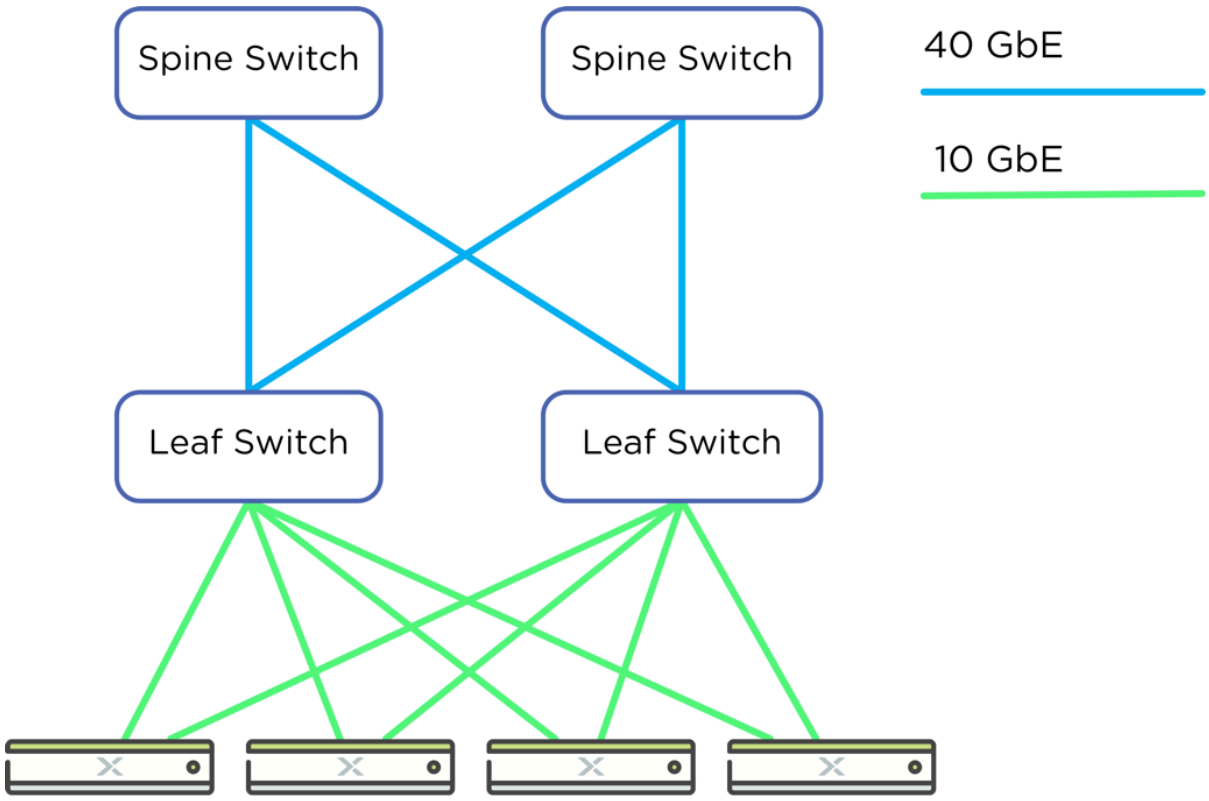


Figure 2: Leaf-Spine Network

To scale the leaf-spine network, add leaf and spine switches. Because there are no more than three switch hops between any two Nutanix nodes in this design, a Nutanix cluster can easily span multiple racks and still connect to the same switch fabric.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1697

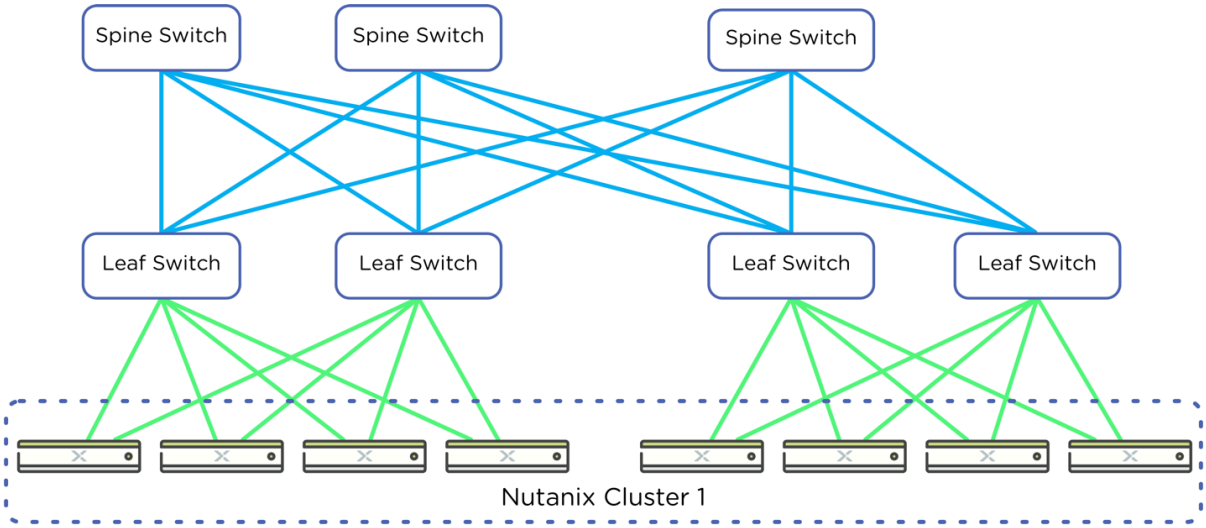


Figure 3: Scaling the Leaf-Spine Network

Core-Aggregation-Access Design

The core-aggregation-access (or three-tier) design is a modular layout that allows you to upgrade and scale layers independently. Ensure that all nodes in a Nutanix cluster share the same aggregation layer to comply with the three-switch-hop rule.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1698

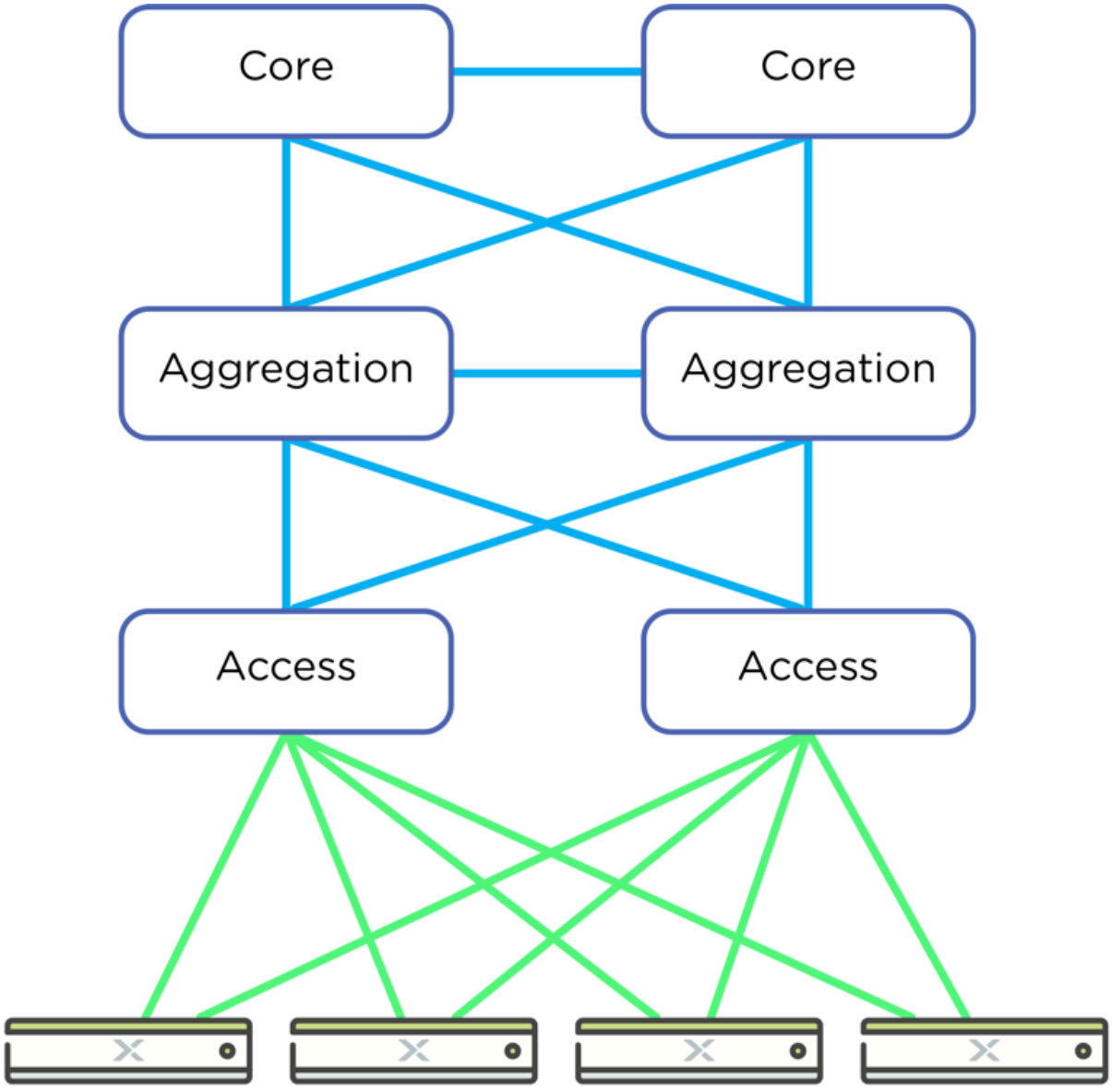


Figure 4: Core-Aggregation-Access Network

Scaling the three-tier network design might require adding another aggregation and access layer to the core, which creates more than three switch hops between the two access layers. Ensure that you add Nutanix nodes in separate aggregation and access layers to separate clusters to keep the number of switch hops between nodes in the

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1699

same cluster to three or fewer. In the following example, Cluster 1 connects to one aggregation layer and Cluster 2 connects to another.

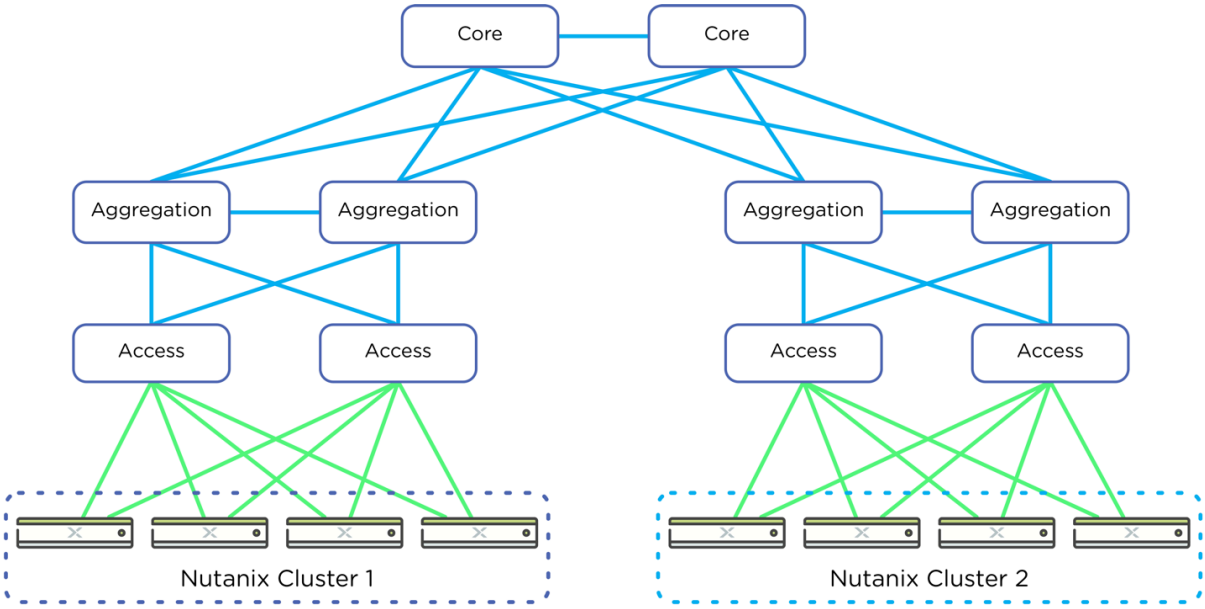


Figure 5: Scaling the Core-Aggregation-Access Network

You can connect switches in many different ways in the three-tier design, so your deployment might look slightly different than the one shown in the previous images.

Multisite Designs

When two or more physical sites or physical availability zones exist, don't use one Nutanix cluster to span them. Instead, create multiple Nutanix clusters (one per availability zone) and connect them with tools such as asynchronous disaster recovery, NearSync, and Metro Availability. This design provides high availability for data and applications and eliminates the possibility of a split-brain scenario in which a Nutanix cluster is partitioned when the two sites lose connectivity.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1700

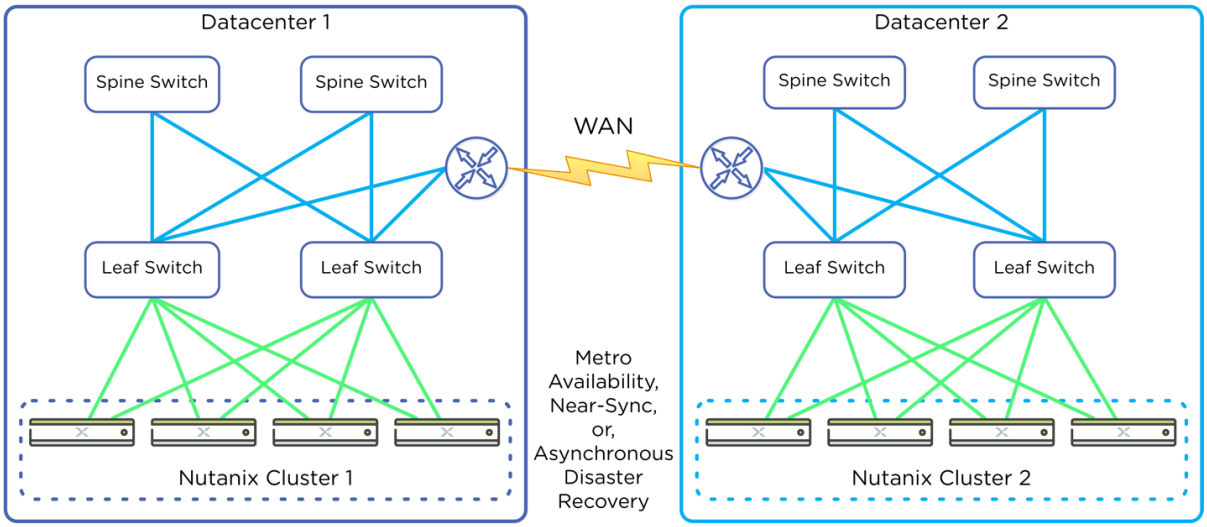


Figure 6: Multisite Network Design Using Replication

© 2025 Nutanix, Inc. All rights reserved

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1701

5. Conclusion

We often talk to customers concerned about the network for their datacenters and their individual Nutanix clusters. Although networking might seem daunting, it requires attention to only three key points:

- Procure the right switches.
- Select the right network design.
- Use the right replication technologies.

If you connect your Nutanix cluster to a well-designed datacenter network, your storage platform can be highly available while still providing you with excellent performance.

For feedback or questions, contact us using the Nutanix Community forums.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1702

6. Appendix

Physical Networking Best Practices Checklist

Follow these physical networking best practices:

- Use a maximum of three switch hops between any two Nutanix nodes in the same cluster.
- Connect all Nutanix nodes in the same cluster to the same switch fabric (leaf-spine network) or aggregation layer.
- Avoid WAN or remote links between Nutanix nodes in the same Nutanix cluster.
- Enable IGMP snooping in both the physical network and the AHV virtual switches when multicast traffic is present.
- Separate Nutanix CVM and hypervisor hosts into a dedicated VLAN that doesn't include any VM traffic.
- After consulting your network team, disable flood optimization in this Nutanix VLAN to allow discovery.
- Trunk only the required VLANs to switch ports facing Nutanix servers and remove all other VLANs.
- Consider policing or flood optimization in non-Nutanix VLANs to prevent excessive broadcast or multicast traffic.
- Disable proxy ARP in the Nutanix VLAN before configuring network segmentation and other AHV virtual switch operations to prevent unexpected failures.
- Don't place Nutanix nodes in the same Nutanix cluster if the stretched L2 network spans multiple datacenters or availability zones or if there is a remote link between the two locations.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1703

- Only use a stretched L2 network over L3 when the Nutanix cluster remains in the same switch fabric or aggregation layer, such as a L2 network stretched between two racks in the same datacenter.

  Nutanix VPCs can stretch the L2 network for user VMs but not for CVMs.

- Don't use features like block or rack awareness to stretch a Nutanix cluster between different physical sites.
- Configure adequate uplinks between switches or interswitch links for east-west storage traffic to minimize port-to-port oversubscription.

  For example, use multiple 40 Gbps or faster uplinks (or interswitch links).

- Connect hosts using redundant links.
- Configure switch ports facing Nutanix servers as spanning tree portfast or edge to skip the listening and learning phases and prevent cluster outages due to spanning tree topology changes.

These requirements and recommendations keep latency between nodes minimal and predictable. Networks that have too many switch hops or introduce WAN links between only some of the nodes introduce variable latency, which negatively affects storage latency, and variable throughput. Networks that are larger than required also add components (datacenters, zones, switches, and switch fabrics) that can all affect availability.

References

1. Data Protection and Disaster Recovery
2. Data Protection for AHV-Based VMs
3. Metro Availability
4. Nutanix AHV Networking
5. VMware vSphere Networking
6. VMware NSX for vSphere
7. Cisco ACI with Nutanix
8. NVIDIA Networking with Nutanix
9. Networking: Arista EOS Recommended Practices

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1704

10. Cisco Nexus Recommended Practices

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1705

About Nutanix

Nutanix offers a single platform to run all your apps and data across multiple clouds while simplifying operations and reducing complexity. Trusted by companies worldwide, Nutanix powers hybrid multicloud environments efficiently and cost effectively. This enables companies to focus on successful business outcomes and new innovations. Learn more at Nutanix.com.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1706

List of Figures

Figure 1: Host Network Connections..... 15
Figure 2: Leaf-Spine Network..... 19
Figure 3: Scaling the Leaf-Spine Network..... 20
Figure 4: Core-Aggregation-Access Network..... 21
Figure 5: Scaling the Core-Aggregation-Access Network..... 22
Figure 6: Multisite Network Design Using Replication..... 23

HDD/SSD Replacement (Dual SSD Platforms)

Platform ANY

NX-1065-G9/NX-3035-G9/NX-3060-G9/NX-3155-G9/ NX-8150-G9/NX-8155-G9/NX-8155A-G9/NX-8170-G9

October 10, 2024

NUTANIX

Contents

Drive Replacement 3
- Replacing Hardware Components in a Block 3
- Drive Slot Numbering 3

Physically Replacing a Drive 5
- Summary: Replacing an SSD or HDD 5
- SSD or HDD Failure Indication 5
- Replacement Prechecks 7
- Preparing to Replace an SSD or HDD 8
- Physically Replacing an SSD or HDD 10
- Completing SSD or HDD Replacement 17
- Replacement Post Checks 21

Upgrading SSDs to a Higher Capacity 23

Copyright 25

DRIVE REPLACEMENT

Replacing Hardware Components in a Block

This section provides general information about Nutanix hardware component replacement.

> **Note:** For tool-less component replacement, such as drive, AIOM, PSU, etc., you do not need the tools listed in this section.

Tools and supplies required:

- Antistatic wrist strap
- Phillips screwdriver (#2)
- Torque screwdriver

The following table provides the recommended torque values for various components. Use the torque values provided in the table to prevent any potential damage to the components.

Table 1: Recommended Torque Values

Component	Torque (in-lb)
Chassis cover screws	7.0 +/- 1.0
NIC bracket screws	7.0 +/- 1.0
M.2 drives screws	5.6 +/- 0.8
Chassis rail mount screws (M5 fastener)	20.0 +/- 2.0

> **Warning:**
>
> A qualified service technician must perform all services. To avoid ESD damage to the component or system, wear a grounding wrist strap. Handle all components with care: Place them on soft, static-free surfaces.
>
> Coordinate service with the customer for any operation that involves the hypervisor host (ESXi or AHV), virtual machines, or Nutanix software.
>
> If you locked down the cluster or hypervisor, you must enable SSH access again. For more information, see the *Cluster Access Control* topic in the *Web Console Guide*.

Return failed components to Nutanix. For the replacement parts, follow the instructions provided on the box. If the instructions are missing or you have other questions, call the Nutanix returns department at 1-866-884-7958 in the US or +1-508-623-1040 international.

> **Note:** Nutanix does not provide a warranty or support services for non-Nutanix components, and any problems arising from your use of non-Nutanix components are expressly excluded from the Nutanix warranty and support terms. If you replace or modify Nutanix components or install non-Nutanix components, you do so at your risk.

Drive Slot Numbering

The following figures provide drive slot numbering for Nutanix G9 platforms.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1710

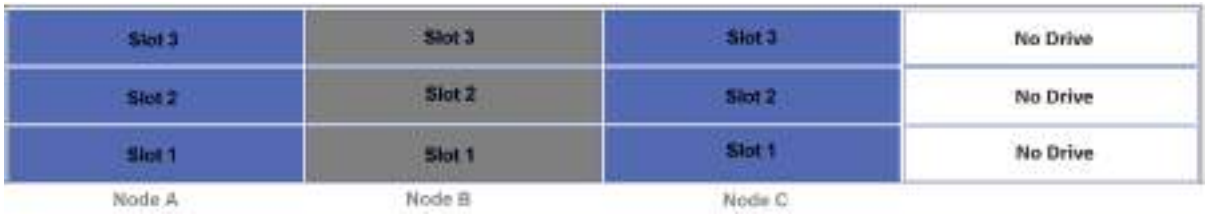


Figure 1: Drive Slots - NX-1065-G9

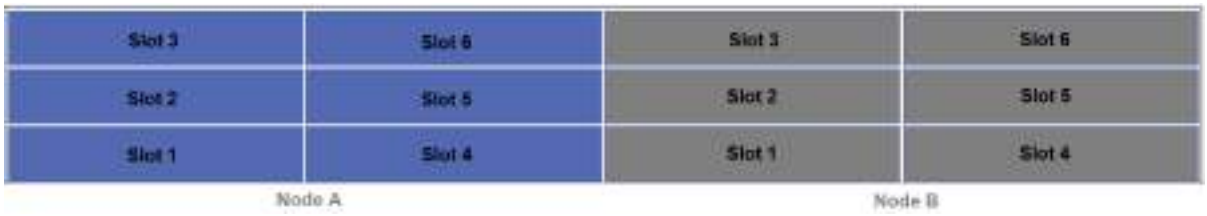


Figure 2: Drive Slots - NX-3035-G9

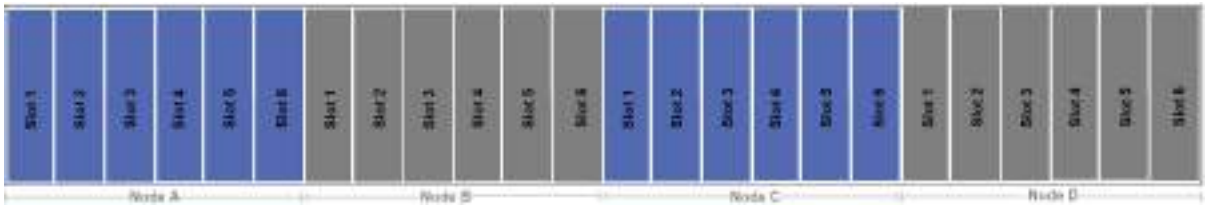


Figure 3: Drive Slots - NX-3060-G9

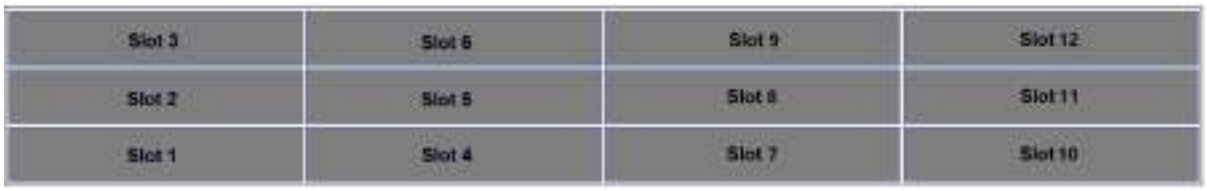


Figure 4: Drive Slots - NX-8155-G9/NX-8155A-G9

Figure 5: Drive Slots - NX-8170-G9

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1711

PHYSICALLY REPLACING A DRIVE

Summary: Replacing an SSD or HDD

About this task

Use this procedure to replace any drive that has a data partition, including metadata and Controller VM boot drives.

Nutanix supports hot-swapping of drives. Node shutdown is not required for replacing a failed drive.

Upgrading SSDs to a Higher Capacity

- On platforms that use versions of Nutanix AOS earlier than 6.0, all SSDs in a node must have the same capacity.
- Platforms that use AOS 6.0 or later allow mixing of SSDs with different capacities in the same node, for replacement cases where only higher-capacity SSDs are available.
  - If you mix SSDs of different capacities, the node treats the higher-capacity SSDs as if they have the same capacity as the lower-capacity SSDs.
  - The only way to increase the overall storage capacity of the node is replace all SSDs with higher-capacity SSDs. Follow the procedure in Upgrading SSDs to a Higher Capacity on page 23.

Procedure

1. Review the drive failure indications by following SSD or HDD Failure Indication on page 5.
2. Identify the proper drive slot by consulting Drive Slot Numbering on page 3.
3. Run the NCC pre-checks by following Replacement Prechecks on page 7.
4. If you are replacing an encrypted drive, verify that the key management server is connected before you replace the drive.
   For more information, see the data-at-rest encryption topic in the *Web Console Guide*.
5. Prepare to replace the failed drive by following Preparing to Replace an SSD or HDD on page 8.
6. Replace the failed drive by following Physically Replacing an SSD or HDD on page 10.
7. Configure the new drive by following Completing SSD or HDD Replacement on page 17.
8. Run the drive replacement post checks by following Replacement Post Checks on page 21.

SSD or HDD Failure Indication

This section provides failure indications for solid-state drives (SSDs) and hard disk drives (HDDs).

Two failure scenarios for SSDs and HDDs are possible:

- A drive fails completely.
- The drive experiences recoverable errors and warnings that indicate potential failure.

In both scenarios, make sure that logical removal of the disk completes successfully before you begin the physical replacement.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1712

Indications

- The red LED on the front of a drive carrier is illuminated.

Figure 6: Drive Failure Indication - Red LED illuminated

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1713

- The Prism web console displays a disk alert.

> **Note:** The following figures are generic representation of failed drives. The actual drive slot and numbering can vary based on different platforms. See Drive Slot Numbering on page 3 for drive slot numbers of your platform.

Figure 7: Disk Alert (Multi-Node Block)

Figure 8: Disk Alert (Single-Node Block)

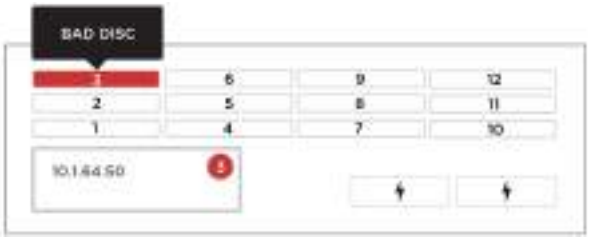


Figure 9: Disk Alert (Single-Node Block)

Replacement Prechecks

Check the health of the cluster before replacing a failed component.

Before you begin

Who is responsible: This procedure can be performed by a customer or partner, under the guidance of a Nutanix support engineer if necessary.

Estimated time to complete: Five minutes

About this task

Perform the following health check to make sure that no issues exists on the cluster. NCC health checks provide a summary of the current state of the entire cluster so that you can identify and fix any unexpected issues before you proceed with the replacement procedure.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1714

Procedure

1. In Prism, go to the **Home** page and make sure that **Data Resiliency Status** displays a green **OK**.
2. In Prism, go to the **Health** page and select **Actions** > **Run NCC Checks**.
3. In the dialog box that appears, select **All Checks** and click **Run**.

   Alternatively, issue the following command from the CVM:

   ```
   nutanix@cvm$ ncc health_checks run_all
   ```
4. If any checks fail, see the related KB article provided in the output and the *Nutanix Cluster Check Guide: NCC Reference*.
5. If you have any unresolvable failed checks, contact Nutanix Support.
6. Gather component details by running the NCC `show_hardware_info` command:

   ```
   nutanix@cvm$ ncc hardware_info show_hardware_info
   ```
7. Save the output of the `show_hardware_info` command so that you can compare details when verifying the component replacement later.
8. Turn on the chassis identifier lights on the front and back of the node.

   » In the IPMI console, go to **Miscellaneous** > **UID**, select **TURN ON**, and click **SAVE**.

   » Log on to a Controller VM and issue the following command:

   ```
   nutanix@cvm$ ~/serviceability/bin/chassis-identify -s cvm_ip_addr -t 240
   ```

   Replace *`cvm_ip_addr`* with the Controller VM IP address for the node to be removed.

   » For AHV: Log on to the hypervisor host (*`hypervisor_ip_addr`*) with SSH and issue the following command:

   ```
   root@ahv# /usr/bin/ipmitool chassis identify 240
   ```

   This command returns the following:

   ```
   Chassis identify interval: 240 seconds
   ```

   » For vSphere: Log on to the hypervisor host (*`hypervisor_ip_addr`*) with SSH and issue the following command:

   ```
   root@esx# /ipmitool chassis identify 240
   ```

   This command returns the following:

   ```
   Chassis identify interval: 240 seconds
   ```

Preparing to Replace an SSD or HDD

Perform the following procedure to prepare a data drive for removal before you proceed with the physical replacement procedure.

Before you begin

Who is responsible: This procedure can be performed by a customer or partner, under the guidance of a Nutanix support engineer if necessary.

Estimated time to complete: Variable, can take up to several hours

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1715

About this task

Do not use this procedure to replace non-volatile memory express (NVMe) drives. NVMe drives are not hot-swappable. For NVMe drives replacement, see NVMe Drive Replacement.

Procedure

1. Log on to the Prism Element web console.
2. If you are replacing an encrypted drive, verify that the key management server is connected before you replace the drive.

   For more information, see the *Data-At-Rest Encryption* topic in the *Web Console Guide*.
3. From the Prism Element web console, select **Hardware** > **Diagram** .

Figure 10: Failed drive information

   Move the pointer over the failed drive for an overview. Click the drive for more details.
4. Record the location of the node and the drive.

   You need the disk and node information to verify correct replacement later in this procedure.
5. From the web console **Summary** > **Disk Details** field, obtain the **Storage Pool** ID and record it.

Figure 11: Storage pool ID menu

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1716

6. Use the web console to remove the failed drive from the Controller VM (CVM) configuration.

> **Caution:** For single node clusters, ensure that the cluster has sufficient rebuild capacity before performing a disk removal. If a cluster does not have sufficient capacity, disk rebuild can fail and result in data loss.
>
> For more details on Single Node Cluster, see the Single-node Clusters section in the *Prism Element Web Console Guide*.

a. Select the disk for removal and click **Remove Disk**.

Figure 12: Removing a disk

b. Wait for data migration to complete.

> **Caution:** If you physically remove a disk before data migration is complete, the data is not correctly replicated to the replacement drive.

c. In the **Hardware Diagram** view, verify that the disk is marked red and unmounted.

Figure 13: Unmounted Drive (Single-Node Block)

> **Note:** If a background process continues to access a disk after Prism marks the disk for removal, unmounting the disk triggers a CVM restart. No action is necessary.

Physically Replacing an SSD or HDD

This procedure describes how to replace an SSD or HDD.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1717

Before you begin

Who is responsible: This procedure can be performed by a customer, partner, or service technician, under the guidance of a Nutanix support engineer if necessary.

Estimated time to complete: Five minutes

About this task

Nutanix supports hot-swapping of SSDs and HDDs. Node shutdown is not required for replacing a failed drive.

> **Caution:** To ensure adequate cooling, replace drives promptly.

The drive carriers have colored labels that indicate the drive capacity and type as follows:

- Blue - HDD
- Green - SSD
- Orange - Encrypted SSD
- Black - Encrypted HDD

A 2.5 inch replacement drive does not come with drive carrier installed. When replacing a 2.5 inch drive, you must remove the failed drive from the drive carrier and install the replacement drive onto the drive carrier. The 3.5 inch replacement drive comes with drive carrier installed.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1718

Procedure

1. If your chassis has a bezel installed, remove the bezel.
   a. Obtain the bezel key.
   b. Insert the key and turn anticlockwise to unlock the bezel.
   c. Push the latch to the left and lift off the bezel.

Figure 14: Bezel for 2U Platforms

Figure 15: Bezel for 1U Platforms

2. Press the tab on the front of the drive to release the lever.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1719

3. Grasp the lever and pull the drive out from the node.

Figure 16: 2.5 inch Drive Removal

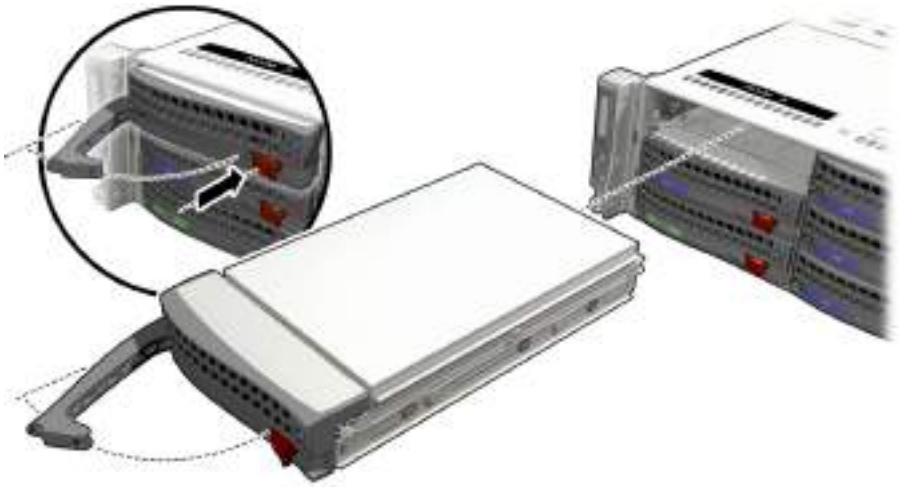


Figure 17: 3.5 inch Drive Removal

4. Confirm that the serial number on the drive that you removed matches the serial number of the failed drive.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1720

5. If you are replacing an encrypted drive, find the PSID number on the drive to ensure that the replacement drive is also an encrypted drive.

Figure 18: Drive serial number labels

> **Note:** If you are replacing a 2.5 inch SSD, proceed to step 6 or step 7 depending on the type of drive carrier in you platform.
>
> If you are replacing a 3.5 inch HDD, skip to step 8.

6. For push fit type drive carrier: Remove the failed SSD from the drive carrier and install the replacement SSD into the drive carrier.

   a. Push the SSD out from the carrier using both your thumbs and remove it from the drive carrier.

   b. Place the replacement SSD on the drive carrier and push until it snaps in place.

Figure 19: Removing 2.5 inch drive from drive carrier (Press fit style carrier shown)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1721

7. For drive carrier with blue clips: Remove the failed SSD from the drive carrier and install the replacement SSD into the drive carrier.

   a. Lift open the two blue clips on the side of the drive carrier.

Figure 20: Opening the Blue Clips on the 2.5 inch Drive Carrier

   b. Lift the drive free from the carrier.

Figure 21: Removing the Drive from the Drive Carrier

   c. Align the pins with the replacement drive.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1722

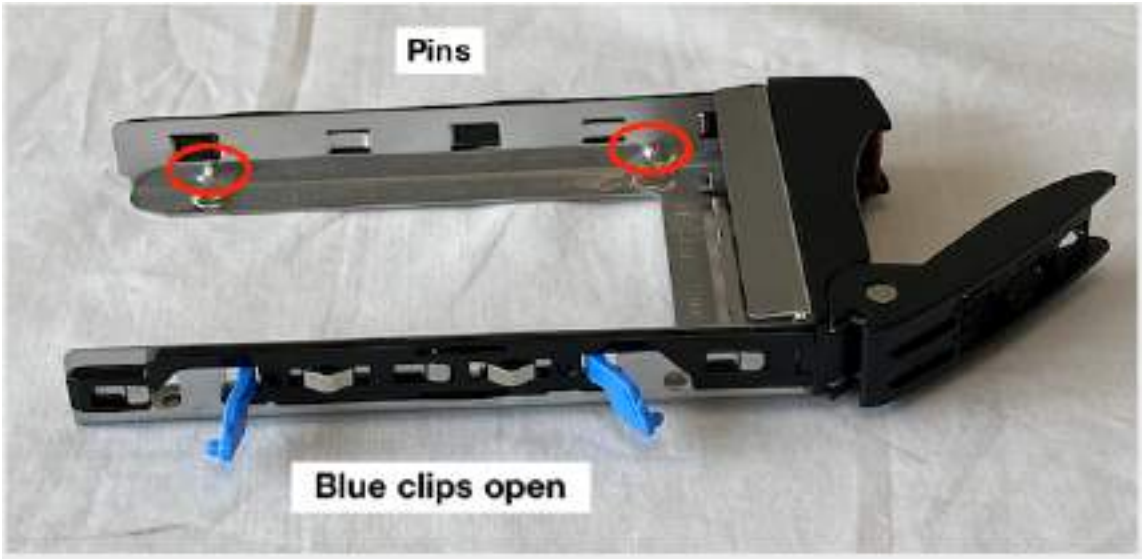


Figure 22: Alignment Points in the Drive Carrier

d. Place the drive in the carrier and secure both blue clips.

e. Verify that all pins and clips are properly aligned and closed.

8. Press the tab on the front of the replacement drive to release the lever.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1723

9. Insert the replacement drive into the empty slot in the chassis and push it in until you feel resistance.

Figure 23: 2.5-inch Drive replacement

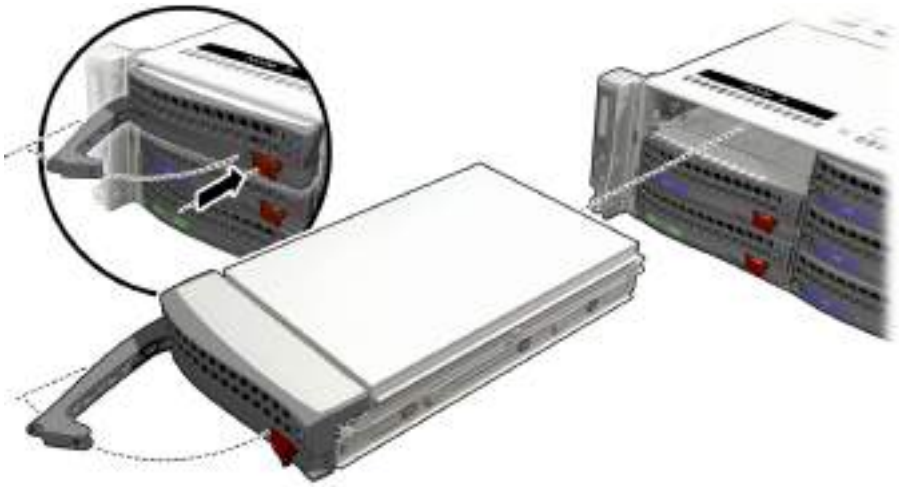


Figure 24: 3.5-inch Drive replacement

10. Push the lever on the front of the drive down until it catches and you hear it click in place.
11. (If you removed the front bezel) After you verify that the drive is working correctly by following the steps in Completing SSD or HDD Replacement on page 17 and Replacement Post Checks on page 21 topics, replace the front bezel.

Completing SSD or HDD Replacement

Make sure that the system recognizes the new drive.

Before you begin

Who is responsible: This procedure can be performed by a customer or partner, under the guidance of a Nutanix support engineer if necessary.

Estimated time to complete: 10 minutes

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1724

About this task

Procedure

1. Log on to the Prism Element web console, go to **Hardware** > **Diagram** and click the replacement drive.

Figure 25: Replaced Drive (Single-node platforms)

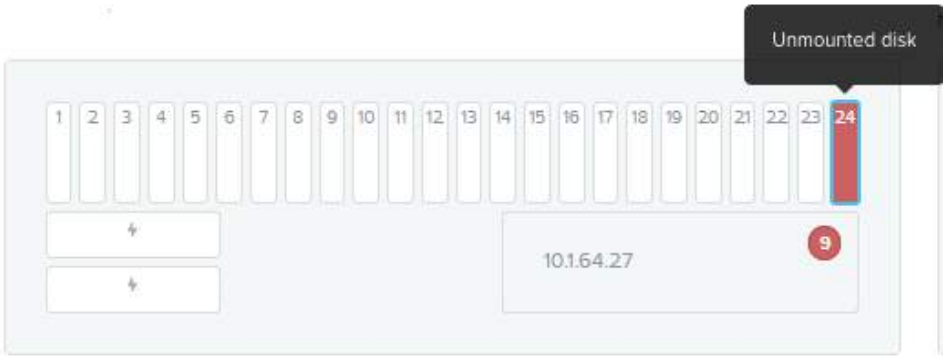


Figure 26: Unmounted Drive (Single-node platforms)

» If the drive is red and shows a label of `Unmounted Disk`, continue to Step 2.

» If the drive is not red, and Prism does not show a failure message when you select it, that means Prism added the drive automatically. Skip to Step 3.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1725

2. Select the drive and click **Repartition and Add** under the diagram.

   a. On platforms that use Nutanix AOS 6.0 or later only: Specify whether you are replacing a faulty disk or upgrading disk capacity.

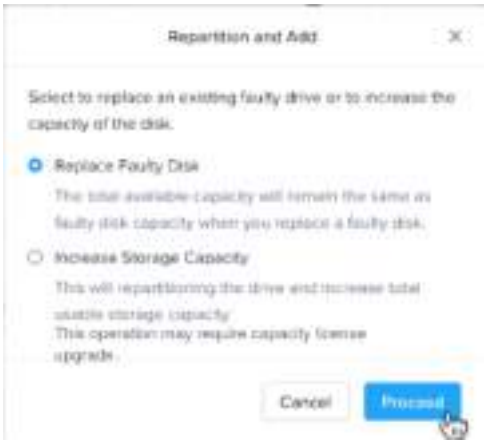


Figure 27: Repartition and Add dialog (AOS 6.0 and later)

   b. Click **Proceed**.

> **Caution:** This action removes all data on the drive. Do not repartition the drive until you confirm that the drive contains no needed data.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1726

3. From the web console **Summary** > **Disk Details** field, verify that Prism added the disk to the original storage pool.

Figure 28: Disk Details

If the cluster has only one storage pool, Prism automatically adds the disk to that storage pool.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1727

4. If Prism did not add the drive to the storage pool because the cluster has more than one storage pool, add the drive to a storage pool. Use the storage pool ID that you recorded earlier in Preparing to Replace an SSD or HDD on page 8.

   a. In the Prism web console, select **Storage** from the drop-down main menu (upper left of screen), then select the **Table** > **Storage Pool**.

Figure 29: Storage Pool Table View

   b. Select the target storage pool and click **Update**.
   The **Update Storage Pool** window appears.

   c. In the **Capacity** field, check the **Use unallocated capacity** box to add the available unallocated capacity to this storage pool, then click **Save**.

   d. Go back to **Hardware** > **Diagram**, select the drive, and confirm that it is in the correct storage pool.

5. Verify the SSD or HDD firmware version:

```
nutanix@cvm$ ncc health_checks hardware_checks disk_checks disk_firmware_check
```

Replacement Post Checks

Check the health of the cluster after you replce a failed component.

Before you begin

Who is responsible: This procedure can be performed by a customer or partner, under the guidance of a Nutanix support engineer if necessary.

Estimated time to complete: 10 minutes

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1728

Procedure

1. Ensure that the system is running the latest supported firmware, BIOS, and BMC versions.

   Nutanix recommends performing an LCM inventory and then running the relevant updates by following the Life Cycle Manager Guide.

   In scenarios where you cannot run LCM, manually update the firmware. For more information, see Manual Firmware Updates in the *NX Series Hardware Administration Guide*.

   Optionally, after the manual firmware update, you can run the following command from a CVM and check the output to confirm the firmware versions:

   ```
   nutanix@cvm$ ncc hardware_info show_hardware_info --cvm_ip=controller_vm_ip_address
   ```

   Replace `controller_vm_ip_address` with the IP address of the CVM.

2. In Prism, go to the **Health** page and select **Actions** > **Run NCC Checks**.

3. In the dialog box that appears, select **All Checks** and click **Run**.

   Alternatively, issue the following command from the CVM:

   ```
   nutanix@cvm$ ncc health_checks run_all
   ```

   If any checks fail, see the related KB article provided in the output and the *Nutanix Cluster Check Guide: NCC Reference*.

4. If you have any unresolvable failed checks, contact Nutanix Support.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1729

UPGRADING SSDS TO A HIGHER CAPACITY

This procedure describes how to replace existing SSDs in your platform with higher capacity SSDs.

About this task

On platforms that use versions of Nutanix AOS earlier than 6.0, all SSDs in a node must have the same capacity. If you upgrade one SSD, you must upgrade all remaining SSDs, one SSD at a time.

On platforms that use Nutanix AOS 6.0 or later, AOS allows you to mix SSDs of different capacities in the same node, for replacement cases where only higher-capacity SSDs are available. In these cases, the node treats the replacement SSDs as if they have the same capacity as the lower-capacity SSDs. To increase the overall storage capacity of the node, you must upgrade all SSDs.

Before you begin

Check `/etc/nutanix/hcl.json` to make sure that the SSD type to be added appears in the AOS hardware compatibility list (HCL):

```
nutanix@CVM:~$ cat /etc/nutanix/hcl.json | grep model
```

If your model does not appear in the HCL, either update to a more recent version of AOS or contact Nutanix Support for assistance.

> **Note:** If you are upgrading SSDs on a Single-node cluster, before starting the procedure contact Nutanix Support referencing KB 15353.

Procedure

1. In Prism, find the first SSD to be removed in the **Hardware Diagram** and click **Remove Disk**.

Figure 30: Removing a disk

2. Wait for data migration to complete.
3. In the **Hardware Diagram**, check that the drive is marked red and unmounted.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1730

4. When Prism finishes removing the disk, physically replace the SSD with the higher capacity SSD, following the procedure in Physically Replacing an SSD or HDD on page 10.
5. When the SSD replacement is complete, make sure that the system recognizes the new drive, following the procedure in Completing SSD or HDD Replacement on page 17.
6. Repeat Steps 1 through 5 for every SSD in the node.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1731

COPYRIGHT

Copyright 2024 Nutanix, Inc.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Nutanix and the Nutanix logo are registered trademarks of Nutanix, Inc. in the United States and/or other jurisdictions. All other brand and product names mentioned herein are for identification purposes only and may be trademarks of their respective holders.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1732

Nutanix Flow

VISUALIZE | SECURE | MONITOR

FUNCTIONS

VM Microsegmentation

Application Visualization

Service Chaining

Policy-based Control

Identity Based Policy

Traffic Monitoring and Threat Detection

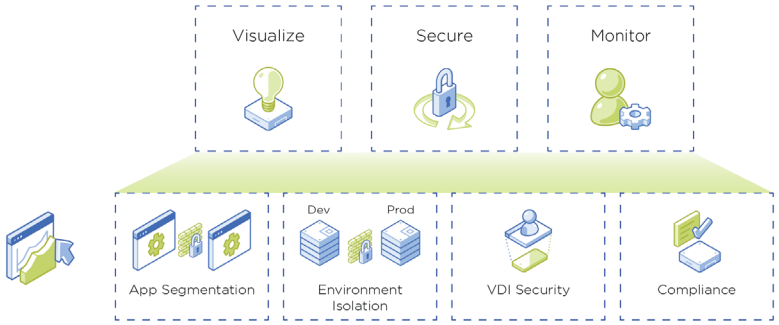
Compliance Audit and Reporting

The network is the foundation for the connected Enterprise. With increasing application complexity, driven by distributed services and rapid growth in SaaS and cloud-based offerings, the need to easily visualize, analyze and govern network communications becomes critical.

Nutanix Flow delivers advanced network security, providing visibility into the virtual network, application-centric protection from network threats, malware, and ransomware and security and compliance monitoring.

Flow allows organizations to deploy software-defined virtual network security without the complexity of installing and managing additional products that have separate management and independent software maintenance requirements.

Fully integrated into the Nutanix private cloud solution and Nutanix AHV virtualization, Nutanix Flow differs from traditional perimeter firewalls by allowing network policy to be attached to VMs and applications, rather than specific network segments (e.g., VLANS) or identifiers (IP addresses). Through centralized management from Prism, policies are auto-updated throughout the VM lifecycle, removing the burdens of change management.



Application and Network Visualization

Creating the right network policies requires a complete understanding of workload behavior. Nutanix Flow provides a detailed visualization of communications between VMs along with assistance in categorizing and grouping workloads, making it simple and straight-forward to set the right policies for the environment.

NUTANIX

©2021 Nutanix, Inc. All Rights Reserved

KEY BENEFITS

- Application centric network policies for VMs
- Works with any network topology or architecture
- Application and network visibility
- Policy change management tied to VM lifecycle
- Prevent the propagation of network security threats
- Adds Identity based security to EUC/VDI deployments
- Security posture visibility and tracking dashboard
- Compliance audit and reporting regulations like HIPAA, PCI, NIST, and more
- Expand functionality via third-party network inspection and policy tools

Network Isolation and Microsegmentation

Microsegmentation provides granular control and governance of all traffic into and out of a virtual machine (VM), or groups of VMs. It ensures that only permitted traffic between application tiers or other logical boundaries is allowed and protects against advanced threats propagating within the virtual environment.

Identity-Based Network Policy

Identity Firewall in Flow allows EUC policy to incorporate the additional context of a user's identity. Group and role information pulled from directory services combine to create a more granular yet dynamic policy model.

Service Insertion and Chaining

Nutanix Flow functionality can be extended to leverage virtualized network functions from third-party software. These services are inserted in-line or in tap-mode with VM traffic, and can be easily enabled for all traffic, or deployed only for specific network traffic. Common network functions include virtual firewalls, load balancers, threat detection, and application performance monitoring.

Monitoring, Compliance Audit, and Reporting

Flow's Security Central provides a security operations portal for your Nutanix infrastructure adding visibility and control of network traffic and Nutanix security configurations along with out of the box audit and reporting for common security and compliance regulations such as HIPAA, PCI, and NIST. You can also create custom audit checks to align with your specific security compliance needs.

RESOURCES

- nutanix.com/products/flow
- nutanix.com/products/ahv
- nutanix.com/security

PRICING AND AVAILABILITY

Nutanix Flow is built into the Nutanix software and works seamlessly with AHV virtualization. Capabilities are delivered with AHV and are licensed separately from AOS Editions.

	AHV	Flow License
Simple Service Insertion and Chaining	✓	
Network Automation	✓	
Application Flow Visualization		✓
Policy-Based Service Insertion and Chaining		✓
Application Security with Microsegmentation		✓
Flow Security Central: Compliance Audit and Reporting, Security Posture and Status Dashboards		✓

NUTANIX™
YOUR ENTERPRISE CLOUD

T. 855.NUTANIX (855.688.2649) | F. 408.916.4039
info@nutanix.com | www.nutanix.com | @nutanix

©2021 Nutanix, Inc. All rights reserved. Nutanix, the Nutanix logo and all product and service names mentioned herein are registered trademarks or trademarks of Nutanix, Inc. in the United States and other countries. All other brand names mentioned herein are for identification purposes only and may be the trademarks of their respective holder(s).

DETAILED PRODUCT DESCRIPTION

ExaGrid Tiered Backup Storage

EXAGRID®

Tiered Backup Storage

Table of Contents

Executive Summary . . . 3
ExaGrid Basic Concept . . . 4
ExaGrid Technology Overview . . . 5
ExaGrid Appliance Models . . . 6
Designed for Storage Efficiency . . . 7
Data Deduplication . . . 7
Data Backup Performance . . . 7
Data Restore Performance . . . 8
Fastest Performance . . . 9
Scalable Architecture – Scale-Out . . . 10
Support for Heterogeneous Backup Applications and Utilities . . . 12
Advanced Backup Features . . . 13
Veritas Integrations . . . 13
Veeam Accelerated Data Mover . . . 15
ExaGrid as an S3 Object Store for Veeam/Veeam Backup for M365 . . . 16
Veeam Scale-Out Backup Repository (SOBR) . . . 17
Rubrik . . . 18
Commvault . . . 19
Oracle RMAN Channels . . . 20
Security, Reliability, and Redundancy . . . 21
ExaGrid Retention Time-Lock for Ransomware Recovery . . . 22
RAID 6 Internal Storage with Consistency Checking . . . 26
Flash-Backed RAID Cache . . . 26
Backup Data Checksums with Automatic Repair . . . 26
Deduplicated Metadata Transactional Consistency . . . 26
Internal Database Backups and Self-Describing Metadata . . . 26
Logging Filesystem . . . 26
Data Security . . . 27
Active Directory Support . . . 27
Periodic Assessments Using a Network Vulnerability Scanner . . . 27
Offsite Data Protection for Disaster Recovery . . . 28
Total Cost of Ownership . . . 30
Cost Effectiveness Up Front . . . 31
Cost Effectiveness as Data Grows . . . 32
Summary . . . 33
About ExaGrid . . . 35

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1736

Executive Summary

ExaGrid provides Tiered Backup Storage with a unique disk-cache Landing Zone, non-network-facing long-term retention repository, and scale-out architecture. ExaGrid's Landing Zone provides for the fastest backups, restores, and instant VM recoveries. The disk-cache Landing Zone tier allows for the fastest backups and restores. The Repository Tier offers the lowest cost for long-term retention and a non-network-facing tier to be able to recover from security attacks, such as ransomware. ExaGrid's scale-out architecture includes full appliances and ensures a fixed-length backup window as data grows, eliminating expensive forklift upgrades and planned product obsolescence.

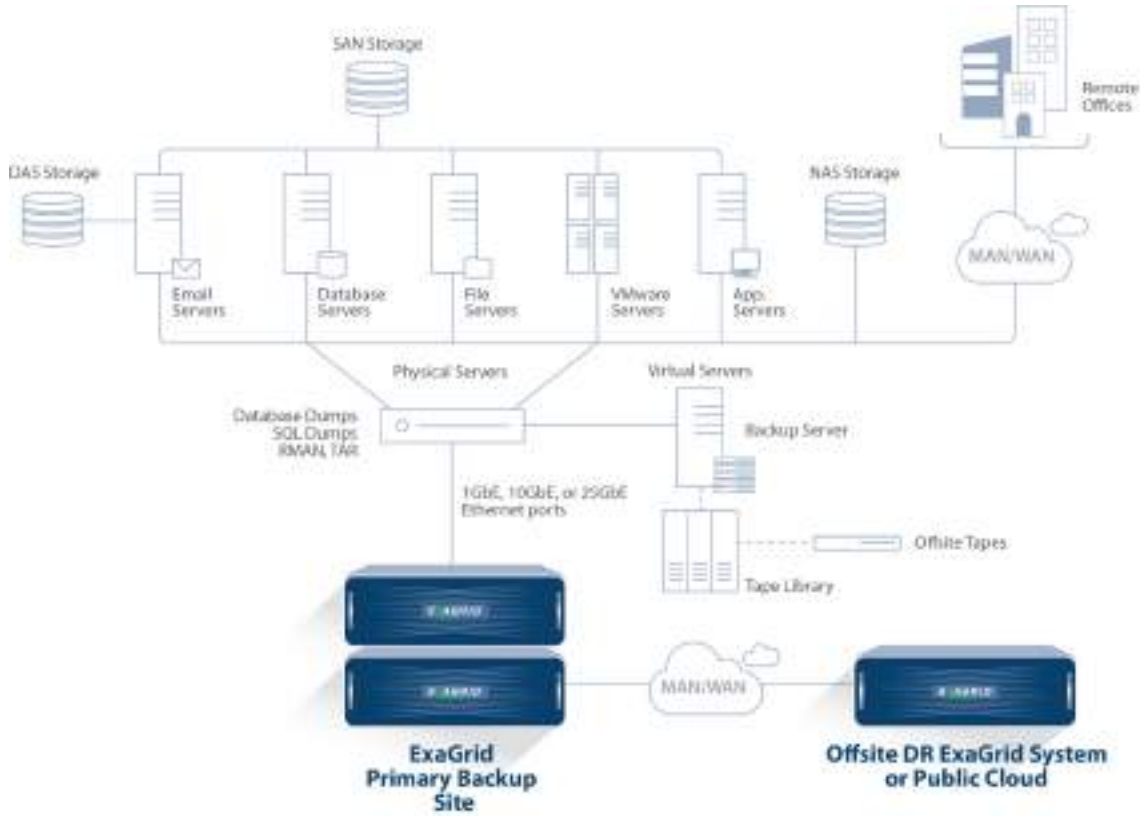
ExaGrid Tiered Backup Storage makes backup better with:

- Fastest backups resulting in the shortest backup window
- Fastest restores
- Instant VM recoveries in seconds to minutes
- Fastest offsite tape copies, copy jobs, and AUX copies
- A fixed-length backup window as data grows, eliminating expensive future forklift upgrades
- Retention Time-Lock (RTL) to ensure recovery from a ransomware attack – non-network-facing tier creates a tiered air gap
- Industry-leading deduplication ratios for storing long-term retention data for low-cost retention storage
- Deduplication efficiency across the entire system with global deduplication
- Further deduplicates data already deduplicated by the backup application
- Virtualized storage efficiency with automatic load balancing
- Fast, reliable, and up-to-date offsite disaster recovery using Adaptive Deduplication
- Linear scalability – scale-out architecture – pay as you grow
- Low cost up front and over time as data grows
- No forklift upgrades or planned product obsolescence

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1737

ExaGrid Basic Concept

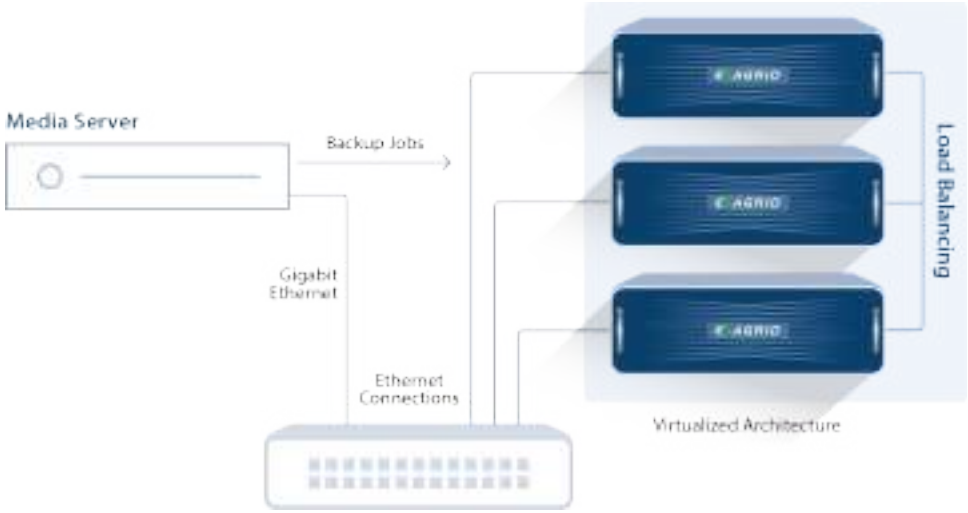
ExaGrid appliances work seamlessly with over 25 industry-leading backup applications and database utilities by presenting themselves as standard NAS shares (CIFS or NFS), a Veeam Data Mover target, Veritas NetBackup OST target, or as an S3 object store. ExaGrid appliances are easily integrated into existing backup environments, as illustrated below.



ExaGrid sits behind the existing backup server and replaces straight disk, inline deduplication appliances or tape backup storage, both onsite and offsite.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1738

ExaGrid Technology Overview



ExaGrid Appliances Connect to Form a Single Scale-Out System

ExaGrid appliances are comprised of processors, memory, networking, IPMI, RAID 6, and a hot spare drive per appliance, using enterprise-class SAS drives and ExaGrid software. See the **ExaGrid Technical Specifications** data sheet for more details.

Each appliance plugs in and is virtualized into a shared system with a single user interface, global deduplication, and automatic load balancing. The media server is connected to the same network and sees the appliances as one or more NAS shares, Veeam Data Mover targets, Veritas NetBackup OST targets, or S3 Object Storage. Since each appliance includes the appropriate amount of processor, memory, Landing Zone disk, deduplicated repository disk, and bandwidth for the rated data size, performance increases as more appliances are added to the system.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1739

ExaGrid Appliance Models

ExaGrid's multiple appliance models can be combined into a single scale-out system with a configuration of up to 32 appliances in a single system for a total of: 13.82PB raw capacity, 12PB of usable capacity, and supports a full backup of up to 6.04PB, total backup logical data capacity of 96.76PB.

ExaGrid Model	Raw Capacity (TB)	Usable Capacity (TB)	Capacity for Weekly Full (TB)	Max Backup Thruput (TB/hr)	Form Factor	Optional Data at Rest Encryption (SEC)
ExaGrid Appliances						
EX36	96	72	36	7.90	2U	√
EX54	162	108	54	5.80	2U	√√
EX81	216	162	81	8.70	2U	√√
EX84	192	168	84	15.25	2U	√√
EX135	324	270	135	14.50	2U	√√
EX189	432	378	189	20.30	2U	√√

In addition, ExaGrid offers these appliance models to accommodate larger organizations that have smaller data center locations worldwide:

ExaGrid Model	Raw Capacity (TB)	Usable Capacity (TB)	Capacity for Weekly Full (TB)	Max Backup Thruput (TB/hr)	Form Factor	Optional Data at Rest Encryption (SEC)
ExaGrid Appliances for larger accounts with smaller data center locations						
EX10	32	20	10	3.90	2U	√
EX20	64	40	20	4.40	2U	√

√√ = Software Updgradeable SEC for Data Encryption at Rest

(Note: available in select 2025 version EX54 models, not available in previous EX54 models)

Scales to 32 appliances in a single scale-out system
(6PB full backup @ 649.60TB/hr. ingest rate)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1740

Designed for Storage Efficiency

Data Deduplication

ExaGrid's innovative approach to data deduplication minimizes the amount of data to be stored by using zone-level data deduplication across all received backups.

ExaGrid's patented zone-level technology stores only the changed data at a granular level from backup to backup instead of storing full copies. ExaGrid uses zone stamps and similarity detection.

This unique approach reduces the disk space required by an average of 20:1 and from 10:1 up to 50:1 depending on data type, retention and backup rotation delivering unparalleled performance for the fastest backups and restores.

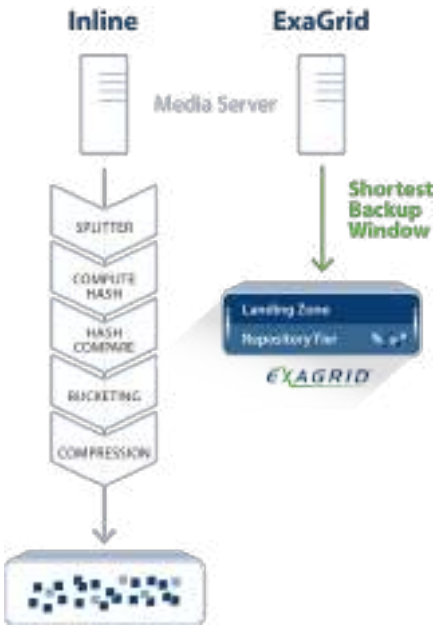
ExaGrid is the only vendor that allows backup applications such as Veeam and Commvault to keep their deduplication turned on and then ExaGrid further deduplicates the data for increased storage efficiency.

Data Backup Performance

The ExaGrid system performs deduplication in parallel with backups by using idle system cycles. Termed "adaptive deduplication," this approach keeps deduplication out of the backup path, resulting in faster backups and a shorter backup window. Adaptive Deduplication gives full system resources to backups for the shortest backup window and uses idle cycles to perform deduplication and offsite replication, allowing data to be replicated offsite for a strong offsite recovery point (RPO) for update to data for disaster recoveries.

ExaGrid supports automated job management utilizing Veeam SOBR, Veritas NetBackup Single Target Storage Pool, Commvault Spill & Fill, Oracle RMAN Channels, HYCU Scale-out and other automated job management facilities. ExaGrid globally deduplicates data across all appliances in a scale-out system. Global deduplication ensures that all data is deduplicated regardless of the number of appliances in a system. In addition, global deduplication allows organizations the flexibility to redirect backup jobs to any appliance at any time while maintaining data deduplication globally across the entire system.

Once the backup job is complete and off the network, the data is protected and immediately available to be restored. When deduplication and replication are complete, the data is ready for restore on the ExaGrid appliances at the disaster recovery site. ExaGrid uses Adaptive Deduplication that avoids the performance penalty of inline deduplication. ExaGrid deduplicates in parallel with backups coming in but performs no inline processing which allows for at least a 3X performance advantage over inline deduplication appliances. As shown in the diagram to the right, backup data is written directly from the backup server to ExaGrid's disk-cache Landing Zone at the highest possible rate with no inline processing to interfere, resulting in the shortest possible backup window.



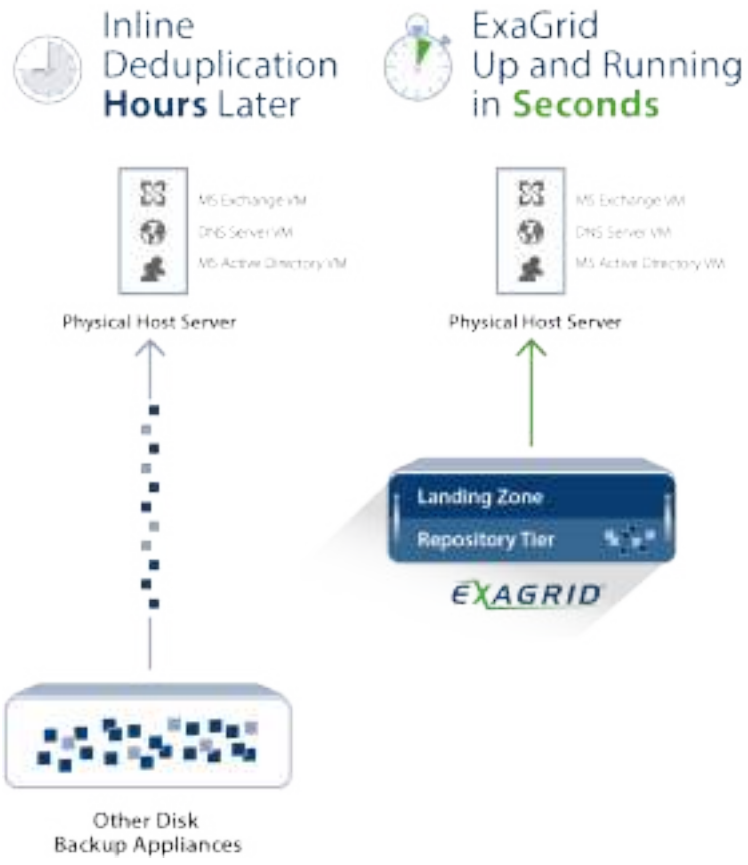
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1741

Data Restore Performance

Because ExaGrid's appliance allows each full backup to first land on the disk-cache Landing Zone before deduplication, the system maintains the most recent backup in its full, undeduplicated form for fast restores, instant VM recoveries in seconds to minutes, and fast offsite tape copies, copy jobs, and AUX copies.

Since over 90% of restores and 100% of instant VM recoveries and tape copies are done from the most recent backup, this approach avoids the overhead incurred from "re-hydrating" data during critical restores. As a result, restore, recovery, and copy times from an ExaGrid system are an order of magnitude faster than solutions that only store deduplicated data. The most recent data is available in an undeduplicated native backup format for fast restores to keep user productivity up by quickly recovering deleted files, overwritten files, corrupted files, encrypted files, etc. The non-network-facing Repository Tier stores the most recent backups as well as all the long-term retention in a storage efficient deduplicated format. Legal discoveries, SEC audits, financial audits, regulatory audits etc. have a lead time to recover the data where recovering for users does not. ExaGrid has found the balance between fast user data restores and long-term retention data storage efficiency.

Restore Performance



Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1742

Fastest Performance

ExaGrid has a unique architecture with a front-end disk cache Landing Zone where the most recent data is stored in a non-deduplicated native backup application format for fast backups and restores. The second tier is a non-network-facing Repository Tier for the storage of long-term retention data in a storage efficient deduplicated data format.

To ensure fast performance, the backup storage files system must be able to handle large backup jobs unlike NAS storage which optimized for files or SSD storage which is optimized for transactional databases. In addition, to further increase performance, advanced backup protocols, concurrency and other techniques need to be deployed. Standard disk or SSD storage is not optimized for backup.

ExaGrid is designed and optimized for large backup jobs. ExaGrid uses all the following techniques to achieve the fastest backup performance. In side-by-side tests ExaGrid is faster than any other storage for ingest performance resulting in the shortest backup window.

- Backups are written direct to the disk Landing Zone (no inline deduplication)
- ExaGrid is integrated with backup applications scale-out functionality that allow backup applications to write to any ExaGrid appliance that is not still processing data allowing all appliances to be utilized for performance. The combination of the Veeam SOBR, Veritas NetBackup Single Target Disk Pool, Commvault Spill & Fill, Oracle RMAN Channel, HYCU Scale-out, and others allows for front-end performance load balancing. Data can go to any appliance at any time as ExaGrid supports a scale-out storage architecture, global deduplication and automatic load balancing.
- File system optimized for large backup files. Most storage is optimized for files or database transactions. Backup files are very large and require a file system optimized for backup. Since ExaGrid is dedicated backup storage it is optimized for large backup jobs
- Use of advanced protocols. ExaGrid has full appliances in a scale-out system. ExaGrid runs software that brings functionality but also integrates with backup applications. ExaGrid can gain an additional 30% ingest performance over CIFS and NFS by using protocols or layers built specifically for large backup jobs such as the Veeam Data Mover and Veritas NetBackup OST.
- Job concurrency allows for backup jobs to be written in parallel allowing full use of all appliances, resulting in improved performance.

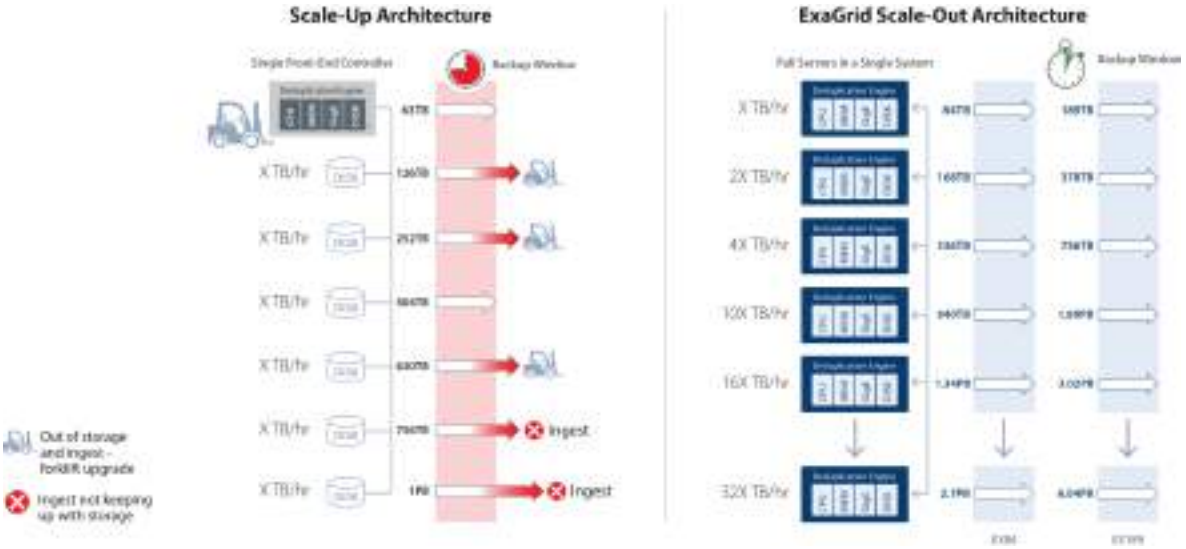
When tested against primary storage or SSD storage ExaGrid is typically 2X the performance due to SSD file system limitations. When tested against inline deduplication appliances (which are compute bound by performing the deduplication before writing to the disk), ExaGrid is typically 3X to 4X faster. ExaGrid is as much as 5X faster than general purpose files systems such as Microsoft ReFS to disk.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1743

Scalable Architecture – Scale-Out

The typical business or organization is seeing data growth of 30% a year which doubles data every 2.5 years. This data growth presents challenges to IT to ensure their backup system can scale easily to support that growth. With scale-up disk backup solutions that have a front-end server/controller architecture and add just disk shelves as data grows, you start with a short backup window, but as data grows, the backup window expands because only disk is added but no additional deduplication processing resources. Eventually, the backup window expands to a point where you must replace the front-end server with a more powerful server via a costly "forklift upgrade."

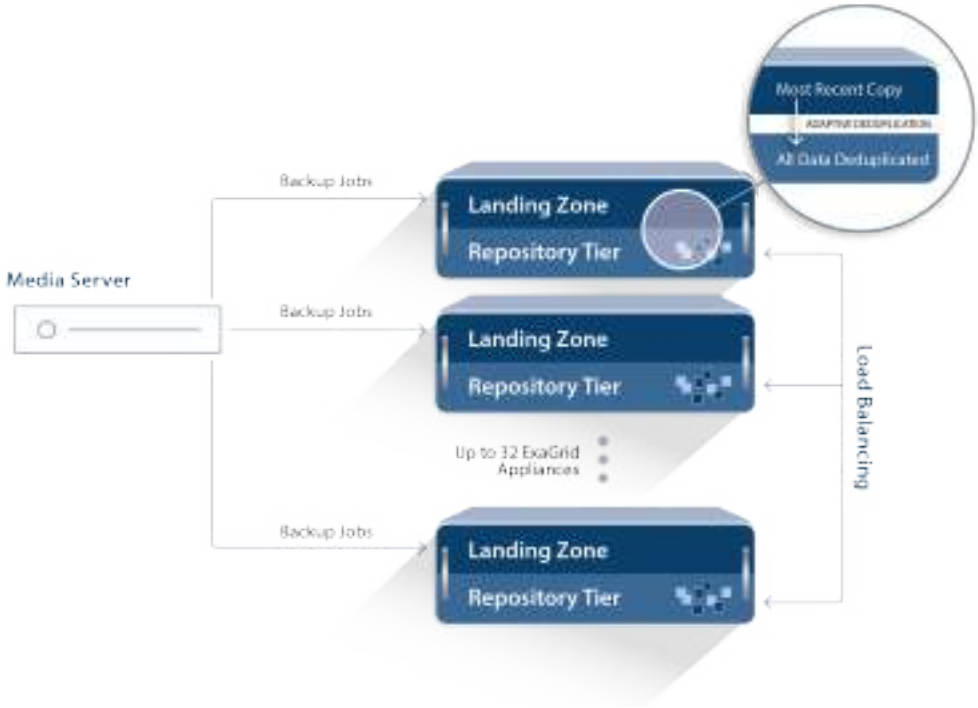
In contrast, ExaGrid's scale-out approach with global deduplication adds full appliances—including memory, processor, and bandwidth, as well as disk. The figure below shows the differences between how the two different architectures cope with data growth over time.



Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1744

ExaGrid's scale-out approach provides the following benefits:

- **No Expansion of Backup Windows as Data Grows** – By adding full appliances, ExaGrid maintains consistently fast backup performance and a fixed length backup window as data increases.
- **Seamless Scalability with No Forklift Upgrades** – ExaGrid's scale-out approach avoids forklift upgrades by adding modular capacity with full servers to the existing system in full backup increments of 10, 20, 36, 54, 81, 84, or 189TB with up to 32 appliances in a single system that scales to 6PB full backup.
- **No Obsolescence of Previous Model Systems** – All ExaGrid appliances can be seamlessly added to any existing ExaGrid deployment and can be mixed and matched with older appliances of any size, thereby eliminating planned product obsolescence. Adding a new ExaGrid appliance is as simple as plugging it in and pointing backup jobs at the appropriate appliance. If any model is no longer offered, the models still work in a scale-out system with older and newer models, maintenance and support is always offered and maintenance and support will not go up more than 3% per year allowing organizations to get their full lifetime use out of all appliances in the system.



ExaGrid appliances include scalable computing software, which allows them to virtualize and share data storage capacity with one another (automatic load balancing across all repositories). This scalable system (shown above) can expand as data grows by adding appliances, providing up to: 13.82PB raw capacity, 12PB usable capacity, and allowing full backups of up to 6PB in a single scale-out system. Multiple systems can be used at a single location, and up to 16 separate locations can be managed through a single user interface.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1745

Support for Heterogeneous Backup Applications and Utilities

Customer environments are made up of many backup approaches, backup applications, and utilities. Customers may have any number of backups occurring in their environment, including traditional backup applications such as Veeam, Veritas NetBackup, Commvault, IBM Spectrum Protect (TSM), Oracle RMAN Direct, HYCU, and many others as well as direct-to-disk SQL dumps, Oracle RMAN direct backups, and specific UNIX utilities such as UNIX TAR. ExaGrid supports over 25 backup applications and utilities.

ExaGrid supports backup data from multiple sources, including a variety of backup applications and database dump utilities. Performing deduplication in the backup application software limits the ability to have all data from all sources stored and deduplicated in a single target device. Unless 100% of your backup data passes through that particular backup application, a Tiered Backup Storage appliance such as ExaGrid's is the best choice to meet the requirements of your entire environment.

In contrast, backup application software solutions that have incorporated deduplication by definition only support their own backup application, with its own media server software and its own backup client agents. These solutions are not able to support backup data from other backup applications or utilities. For example, if you have a physical environment, for backup applications that employ data deduplication but want to use a separate utility for VMware (ex: Veeam) and also do direct database dumps, only the data running through the physical system's backup application will be deduplicated. Also, deduplication in backup software ranges from 2:1 to 5:1 and therefore uses a lot more disk and bandwidth as retention grows versus target-side deduplication appliances that employ far more aggressive deduplication algorithms, since with appliances, resources are dedicated to the task. Dedicated appliances achieve ratios on average of 20:1.

ExaGrid allows for Veeam, Commvault, and Rubrik to leave deduplication turned on and ExaGrid will further deduplicate the data for increase storage efficiency.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1746

Advanced Backup Features

Veritas Integrations

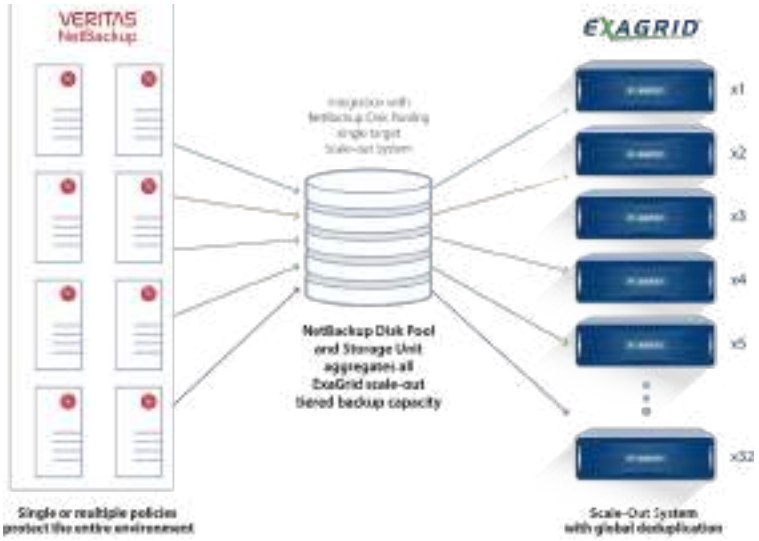
An important consideration when looking at disk-based backup solutions is how well a particular solution supports advanced backup application features such as GRT (Granular Restore) and Veritas' OST (Open Storage Technology) for NetBackup. Some solutions do not integrate well with these features; poorly implemented GRT solutions, for example, may take hours to restore an individual e-mail or may not work at all.

Veritas' Open Storage Technology is another popular feature that allows for more integrated offsite data protection, and it is important to check whether these features are supported if you are using Veritas NetBackup, OST allows for faster performance, better management, and unbalanced onsite and offsite retention.

ExaGrid supports and is Veritas NetBackup certified for:

- Storage target behind Veritas physical media servers
- OST integration
- Accelerator support
- Auto Image Replication (AIR)
- Optimized Duplication (Replication)
- Instant Recovery
- Granular Recovery Technology (Exchange, SharePoint, VMs)
- NetBackup IT Analytics
- Support for NetBackup Flex Media Server Appliances with the OST plug in
- Veritas Single Target Storage Pool

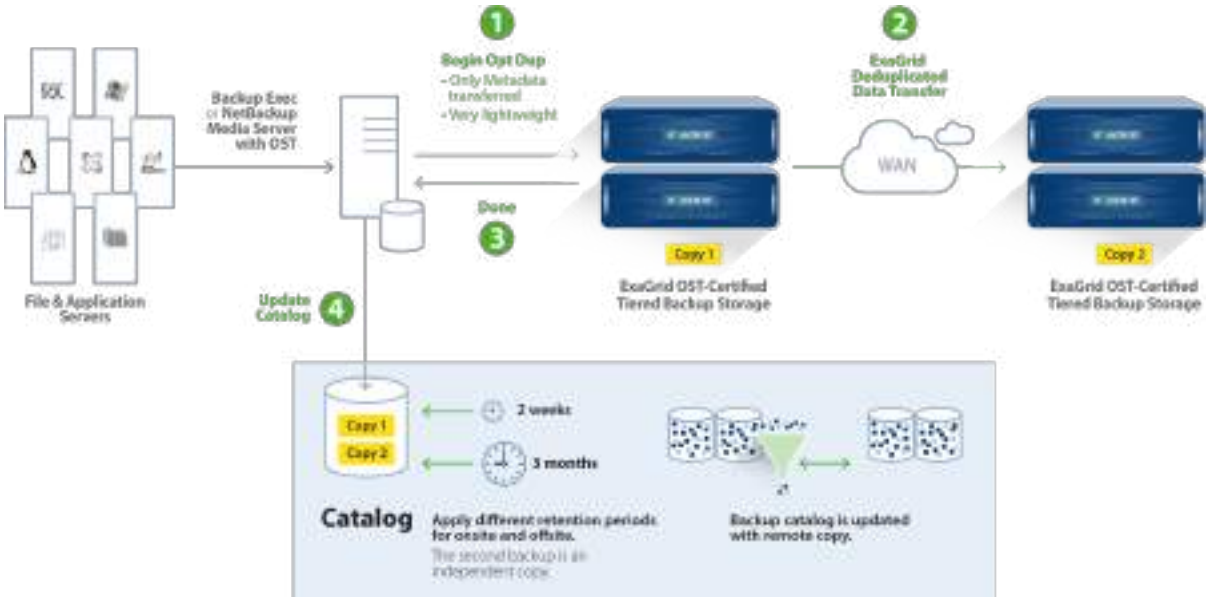
ExaGrid is the only solution in the market for Veritas NetBackup Accelerator that can reconstitute a full backup in its Landing Zone so that a complete backup is ready for restore in its already hydrated form for faster restores and VM boots.



- Automated job management
- Fastest backups with ExaGrid disk-cache Landing Zone
- Performance load balancing
- Automatic repository load balancing
- Global deduplication across all repositories
- 6PB full backup in a single system
- Future-proof scalability for data growth by simply adding another appliance
- Failure tolerance with automated job redirect

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1747

ExaGrid integration with Veritas OST

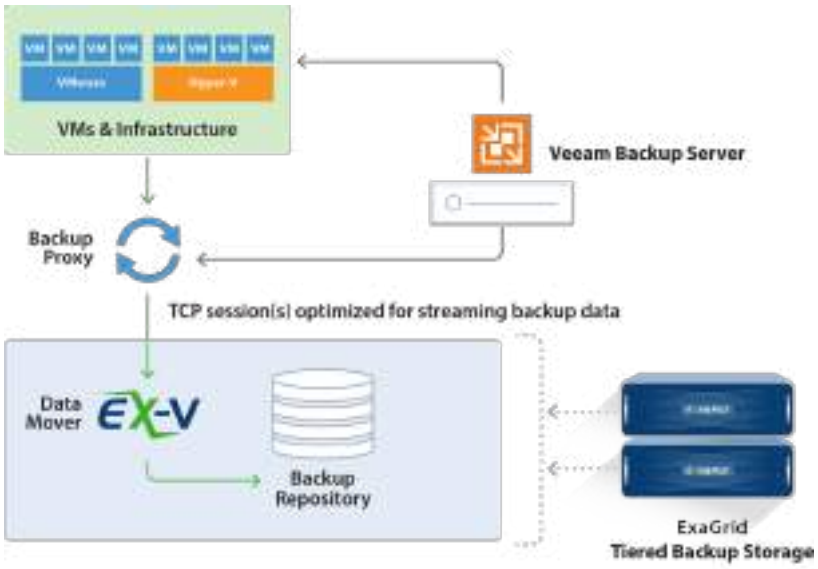


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1748

Veeam Accelerated Data Mover

Most of Veeam's unique features such as its Scale-Out Backup Repository (SOBR), Sure Backup, Virtual Lab, Instant VM Recovery, Copy and Replicate, and other advanced features require an undeduplicated copy in Veeam native format on disk. Only ExaGrid provides this with its unique disk-cache Landing Zone. All other solutions only store deduplicated data. In addition, ExaGrid includes an integrated Veeam data mover with each appliance called the "ExaGrid-Veeam Accelerated Data Mover." This improves all backup and restore processes, increases security with a closed end-to-end communications protocol and also allows a synthetic full to be created directly on the ExaGrid system for increased performance.

ExaGrid also supports Veeam Fast Clone, which allows for 30x faster synthetic fulls, which takes minutes. Automatic resynthesis of the synthetic fulls into actual full backups takes place in parallel with backups, which allows for the fastest restores & VM boots for Veeam data in the industry.



Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1749

Support of S3 Object Storage with Object Locking and Veeam Backup for M365

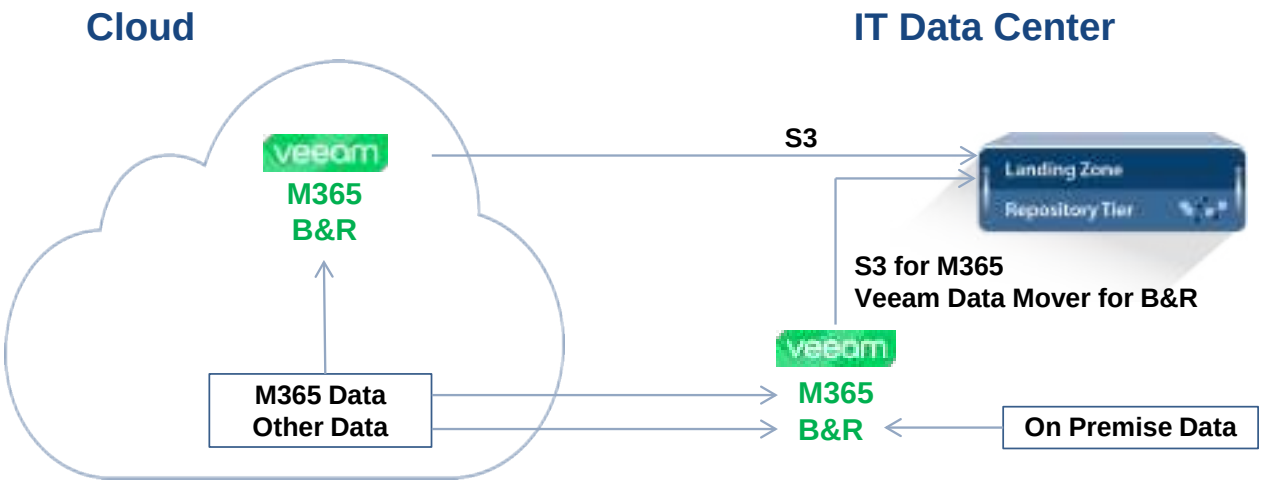
ExaGrid supports Veeam writing to ExaGrid Tiered Backup Storage as an object store target using the S3 protocol, as well as supporting Veeam Backup for Microsoft 365 directly to ExaGrid.

ExaGrid locks the data for the time period provided by Veeam:

- S3 Locks data in the Landing Zone
- S3 Locks data in the Repository Tier
- ExaGrid RTL - Retention Time-Lock
  - Double locks the repository
- ExaGrid supports the S3 API
- ExaGrid supports the Veeam S3 Extension (SOSAPI) when used with Veeam Backup and Replication

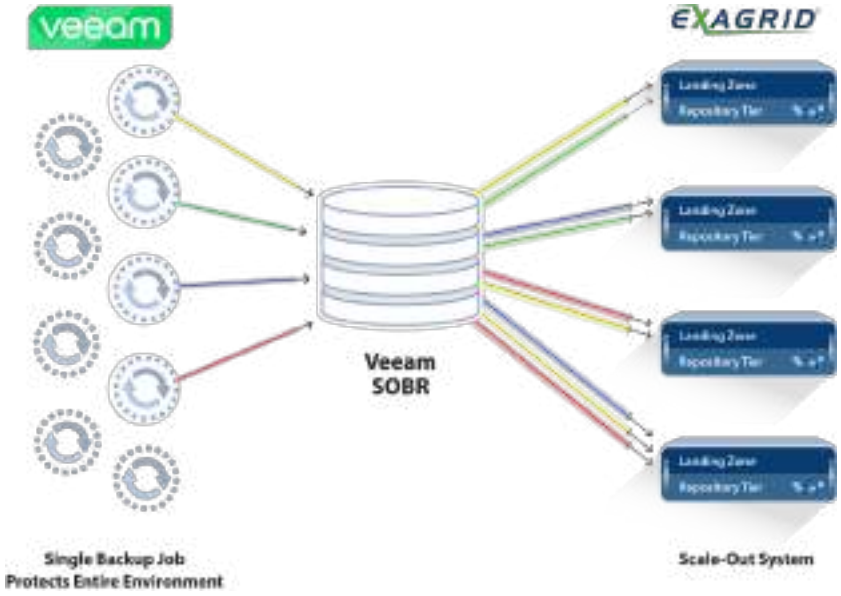
Chose the best combination of:

- S3
- Veeam Data Mover



Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1750

Veeam Scale-Out Backup Repository (SOBR)



Veeam's Scale-Out Backup Repository (SOBR) allows backup administrators using Veeam to direct all jobs to a single repository made up of ExaGrid shares across multiple ExaGrid appliances with global deduplication in a scale-out system, automating job management to ExaGrid appliances. ExaGrid's support of SOBR also automates the addition of appliances into an ExaGrid system as data grows by simply adding appliances to a Veeam repository group. The combination of Veeam SOBR and ExaGrid's appliances in a scale-out system creates a tightly integrated end-to-end backup solution that allows backup administrators to leverage the advantages of scale-out in both the backup application as well as the backup storage. The combination of Veeam backups to the ExaGrid disk-cache Landing Zone, the integrated ExaGrid-Veeam Accelerated Data Mover, and ExaGrid's support of Veeam SOBR is the most tightly integrated solution on the market for a scale-out backup application to scale-out backup storage.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1751

Rubrik

ExaGrid improves the storage economics of Rubrik environments by working with Rubrik compression and deduplication and can achieve an additional reduction of 3:1 to 10:1 in addition to Rubrik's compression and encryption, further reducing storage by as much as 90% depending on the retention. The combined deduplication is between 6:1 and 20:1 depending on retention.

When using Rubrik Archive Tier with Instant Archive enabled, it is common to keep 2 weeks of retention on Rubrik and then write archive data (retention beyond the 2 weeks) or Instant Archive data (duplicative copy of the data on the Rubrik plus retention data) to either cloud storage or on-premise archive storage.

ExaGrid can considerably reduce the storage costs.

- Versus cloud storage, ExaGrid will be far less over time and restores of the data are faster from an on-premise ExaGrid system than pulling the data from the Cloud
- Versus on-premise archive storage, ExaGrid will be far less due to deduplication

In both cases, ExaGrid brings further value when using the Rubrik Archive Tier with Instant Archive enabled:

- ExaGrid's Retention Time-Lock for Ransomware Recovery (RTL) for an additional layer of recoverability behind Rubrik's ransomware recovery
- Disaster recovery, when leveraging ExaGrid at a second data center

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1752

Commvault

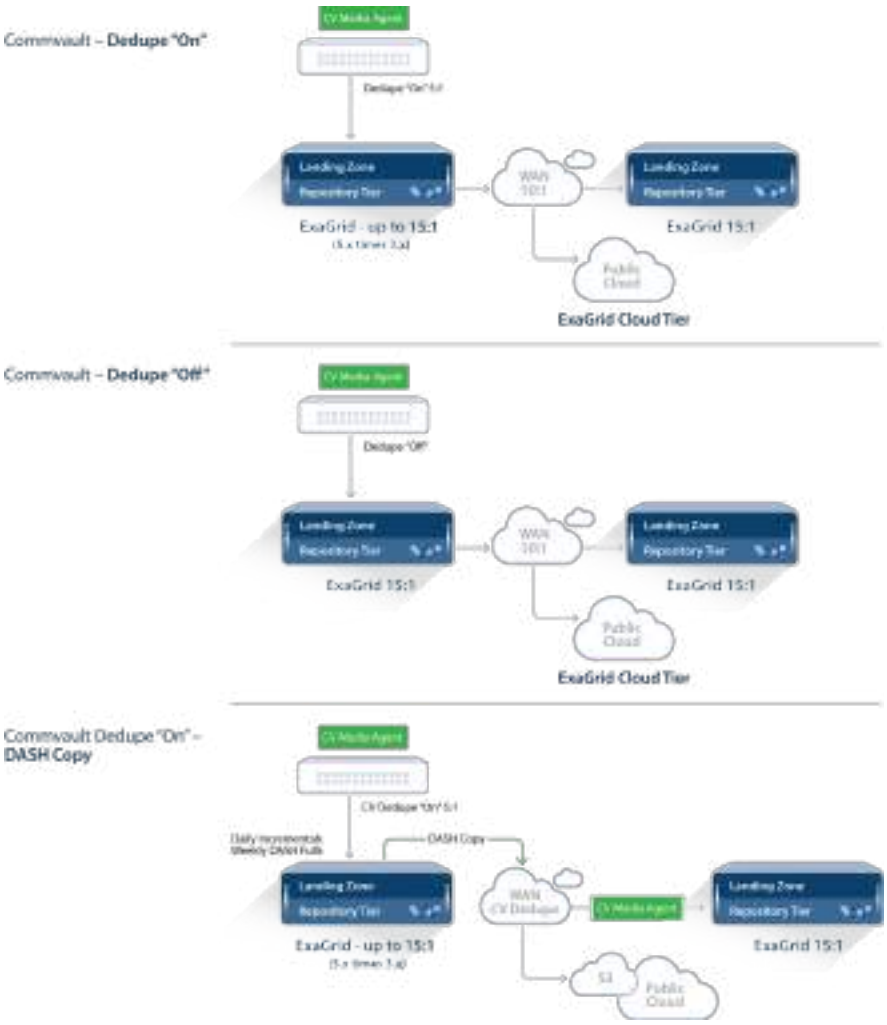
ExaGrid allows for Commvault compression and deduplication to be enabled or disabled. ExaGrid further deduplicates the Commvault data by a factor of 3X greatly reducing the amount of backup storage required.

ExaGrid can also allow users to turn Commvault deduplication off, with Commvault compression either turned on or off, to increase backup performance while retaining the same cost storage as leaving Commvault deduplication on with ExaGrid's additional deduplication impact.

ExaGrid supports Commvault Spill & Fill for automatic job management where all jobs are sent to ExaGrid appliances in the system by Commvault automatically. Jobs can be sent to any appliance at any time as ExaGrid has both global deduplication across all appliances in the system and automatic load balancing of all long-term retention data repositories.

ExaGrid brings the following value to Commvault environments

- Lower cost storage by further deduplicating Commvault deduplicated data by an additional 3X increasing performance by 20% to 30% by performing data encryption at rest at the drive level freeing up the Commvault agents resulting in increased throughput performance
- Scale-out storage architecture to keep the backup window fixed-length as data grows
- Non-network-facing tier with delayed deletes and immutable data objects to ensure recovery of data from a ransomware attack or other security event



Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1753

Oracle RMAN Channels

ExaGrid supports Oracle RMAN Channels targeted at multiple NAS shares across multiple appliances with global deduplication in a scale-out system. RMAN Channels automatically writes "sections" in parallel to all NAS shares and automatically redirects the next "section" based on available targets. RMAN Channels with ExaGrid has six major advantages.

1. A single Oracle database can be up to 6PB in size and can be backed up in parallel to a single ExaGrid scale-out system.

2. The database backup performance is accelerated as the sections are backed up in parallel across multiple appliances in a scale-out system.

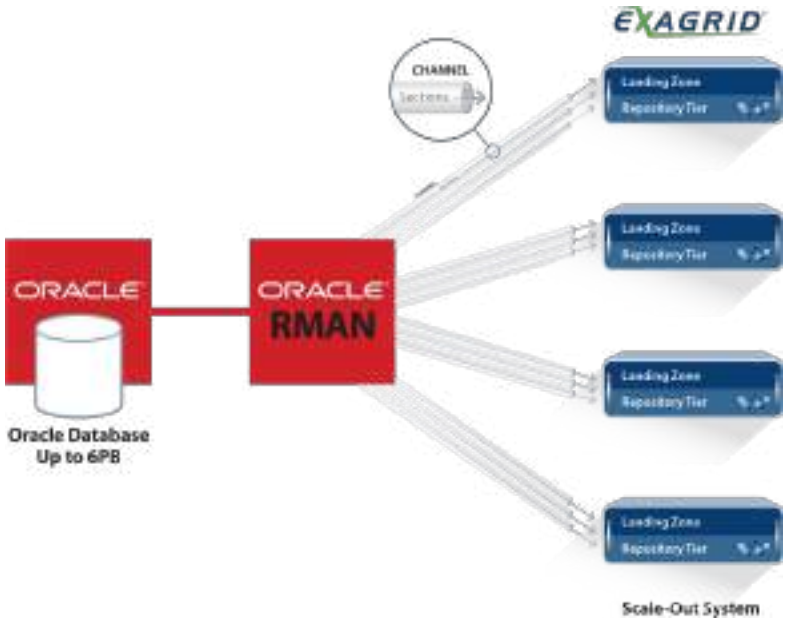
3. The database backup performance is maximized as each new section is automatically sent to the highest performance availability NAS shares and/or appliance, resulting in the best possible performance based on NAS share and appliance ingest availability.

4. If any appliance fails, the segments are automatically redirected to the active appliance, providing for automatic failover.

5. The most recent database is stored in an undeduplicated form in the ExaGrid disk-cache Landing Zone, allowing for fast restores while still allowing for storage efficiency as all long-term retention data is stored in deduplicated form. This avoids the lengthy data re-hydration process of inline scale-up appliances that only store deduplicated data.

6. As the database data grows, the backup window stays fixed in length as full appliances are added into a scale-out system bringing compute with capacity. This eliminates the forklift upgrades associated with inline scale-up deduplication appliances.

Database Backup Performance



Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1754

Security, Reliability, and Redundancy

Organizations using a disk-based backup appliance to hold their invaluable backup data should carefully consider how the appliance is architected for security, reliability, and redundancy. Compromises in a product's architecture or implementation may reduce product cost, but those savings are quickly negated by the risk and real cost to an organization of a loss of some or all backup data.

ExaGrid's architecture and implementation have multiple facets of reliability and redundancy, allowing organizations that are considering disk-based backup appliances to make informed vendor selections.

ExaGrid offers the following ease of use, redundancy and security features, some of which are explained below:

- Single user interface for all appliances in a system and across sites
- RAID 6 protection with a hot swappable spare
- Redundant hot swappable power supplies
- Active Directory for management interface and backup target security
- SNMP and sys-logging interface for integration with enterprise management apps
- Role-based access control
- Retention Time-Lock for Ransomware Recovery
- Two-factor authentication
- Data encrypted at rest
- Data encryption while replicating over the WAN
- Security checklist makes it easy to apply best practices
- Data is checksummed to ensure data integrity
- Internal self-describing database

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1755

ExaGrid Retention Time-Lock for Ransomware Recovery

ExaGrid's unique approach ransomware recovery is called Retention Time-Lock. It prevents threat actors/hackers from deleting the backup data. The result is a strong data protection and recovery solution at a very low cost of storage.

ExaGrid provides Tiered Backup Storage with a front-end disk-cache Landing Zone and separate Repository Tier containing all retention data. Data is written directly to the "network facing" ExaGrid disk-cache Landing Zone. Then it is tiered into a "non-network-facing" long-term retention Repository Tier (tiered air gap) where it is stored as deduplicated data objects to reduce the storage cost of long-term retention data. As data is tiered to the Repository Tier, it is deduplicated and stored in a series of objects and metadata. As with other object storage systems, the ExaGrid objects and metadata never change allowing only for the creation of new objects or deletion of old objects when retention is reached.

ExaGrid's approach to ransomware allows organizations to set up a time-lock period that governs the processing of any delete requests in the Repository Tier. In addition, this tier is non-network-facing and not accessible to hackers. The combination of a non-network-facing tier, a delayed deletion for a period of time and objects that never change (immutable) are the elements of the ExaGrid Retention Time-Lock solution.

For example, if the time lock period for the Repository Tier is set to 10 days, then when delete requests are sent to the ExaGrid from a backup application that has been compromised or from a hacked CIFS or other communications protocols, the data in the Repository Tier is time-locked for up to 10 days against any deletion. The data in the Landing Zone will be deleted or encrypted, however, the Repository Tier data is not deleted upon an external request for the configured period of time. When a ransomware attack is identified, simply put the ExaGrid system into a new recover mode and then restore any and all backup data to primary storage. The time lock period is separate and in addition to the days, week, months and year or retention that is set by the backup application and stored by ExaGrid in the Repository Tier.

The solution provides a retention lock, but only for an adjustable period of time as it delays the deletes. ExaGrid chose not to implement Retention Time-Lock forever because the cost of the storage would be unmanageable. ExaGrid already has the long term backup retention so it would be redundant to have a separate store with retention lock. With the ExaGrid delayed delete approach, all that is needed is up to an additional 10% more repository storage to hold the delay for the deletes. ExaGrid allows the delay of deletes to be changed from the 10 day default.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1756

ExaGrid advantages are:

- Manage a single system instead of multiple systems for both backup storage and ransomware recovery
- Unique second Repository Tier that is only visible to ExaGrid software, not to the network
- Data is not deleted as delete requests are delayed and therefore ready to recover after a ransomware attack
- Weekly, monthly, yearly, and other purges still occur to keep storage costs in line with the retention periods
- Only requires up to an additional 10% of repository storage
- Storage does not grow forever and stays within the backup retention period set to keep storage costs down
- All retention data is preserved and is not deleted

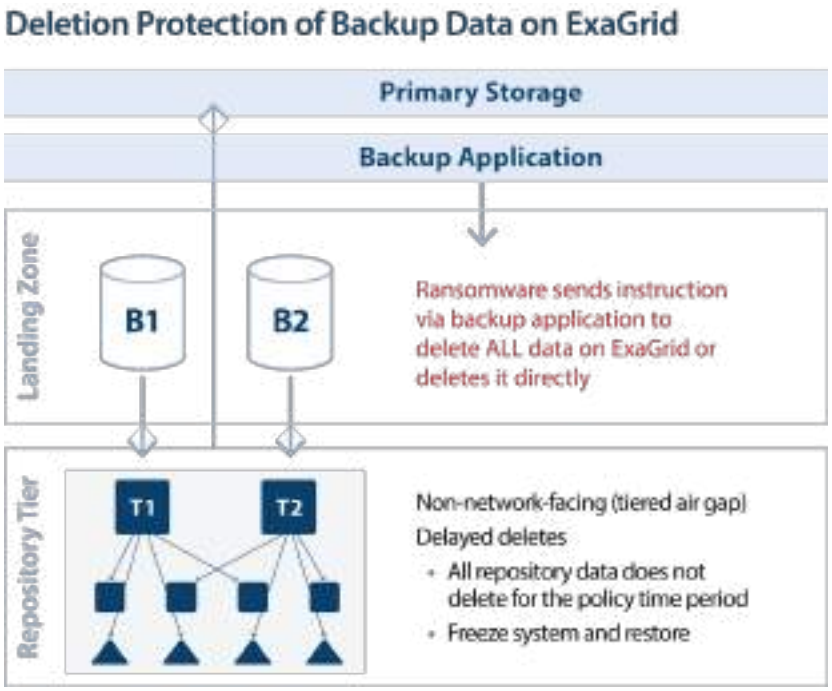
In addition, ExaGrid Retention-Time Lock includes

- Separate roles and logging for the backup IT staff and security to ensure check and balance when changing the security policy
- Two factor authentication (2FA)
- Alert on large delete threshold – early detection of a backup data deletion attack
- Alert on data deduplication ratio change – early detection of a backup data encryption attack

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1757

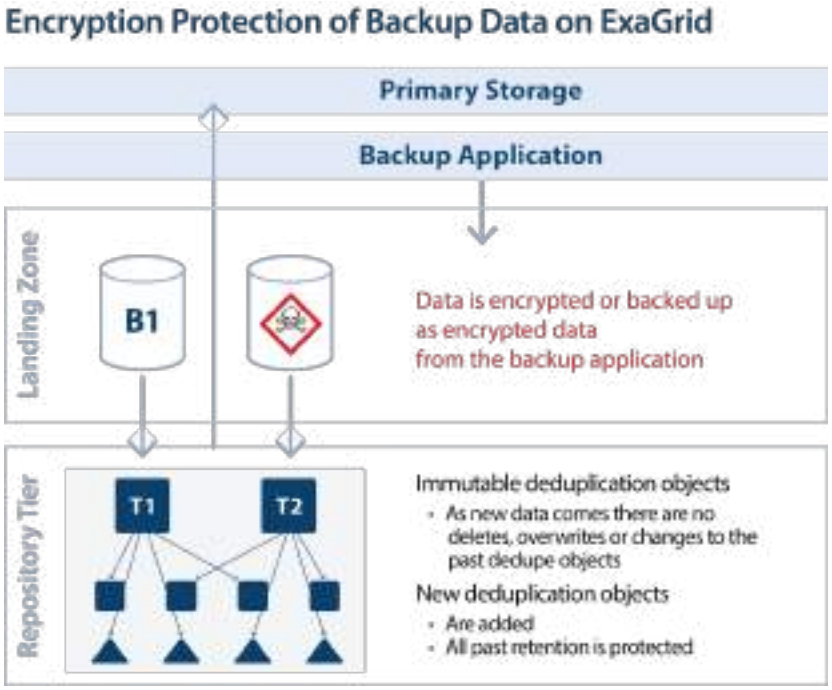
Example Scenarios

1) Data is deleted in the ExaGrid disk-cache Landing Zone via the backup application or by hacking the communication protocol. Since the Repository Tier data has a delayed delete time lock, the objects are still intact and available to restore. When the ransomware event is detected, simply put the ExaGrid in a new recover mode and restore. You have as much time to detect the ransomware attack as the time lock was set for on the ExaGrid. If you had the time lock set for 10 days, then you have 10 days to detect the ransomware attack and put the ExaGrid system in the new recover mode for restoring data.



Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1758

2) Data is encrypted in the ExaGrid disk-cache Landing Zone or is encrypted on the primary storage and backed up to ExaGrid such that ExaGrid has encrypted data in the Landing Zone and deduplicates it into the Repository Tier. The data in the Landing Zone is encrypted. However, all previously deduplicated data objects never change (immutable), so they are never impacted by the newly arrived encrypted data. ExaGrid has all previous backups before the ransomware attack that can be restored immediately. In addition to being able to recover from the most recent deduplicated backup, the system still retains all the backup data according to the retention requirements.



*Note: see **ExaGrid's Retention Time-Lock** data sheet for more detailed information.*

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1759

RAID 6 Internal Storage with Consistency Checking

All ExaGrid internal storage is accessed using an industry-leading PCI RAID controller at the RAID 6 level of disk protection with a global "hot spare" disk. Since RAID 6 keeps stripe parity on two disks, each ExaGrid appliance can tolerate the loss of up to two disk drives at the same time. The first lost disk drive will initiate a parity rebuild operation using the global hot spare as well as informing the backup administrator and (optionally) ExaGrid customer support of the failure. A replacement disk drive is dispatched quickly, typically allowing replacement of the failed disk the next business day. Loss of second disk does not result in loss of data since the remaining parity disk allows for data regeneration; this extends even longer the time available to replace the failed disk(s).

During normal operation, the RAID controller does consistency checking of the data on its disks in the background, correcting any disk media errors using the parity disks.

Flash-Backed RAID Cache

The industry-leading PCI RAID controller has onboard writeback cache backed up by a super-cap powered flash memory. Unexpected loss of appliance power does not result in backup data loss because any in-process writes to any disk are preserved until power is restored.

Backup Data Checksums with Automatic Repair

As backup data is deduplicated, checksums are added to the deduplicated data as it is placed into the internal storage area, called the "repository." These end-to-end checksums cover the deduplicated backup data itself, and are used to verify the backup data during processing and as it is read from disk. The deduplicated backup data can optionally be replicated to a remote site; these checksums are used to validate the replicated data as well.

The ExaGrid software continually scrubs the repository data, confirming checksums and automatically repairing any deduplicated data that does not match its checksum using data from remote site(s). This automatic repair of deduplicated data is covered by one of ExaGrid's patents.

Deduplicated Metadata Transactional Consistency

Metadata that tracks all of the deduplicated data is kept in a database and on internal storage. Software techniques are used to ensure transactional integrity of all metadata changes, including flushing filesystem pages into the flash-backed RAID onboard cache. The data flow of deduplicated backup data is protected end-to-end by the combination of checksums (above) and metadata transactional consistency.

Internal Database Backups and Self-Describing Metadata

The database used to keep metadata that tracks deduplicated data is periodically dumped to internal storage. These dumps are used to quickly restore the metadata database in the case of massive failure. The database dumps are used as an optimization; the metadata kept on disk is self-describing and can be used to completely rebuild the deduplicated data in the internal repository both at the local and remote ExaGrid sites.

Logging Filesystem

Backup data is kept in the ExaGrid internal storage on an industry-standard logging filesystem where file activity is logged for integrity and quick repair after an unclean shutdown.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1760

Data Security

The data security capabilities in the ExaGrid product line, including optional enterprise-class Self-Encrypting Drive (SED) technology, provide a high level of security for data at rest and can help reduce IT drive retirement costs in the data center. All data on the disk drive is encrypted automatically without any action required by users. Encryption and authentication keys are never accessible to outside systems where they can be stolen. Unlike software-based encryption methods, SEDs typically have a better throughput rate, particularly during extensive read operations.

Data can be encrypted during replication between ExaGrid systems. Encryption occurs on the sending ExaGrid system, is encrypted as it traverses the WAN, and is decrypted at the target ExaGrid system. This eliminates the need for a VPN to perform encryption across the WAN.

ExaGrid appliances include support of KMIP (Key Management Interoperability Protocol) using KMIP 1.4 standard, which ensures secure and efficient communication for key lifecycle operations, including key generation, retrieval, rotation, and deletion.

ExaGrid's larger appliance models, including the EX54,* EX81, EX84, EX135, and EX189, offer a Software Upgradeable SEC option to provide Data Encryption at Rest. SEC hardware models that provide Data Encryption at Rest are also available for ExaGrid's entire line of appliance models.

**Software Upgradeable SEC feature to add Data Encryption at Rest is available for select 2025 version EX54 models, not available for previous versions of EX54 models*

Active Directory Support

ExaGrid integrates with Windows Active Directory for centralized credentials management and authentication that can be used to authenticate and authorize access to the ExaGrid management interface and backup target shares.

Dedicated Managed Networks

- Better control of who has access to the ExaGrid management user interface
  - Management traffic on a dedicated NIC for security reasons
- Increased security by walling off the NICs (with a firewall) from external visibility and access outside of the ExaGrid appliance

Periodic Assessments Using a Network Vulnerability Scanner

A complete vulnerability assessment is run periodically against ExaGrid's software. Vulnerabilities flagged by this assessment are evaluated and tracked and mitigated as appropriate.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1761

Offsite Data Protection for Disaster Recovery

ExaGrid appliances can easily maintain offsite backups through the use of an offsite ExaGrid appliance in conjunction with a primary site ExaGrid appliance.

Backing up your data to an ExaGrid appliance at your primary site dramatically reduces the amount of disk space required to store all of that data due to its high-performance data deduplication capability. In a multi-site ExaGrid environment, the onsite ExaGrid system is only sending deduplicated data—the backup data that changes at a granular level between each backup—over the wide area network (WAN) to the offsite ExaGrid appliance. The offsite ExaGrid appliance is ready for data restore and fast recovery in the event of a disaster or other primary site outage.

If the replication is one way only, the second site/offsite ExaGrid can be half the capacity of the primary site ExaGrid greatly reducing overall cost.

Replication between ExaGrid systems across a WAN can be scheduled for the day of the week and multiple times throughout each day. Each scheduled period allows for bandwidth throttling which limits replication to only use the assigned bandwidth. The combination of scheduling flexibility and bandwidth throttling allows for the maximum efficiency of WAN bandwidth used for replication. Replicated data can be encrypted over the WAN using a customer's VPN or by utilizing the ExaGrid built-in replication encryption.

ExaGrid supports various DR options:

Private Cloud

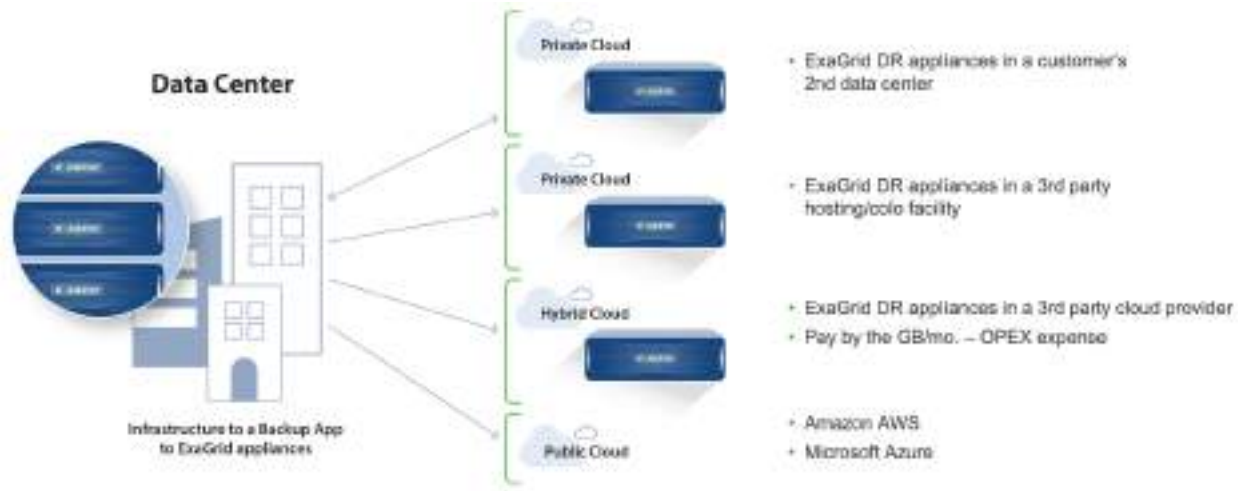
- Replicating to an ExaGrid at a customer's second data center (DR site)
- Replicating to an ExaGrid at a third-party hosted data center (DR site)

Hybrid Cloud

- Replicating to a Managed Service Provider (MSP)

Public Cloud

- Replicating to an ExaGrid VM in a public cloud (Amazon AWS, Microsoft Azure), where DR data is stored in the public cloud and billed by the GB per month using OPEX budget

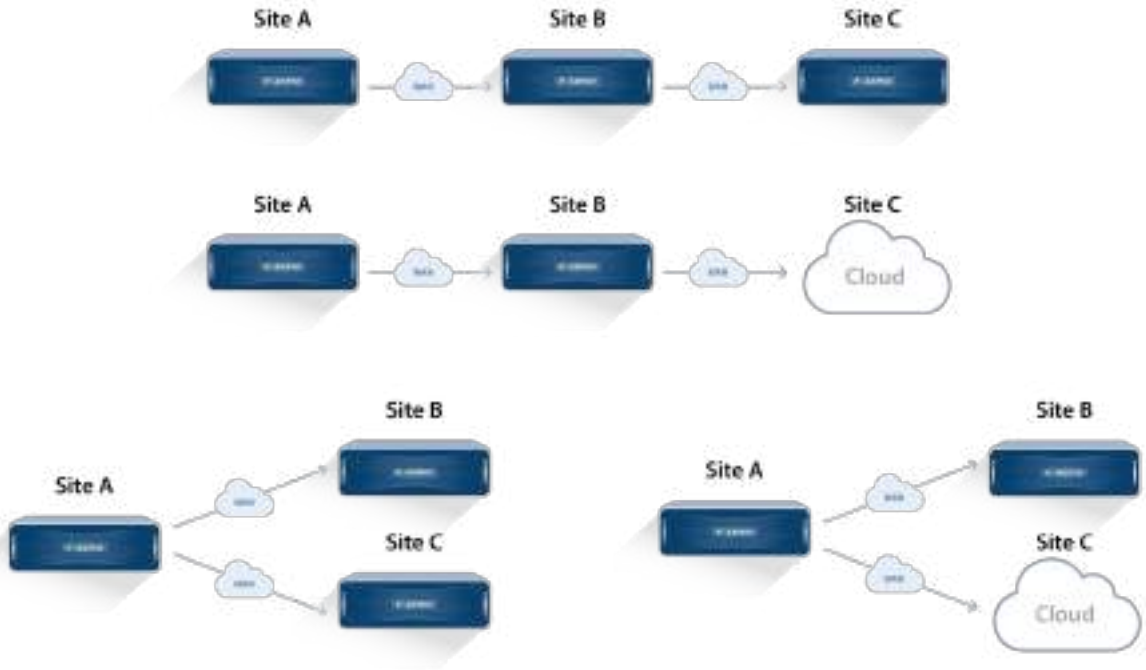


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1762

ExaGrid supports three models for private cloud DR sites at a customer's offsite data center:

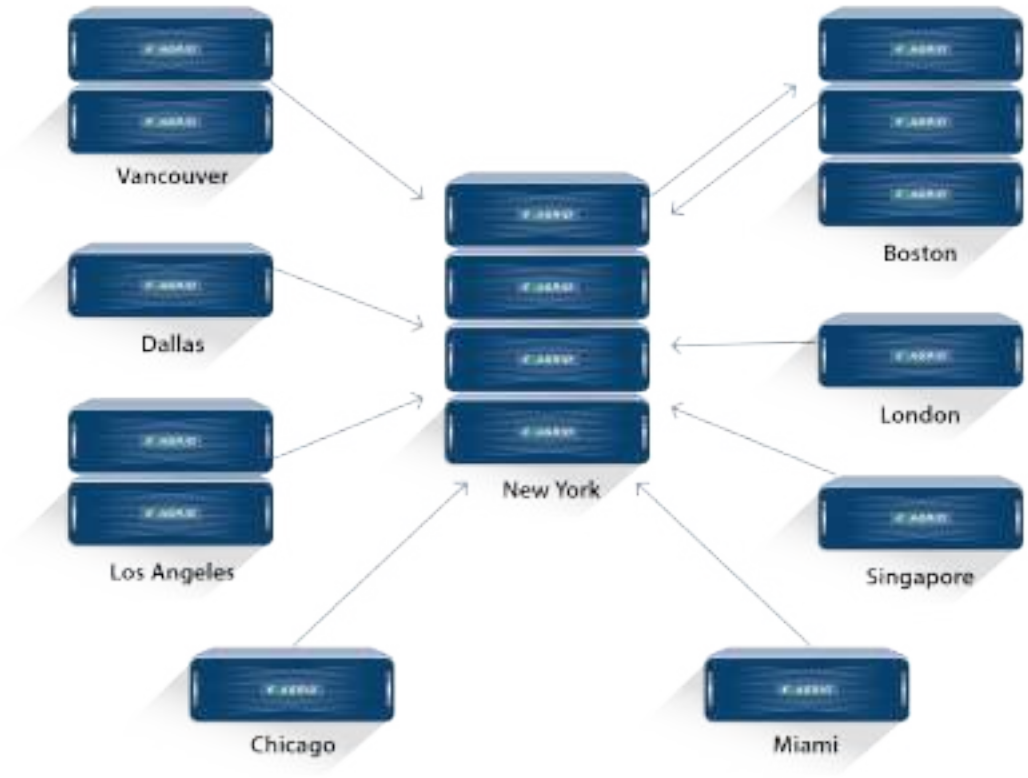
- **Unidirectional replication to offsite for disaster recovery** – In this use case, the entire offsite system can be configured for repository, allowing for a half-size system to be used offsite. ExaGrid is asymmetrical in this use case where all other solutions are symmetrical.
- **Cross protection** – Data can be backed up at both the offsite and onsite systems and cross replicated such that each site becomes the disaster recovery site for the other.
- **Multi-hop** – ExaGrid allows for a tertiary copy with two different topologies.
  - Site A can replicate to site B and then site B can replicate to site C
  - Site A can replicate to site B and site A can also replicate to site C
  - Site C can be a physical site or a cloud provider such as Amazon AWS and Microsoft Azure
- **Multiple data center sites** – ExaGrid can support up to 16 sites in a single hub and spoke topology with 15 spokes to a hub. Full systems or individual shares can be cross replicated such that data center sites can serve as disaster recovery sites for each other.

Multi Hop



Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1763

Multiple Data Center



Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1764

Total Cost of Ownership

Backup and disaster recovery is one area of IT spending which—though critically necessary—is typically viewed purely as cost. While backup is an extremely important area, organizations look to achieve appropriate protection so data is not lost while, at the same time, accomplishing this at the lowest possible cost. ExaGrid is the only vendor that has responded by creating a product that truly meets this different economic model warranted for backup spending. Backup spending has followed the same spending pattern as other IT infrastructure spending, which includes:

- Expensive forklift upgrades when a system is outgrown due to data growth
- Repurchasing of entire systems when an existing system simply "wears out"
- Complete rip-and-replace when a backup system becomes obsolete due to product end of life

ExaGrid redefines the economics of backup by helping you contain costs at every point in the life cycle — up front and as data grows over time.

ExaGrid offers the following to control costs:

- Over the phone/web installation at no charge – typically installed in a few hours
- No forklift upgrades
- No planned product obsolescence
- Scale-out architecture, pay as you grow
- For one-way replication – second site/DR site can be set to all repository, resulting in a system half the size at the DR site
- Everything is included in the yearly support and maintenance – no hidden cost
  - Local customer support in the Americas, EMEA and APAC – in-theater support
  - Assigned level 2 tech support engineer – work with the same person all the time
  - Automatic health monitoring
  - Full and point versions – all new features are included
  - No costs for failed hardware replacement
  - Spares depots around the world for fast failed hardware replacement
- Price protection
  - The price paid for appliances stays at the price for 5 years
  - Yearly maintenance and support will not increase more than 3% per year

Cost Effectiveness Up Front

With ExaGrid Tiered Backup Storage, backups are written directly to a disk-cache Landing Zone, avoiding inline processing and ensuring the highest possible backup performance resulting in the shortest backup window. Adaptive Deduplication performs deduplication and replication in parallel with backups while providing full system resources to the backups for the for the strongest offsite recovery point (RPO). Available system cycles are utilized to perform deduplication and offsite replication for an optimal recovery point at the disaster recovery site. Once complete, the onsite data is protected and immediately available in its full undeduplicated form for fast restores, VM Instant Boot and Recoveries, and tape copies while the offsite data is ready for disaster recovery. This allows ExaGrid to be more cost effective up front than an inline/block deduplication system.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1765

In contrast, other appliances that use inline, block-level deduplication rely on a top-tier processor with large amounts of very fast memory and disk just to keep up with backup data. The premium cost of these components means higher cost compared to ExaGrid appliances. In addition, since the inline scale-up appliances have a fixed and limited ingest, in order to increase ingest, they need to use compute from elsewhere in the environment. To this end, they deploy software on media servers and certain application servers in order to do some of the deduplication work away from the inline appliance. Not only is deploying agents frowned upon by most IT organizations, but even with this approach, the ExaGrid will still be 3X the ingest performance, and with ExaGrid there are no agents to deploy or manage.

When comparing ExaGrid appliances deduplication in the backup application software, it is important to keep in mind that using deduplication in the backup application software typically requires greater resources on the backup server—more processing power, more memory, and more disk. Software deduplication merely shifts the backup performance bottleneck to the media server. Using data deduplication in the backup software uses more disk and bandwidth over time and does not allow for backup environment flexibility such as using a separate utility for virtualized backup, direct TAR backups, and direct database dumps such as SQL dumps or Oracle RMAN dumps. ExaGrid's performance will be the fastest and deduplication will be three to ten times more efficient. In addition, ExaGrid allows Veeam and Commvault deduplication to be turned on and ExaGrid with further deduplicate that data greatly increasing the deduplication ratio to save on storage costs.

Cost Effectiveness as Data Grows

ExaGrid's integrated Landing Zone with unique architecture—full appliances in a scale-out architecture is the most cost-effective way to scale as data grows. Each ExaGrid appliance added to the system includes a full server with additional processor, memory, bandwidth, and disk resources. Total backup capacity keeps pace with continued data growth over time by simply adding ExaGrid appliances to the system. There are no forklift upgrades and no additional future costs to consider.

Other appliances that use inline, block-level deduplication do not support a scale-out architecture and are therefore more costly to scale. Instead of adding capacity by adding full servers, only disk shelves are added over time as data grows. But, at some point, the single front-end controller becomes a bottleneck due to its fixed processor, memory and bandwidth resources and can no longer handle the backup load. Eventually, the entire front-end server must be replaced with the next higher capacity unit in a "forklift upgrade." In fact, you may have to spend as much for the front-end controller upgrade as you originally spent on the original system, including disk shelves. In addition, all data is always deduplicated. For each restore, recovery, and copy request, the data has to be put back together, or "re-hydrated," which can take hours to days.

In addition, unlike other appliances that "end-of-life" in as little as 18 months and are incompatible with newer models from the same vendor, ExaGrid's scale-out architecture allows you to "mix and match" different capacities and generations of appliances within a single system. Only ExaGrid protects your backup investment from obsolescence.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1766

Summary

When organizations evaluate the backup solution and company that can best meet their backup needs and address their challenges, more and more IT organizations are finding that ExaGrid offers not only the fastest backup and restore performance, best scalability and most comprehensive security, but also a total cost of ownership that is typically half that of other solutions.

ExaGrid offers the largest backup storage system in the industry that includes data deduplication. ExaGrid can take in a 6PB full backup including retention and reduce storage capacity by 10:1 to as much as 50:1 depending on data types and retention periods.

Only ExaGrid's unique scale-out architecture and Adaptive Deduplication provide:

Landing Zone Tier

- Fastest backups – optimized for large backup jobs and also avoids inline deduplication bottlenecks
- Fastest restores – no deduplicated data rehydration required
- Supports: CIFS, NFS, Veeam Data Mover, Veritas OST, and S3 Object Storage

Repository Tier

- Low-cost long-term deduplicated retention storage
- Industry-leading 20:1 data deduplication
  - Global Deduplication
- Adaptive Deduplication
- Deduplicates and replicates during the backup window
- Strong offsite RTO and RPO
- Retention Time-Lock for Ransomware Recovery
- Non-network-facing tier
- Delayed deletes
- Immutable deduplication objects

Scale-out Architecture

- High density 2U appliance models for rack space efficiency
- Scales to a 6PB full back up in a single system
- Fixed-length backup window as backup data grows
- Eliminates forklift upgrades of scale-up architectures
- Mix and match appliances – any age and any size
- No planned product obsolescence (no end of life of maintenance and support)
- 8 different capacity sized appliance models
- Scales as your data grows

Disaster Recovery Site options

- Can replicate offsite for DR
- DR site capacity is half the capacity of primary – asymmetrical
- Fewer appliances
- Lower cost
- Cross replication from site A to B and B to A
- Up to 16 sites in a hub and spoke topology
- Multi-hop – site A to B to C, site A to B, and site A to C
- Public Cloud DR site – Amazon AWS and Microsoft Azure

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1767

Easy to Install Appliance Model

- Remote installation in a few hours

Redundancy

- RAID 6 disk storage protection with a hot spare
- Hot swappable storage drives
- Can survive two simultaneous drive failures
- Redundant power supplies
- System runs if either power supply fails

Integrated Systems Management and Security

- Single user interface for all appliances in a system and across sites
- Active Directory for management interface and backup target security
- SNMP interface for integration with enterprise management apps
- IPMI port
- Role-based access control
- Retention Time-Lock for Ransomware Recovery
  - Non-network-facing tier
  - Delayed deletes
  - Immutable deduplication objects
- Two-factor authentication
- Data encrypted at rest
- Data encryption while replicating over the WAN
- Support of KMIP (Key Management Interoperability Protocol) using KMIP 1.4 standard
- Security checklist makes it easy to apply best practices
- Data is checksummed to ensure data integrity
- System logging to external enterprise management applications
- Internal self-describing database

Backup Application Support

- Over 25 backup applications and utilities
- Supports heterogeneous backup application environments
- Veeam
  - Integrated Veeam Data Mover for improved backup performance
  - Scale-Out Backup Repository (SOBR) – automation for job management
  - Support of S3 object storage with object locking
  - Veeam Backup for Microsoft 365 directly to ExaGrid
  - Support of Veeam Fast clone for 30x faster synthetic fulls with automatic re-synthesis for fastest restores of synthetic fulls
  - Improved security
  - Veeam deduplication can be enabled and ExaGrid deduplicates further
- Veritas NetBackup
  - Storage target behind Veritas physical media servers
  - OST integration
  - Accelerator support
  - Auto Image Replication (AIR)
  - Optimized Duplication (Replication)
  - Instant Recovery
  - Granular Recovery Technology (Exchange, SharePoint, VMs)
  - Veritas Analytics
  - Veritas Single Target Storage Pool
- Rubrik
  - Rubrik compression, deduplication, and encryption can be enabled and ExaGrid deduplicates further

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1768

Backup Application Support

- Commvault
  - Commvault compression and deduplication can be enabled and ExaGrid deduplicates further
  - Commvault compression and deduplication can be disabled and ExaGrid deduplicates further
  - Spill and Fill support
  - Encryption at rest performed at the drive level for faster performance
- Oracle RMAN Channel backup support
- SQL Dumps Direct
  - If encryption is enabled in the SQL application (TDA), then ExaGrid can achieve about a 4:1 data reduction with advanced Adaptive Data Deduplication

Worldwide Distribution and Support

- Over 4,700 installed customers with tens of thousands of appliances
- Installed in more than 80 countries
- Spares depots around the world
- In-theater customer support, speaking local languages, around the world
- Included automatic health check system
- Assigned level-2 support engineer
- Work with the same senior level tech all the time
- +81 NPS score

Programs

- Product price protection for 5 years
- Maintenance and support price protection – won't go up more than 3% per year

About ExaGrid

ExaGrid provides Tiered Backup Storage with a unique disk-cache Landing Zone, long-term retention repository, and scale-out architecture. ExaGrid's Landing Zone provides for the fastest backups, restores, and instant VM recoveries. The Repository Tier offers the lowest cost for long-term retention.

ExaGrid's scale-out architecture includes full appliances and ensures a fixed-length backup window as data grows, eliminating expensive forklift upgrades and planned product obsolescence. ExaGrid offers the only two-tiered backup storage approach with a non-network-facing tier (tiered air gap), delayed deletes, and immutable objects to recover from ransomware attacks.

Visit us at **exagrid.com** or connect with us on LinkedIn. See what our customers have to say about their own ExaGrid experiences and why they now spend significantly less time on backup in our **customer success stories**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1769

United States 100 Campus Drive / Marlborough, MA 01752 / (800) 868-6985
United Kingdom 200 Brook Drive / Green Park, Reading, Berkshire RG2 6UB / +44 (0) 1189 497 051
Singapore 1 Raffles Place, #20-61 / One Raffles Place Tower 2 / 048616 / +65 6808 5574

ExaGrid reserves the right to change specifications or other product information without notice. ExaGrid and the ExaGrid logo are trademarks of ExaGrid Systems, Inc. All other trademarks are the property of their respective holders.

©2025 ExaGrid Systems, Inc. All rights reserved.

★★★★★

ExaGrid Tiered Backup Storage

Fastest Backups

Fastest Recoveries

Unparalleled, Cost-effective Scale-out

Comprehensive Security and Ransomware Recovery

ExaGrid Tiered Backup Storage

Product Line Configurations

ExaGrid provides Tiered Backup Storage with a unique disk-cache Landing Zone, long-term retention repository, and scale-out architecture. The system scales as needed by adding ExaGrid appliances, which virtualize into a single scale-out system automatically, adding capacity and processing power while acting and being managed as one unified system.

ExaGrid Tiered Backup Storage utilizes a scale-out architecture, where each appliance has both compute and capacity which allows the system to linearly scale which provides a fixed-length backup window as data grows. The front-end disk-cache Landing Zone, along with Adaptive Deduplication, coupled with a non-network-facing Repository Tier allows for:

- Fastest backups and shortest backup windows with optimal recovery point at disaster recovery site
- Fastest full system restore (from fully hydrated backup copy on disk)
- Boot a VM in minutes versus hours
- Fixed-length backup window as data grows
- Non-network-facing tier with delayed deletes and immutable data objects in order to recover from a security event such as a ransomware attack
- Integrations with backup application scale-out features
- Automatic load balancing and global deduplication
- Seamless scalability as data grows with no forklift upgrades
- No planned product obsolescence, as any age and any size appliance can be mixed and matched in a single system
- Protected data at rest with 256-bit AES encryption (available in ExaGrid SEC hardware models or using Software Upgradeable SEC in select appliance models); data is encrypted on the disk storage using FIPS 140-2 Validated
- Self-Encrypting Drives (SEDs) for data encryption at rest in nanoseconds, improving backup performance

ExaGrid Model	Raw Capacity (TB)	Usable Capacity (TB)	Capacity for Weekly Full (TB)	Max Backup Thruput (TB/hr)	Form Factor	Optional Data at Rest Encryption (SEC)
ExaGrid Appliances						
EX36	96	72	36	7.90	2U	√
EX54	162	108	54	5.80	2U	√√
EX81	216	162	81	8.70	2U	√√
EX84	192	168	84	15.25	2U	√√
EX135	324	270	135	14.50	2U	√√
EX189	432	378	189	20.30	2U	√√

In addition, ExaGrid offers these appliance models to accommodate larger organizations that have smaller data center locations worldwide:

ExaGrid Model	Raw Capacity (TB)	Usable Capacity (TB)	Capacity for Weekly Full (TB)	Max Backup Thruput (TB/hr)	Form Factor	Optional Data at Rest Encryption (SEC)
ExaGrid Appliances for larger accounts with smaller data center locations						
EX10	32	20	10	3.90	2U	√
EX20	64	40	20	4.40	2U	√

√√ = Software Updgradeable SEC for Data Encryption at Rest

(Note: available in select 2025 version EX54 models, not available in previous EX54 models)

With ExaGrid Tiered Backup Storage, backups are written directly to a disk-cache Landing Zone to avoid inline processing and ensure the highest possible backup performance, resulting in the shortest backup window. Adaptive Deduplication performs deduplication and replication in parallel with backups while providing full system resources to the backups for the shortest backup window. Available system cycles are utilized to perform deduplication and offsite replication for an optimal recovery point at the disaster recovery site. Once complete, the onsite data is protected and immediately available in its full undeduplicated form for fast restores, VM Instant Recoveries, and tape copies while the offsite data is ready for disaster recovery.

Simple, Turnkey Appliances

ExaGrid's appliances work seamlessly with the industry's leading backup applications and typically installs in about 30 minutes to 3 hours. The product line's multiple appliance models can be combined into a single scale-out system of up to 12.09 PB usable capacity, allowing full backups of up to 6.04PB.

ExaGrid appliances are comprised of Intel® or AMD processors, enterprise SAS drives, RAID6 with hot spare, and ExaGrid software. Since each appliance includes the appropriate amount of processor, memory, disk, and bandwidth for the data size, as each appliance is added into a single scale-out system, performance is maintained and backup times do not increase as data is added. This combination of capabilities in a turnkey appliance makes the ExaGrid system easy to install, manage, and scale.

Comprehensive Security Features — External Key Management and Data Encryption at Rest (SEC options)

ExaGrid appliances include support of KMIP (Key Management Interoperability Protocol) using KMIP 1.4 standard, which ensures secure and efficient communication for key lifecycle operations, including key generation, retrieval, rotation, and deletion.

ExaGrid's larger appliance models, including the EX54,* EX81, EX84, EX135, and EX189, offer a Software Upgradeable SEC option to provide Data Encryption at Rest. SEC hardware models that provide Data Encryption at Rest are also available for ExaGrid's entire line of appliance models.

**Software Upgradeable SEC feature to add Data Encryption at Rest is available for select 2025 version EX54 models, not available for previous versions of EX54 models*

Scalable Architecture

Multiple core ExaGrid disk-based backup appliances include scale-out computing software which allows them to virtualize into one another when added to the system. Once virtualized, they appear as a single pool of long-term capacity. Capacity load balancing of all data across servers is automatic, and multiple systems can be combined for additional capacity. Data is load balanced across all appliances in the system to ensure the best deduplicated storage efficiency.

High Density 2U Models for Rackspace Efficiency

All ExaGrid appliance models are in a 2U form factor, offering rack space efficiency which allows organizations to save on rack storage and cooling costs while accommodating large data backups and future data growth.

United States 100 Campus Drive / Marlborough, MA 01752 / (800) 868-6985
United Kingdom 200 Brook Drive / Green Park, Reading, Berkshire RG2 6UB / +44 (0) 1189 497 051
Singapore 1 Raffles Place, #20-61 / One Raffles Place Tower 2 / 048616 / +65 6808 5574

exagrid.com

ExaGrid reserves the right to change specifications or other product information without notice. ExaGrid and the ExaGrid logo are trademarks of ExaGrid Systems, Inc. All other trademarks are the property of their respective holders. ©2025 ExaGrid Systems, Inc. All rights reserved.
4.2025

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1772

★★★★★

ExaGrid Tiered Backup Storage

Fastest Backups

Fastest Recoveries

Unparalleled, Cost-effective Scale-out

Comprehensive Security and Ransomware Recovery

ExaGrid Product Overview

Tiered Backup Storage

ExaGrid's unique approach to backup storage delivers the fastest backups, restores, VM boots, offsite tape copies, copy jobs, and AUX copies, as well as the only fixed-length backup window as data grows. In addition, ExaGrid's scale-out architecture and various size appliances allows customers to buy what they need as they need it, avoiding disruptive and costly forklift upgrades. Customers are able to mix older and newer appliances in the same scale-out system, eliminating product obsolescence and protecting their IT investment up front and over time. ExaGrid's non-networking-facing Repository Tier (tiered air gap) with delayed deletes and immutable data objects ensure that data is read to be restored after a ransomware attack or other security event.

Fastest Backups for the Shortest Backup Window

ExaGrid provides advanced and aggressive data deduplication, matching the high deduplication ratios in the industry of 10:1 to as high as 50:1 data reduction, with an average of 20:1, depending on retention periods and data types. However, ExaGrid understands that data deduplication is highly compute intensive and should not be performed during the backup window as the deduplication will slow down ingest performance and, as a result, will lengthen the backup window.

ExaGrid provides a unique disk-cache Landing Zone in each appliance where backups are written directly to disk so that the compute-intensive data deduplication process doesn't impact ingest speed. This approach provides the fastest backup ingest rate of any other deduplication solution. ExaGrid uses Adaptive Deduplication to deduplicate and replicate data to the disaster recovery (DR) site during the backup window (in parallel with the backups) but not inline between the backup application and the disk. In addition, ExaGrid is optimized for large backup jobs, uses advanced transport protocols and job concurrency to further accelerate backup performance. This unique combination of a Landing Zone with adaptive deduplication, along with other performance features and functionality, provides for the fastest backup performance. This results in the shortest backup window as well as a strong disaster recovery point (RPO).

Fastest Restores, VM Boots, and Offsite Tape Copies

Ninety-five percent or more of the total volume of restores, VM boots, and offsite tape copies come from the most recent backup to keep users productive. Keeping the most the most recent backup in only deduplicated form will require a compute-intensive, time-consuming data "rehydration" process that will slow down restore requests. VM boots can take hours from deduplicated data. Since ExaGrid writes directly to the disk-cache Landing Zone, the most recent backups are kept in their full, undeduplicated, native form. All restores, VM boots, and offsite tape copies are fast since the overhead of the data rehydration process is avoided. As an example, ExaGrid can provide the data for a VM boot in seconds to single-digit minutes versus hours for inline data deduplication backup storage appliances that only store deduplicated data. ExaGrid maintains all long-term retention (weeks, months, years) in a deduplicated format for storage efficiency.

Fixed-Length Backup Window

Since data deduplication uses a lot of processor and memory resources, as data grows, the amount of data deduplication to be performed grows as well. The first generation of deduplication storage appliances utilize a "scale-up" storage approach with a fixed resource front-end controller and disk shelves. As data grows, they only add storage capacity.

Because the compute, processor, and memory are all fixed, as data continues to grow, so does the time it takes to deduplicate the data. The backup window becomes so long that the front-end controller has to be upgraded (called a "forklift" upgrade) to a larger/faster controller, which is disruptive and costly. Similarly, deduplication that is built into the backup software is far less aggressive, uses a larger amount of disk, and is much slower for backups and restores.

ExaGrid provides Tiered Backup Storage with a unique disk-cache Landing Zone, long-term retention repository, and scale-out architecture. ExaGrid's Landing Zone provides for the fastest backups, restores, and instant VM recoveries. The non-network-facing retention repository offers the lowest cost for long-term retention. ExaGrid's scale-out architecture includes full appliances and ensures a fixed-length backup window as data grows, eliminating expensive forklift upgrades and product obsolescence.

Highest Performance for Backups

- Fastest backup performance for the shortest backup window by writing directly to a disk-cache Landing Zone, avoiding compute-intensive inline data deduplication
- Backup windows kept permanently short as data grows by adding full servers (with processor, memory, disk, and bandwidth) in a single scale-out system
- Uses advanced protocols, job concurrency, optimization for large backup jobs, encryption at the drive level, and other functionality for improved performance

Fastest Restores and VM Boots for Instant Recovery

- Fastest restore and tape copy performance from the most recent backup kept in its whole form. No reassembly from small blocks and large hash tables is required
- Fast VM boots for instant recoveries from a high-speed Landing Zone, which maintains a non-deduplicated copy of the most recent backup. This approach avoids the time-consuming data rehydration required when using solutions that only store deduplicated data

Most Cost-Effective Solution with No "Forklift" Upgrades

- Scalable next-generation architecture with full appliances provides plug-and-play expansion. To add an ExaGrid appliance, you simply plug it in and let ExaGrid's scale-out software virtualize the backup capacity pool
- Multiple appliances allow full backups per appliance of 10TB, 20TB, 36TB, 54TB, 81TB, 84TB, 135TB, and 189TB. Appliances can be mixed and matched with up to 32 appliances in a single scale-out system, allowing you to pay as you grow. Newer appliances can be added to older appliances in the same system to eliminate product obsolescence. With thirty-two EX189 appliances, a single system can support 12PB of usable storage and can ingest a 6PB full backup
- 50% lower total system cost up front vs. competing systems. Over time, the total system cost is also 50% lower because the costly "forklift" upgrades associated with a first-generation front-end controller/disk shelf architecture are eliminated

Comprehensive Security

- Non-network-facing Repository Tier with delayed deletes and immutable data objects to recover from ransomware attacks and other security events
- Two-factor authentication (2FA)
- Role-based Access Control (RBAC) with separate Backup Operator, Admin and Security Officer roles, which are fully compartmentalized
    - Adding these roles to users can only be done by a user that already has the role – so a rogue admin cannot bypass Security Officer approval of sensitive data management actions
    - Key operations require Security Officer approval to protect against internal threats, such as share deletes and de-replication (when a rogue admin turns off replication to remote site)
- Dozens of other security features

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1774

Advanced Features

- Scale-out architecture allows for cost-effective growth, eliminates planned product obsolescence, and maintains a fixed-length backup window as data grows
- Unique Landing Zone reduces downtime by keeping a full copy of the most recent backup in complete form for instant recovery of VMs, full systems, and files. Competing solutions must rehydrate the most recent backup from millions or billions of deduplicated chunks causing much longer recovery time
- Non-network-facing tier (tiered air gap), delayed deletes, and immutable data objects to ensure recovery after a ransomware attack
- Adaptive Deduplication performs deduplication and replication in parallel with backups while providing full system resources to the backups for the shortest backup window and an optimal recovery point (RPO) at the DR site
- Plug and play expansion – various sized appliance models allow full backups of up to 189TB per appliance with a fastest ingest rate of 516TB/ hour. Combining up to 32 appliances in a single scale-out system allows for scalability up to a 6PB full backup (12PB usable storage). In addition, ExaGrid supports second-site repository storage of up to 12PB for DR and long-term retention
- Supports: CIFS, NFS, Veritas OST, Veeam Data Mover and S3 Object Store
- ExaGrid includes replication to an offsite ExaGrid for disaster recovery, cross replication for multi-site DR and supports offsite tape copy creation
- Private, hybrid, and public cloud DR support including Amazon AWS and Microsoft Azure
- Global deduplication across all appliances in a system
- Bandwidth throttling for WAN efficiency
- Management software notifies via SNMP or email that the system is reaching capacity thresholds
- RAID6 guards against up to two simultaneous disk failures
- Self-Encrypting Drive (SED) technology (encrypted models only) ensures that data at rest is always protected
- WAN encryption for secure data transfer
- Support of Oracle RMAN Channels for multi-hundred terabyte databases with automated performance load balancing and failover
- Support of Veeam Data Mover and Veeam Fast Clone for synthetic fulls that are 30x faster
- ExaGrid further deduplicates Veeam deduplicated data by 7x for an average 14:1 deduplication ratio, providing significant storage savings
- ExaGrid supports Veeam writing to ExaGrid Tiered Backup Storage as an S3 object store target, as well as Veeam Backup for Microsoft 365 directly to ExaGrid
- Support of Veeam SOBR for automated end-to-end scale-out backups to backup storage
- Support of Veritas NetBackup OST, Single Target Pool, and many other Veritas integrations
- ExaGrid increases Commvault deduplication ratio by 3x for a dedupe ratio of 15:1, and allows for Commvault compression and deduplication to be enabled or disabled
- Support of Commvault DASH fulls and DASH copies
- Support of HYCU for Nutanix AHV and ESXi as well as HYCU scale-out
- A comprehensive list of over 25 supported backup apps and utilities can be found **here**

United States 100 Campus Drive / Marlborough, MA 01752 / (800) 868-6985
United Kingdom 200 Brook Drive / Green Park, Reading, Berkshire RG2 6UB / +44 (0) 1189 497 051
Singapore 1 Raffles Place, #20-61 / One Raffles Place Tower 2 / 048616 / +65 6808 5574

exagrid.com

ExaGrid reserves the right to change specifications or other product information without notice. ExaGrid and the ExaGrid logo are trademarks of ExaGrid Systems, Inc. All other trademarks are the property of their respective holders. ©2025 ExaGrid Systems, Inc. All rights reserved.

Anexo Catalogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1775

★★★★★

ExaGrid Tiered Backup Storage

Fastest Backups

Fastest Recoveries

Unparalleled, Cost-effective Scale-out

Comprehensive Security and Ransomware Recovery

ExaGrid Tiered Backup Storage

Retention Time-Lock for Ransomware Recovery

Ransomware attacks are on the rise, becoming disruptive and potentially very costly to businesses. No matter how meticulously an organization follows best practices to protect valuable data, the attackers seem to stay one step ahead. They maliciously encrypt primary data, take control of the backup application and delete the backup data.

Protection from ransomware is a primary concern for organizations today. ExaGrid offers a unique approach to ensuring that attackers cannot compromise the backup data.

The challenge is how to protect the backup data from being deleted while at the same time allow for backup retention to be purged when retention points are achieved. If you retention lock all of the data, you cannot delete the retention points and the storage costs become untenable. If you allow retention points to be deleted to save storage, you leave the system open for hackers to delete all data.

ExaGrid's unique approach is called Retention Time-Lock (RTL). It prevents the threat actors/ hackers from deleting the backups and allows for retention points to be purged. The result is a strong data protection and recovery solution at a very low cost of storage.

ExaGrid is Tiered Backup Storage with a front-end disk-cache Landing Zone and separate Repository Tier containing all retention data. Data is written directly to the "network facing" ExaGrid disk-cache Landing Zone. Then it is tiered into a "non-network-facing" long-term retention repository where it is stored as deduplicated data objects to reduce the storage cost of long-term retention data. As data is tiered to the Repository Tier, it is deduplicated and stored in a series of objects and metadata. As with other object storage systems, the ExaGrid objects and metadata never change allowing only for the creation of new objects or deletion of old objects when retention is reached.

ExaGrid's approach to ransomware allows organizations to set up a time lock period that governs the processing of any delete requests in the Repository Tier as that tier is not network facing and not accessible to hackers. The combination of a non-network-facing tier, a delayed deletion for a period of time and objects that never change are the elements of the ExaGrid Retention Time-Lock solution. For example, if the time lock period for the Repository Tier is set to 10 days, then when delete requests are sent to the ExaGrid from a backup application that has been compromised or from a hacked CIFS or other communications protocols, the data in the Repository Tier is time-locked for up to 10 days against any deletion. The data in the Landing Zone will be deleted or encrypted, however, the Repository Tier data is not deleted upon an external request for the configured period of time. When a ransomware attack is identified, simply put the ExaGrid system into a new recover mode and then restore any and all backup data to primary storage. The time lock period is separate and in addition to the days, week, months and year or retention that is set by the backup application and stored by ExaGrid in the retention repository.

The solution provides a retention lock, but only for an adjustable period of time as it delays the deletes. ExaGrid chose not to implement Retention Time-Lock forever because the cost of the storage would be unmanageable. ExaGrid already has the long term backup retention so it would be redundant to have a separate store with retention lock. The 10-day default policy for delayed deletes only takes an additional 10% of storage space. ExaGrid allows the delay of deletes from 1 day to 30 days.

Recovery Process – 5 Easy Steps

- Invoke recover mode
  - Retention Time-Lock clock is stopped with all deletes put on hold indefinitely until data recovery operation is complete
- Contact assigned level 2 ExaGrid customer support engineer
  - The backup administrator can carry out the recovery using the ExaGrid GUI, but since this is not a common operation, we suggest contacting ExaGrid customer support
- Determine the time of the event so you can plan restore
- Determine which backup on the ExaGrid completed deduplication before the event
- Perform restore from that backup using the backup application

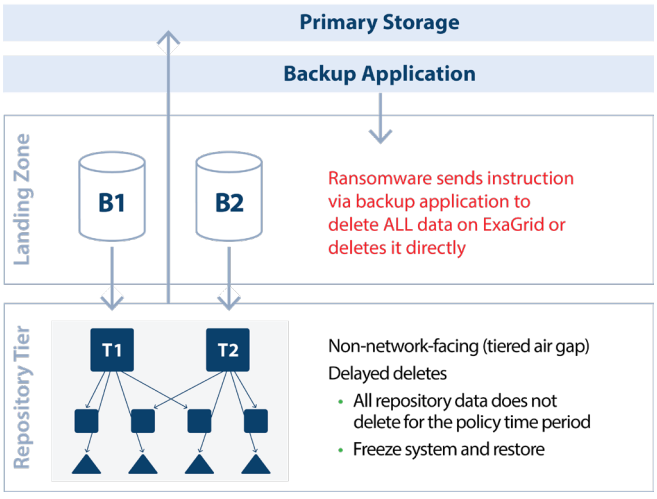
ExaGrid advantages are:

- Manage a single system instead of multiple systems for both backup storage and ransomware recovery
- Unique second Retention Tier that is only visible to ExaGrid software not to the network
- Data is not deleted as delete requests are delayed and therefore ready to recover after a ransomware attack
- Weekly, monthly, yearly and other purges still occur to keep storage costs in line with the retention periods
- The 10-day default policy for delayed deletes only takes an additional 5% to 10% of storage space
- Storage does not grow forever and stays within the backup retention period set to keep storage costs down
- All retention data (most recent backups and all retention) is preserved and is not deleted

Example Scenarios

- Data is deleted in the ExaGrid disk-cache Landing Zone via the backup application or by hacking the communication protocol. Since the Retention Tier data has a delayed delete time lock, the objects are still intact and available to restore. When the ransomware event is detected, simply put the ExaGrid in a new recover mode and restore. You have as much time to detect the ransomware attack as the time lock was set for on the ExaGrid. If you had the time lock set for 10 days, then you have 10 days to detect the ransomware attack and put the ExaGrid system in the new recover mode for restoring data.

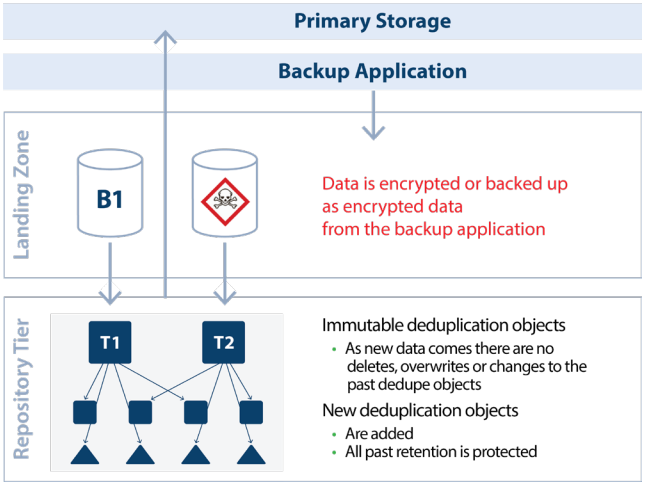
Deletion Protection of Backup Data on ExaGrid



Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1777

- Data is encrypted in the ExaGrid disk-cache Landing Zone or is encrypted on the primary storage and backed up to ExaGrid such that ExaGrid has encrypted data in the Landing Zone and deduplicates it into the Repository Tier. The data in the Landing Zone is encrypted. However, all previously deduplicated data objects never change (immutable), so they are never impacted by the newly arrived encrypted data. ExaGrid has all previous backups before the ransomware attack that can be restored immediately. In addition to being able to recover from the most recent deduplicated backup, the system still retains all the backup data according to the retention requirements.

Encryption Protection of Backup Data on ExaGrid



Features:

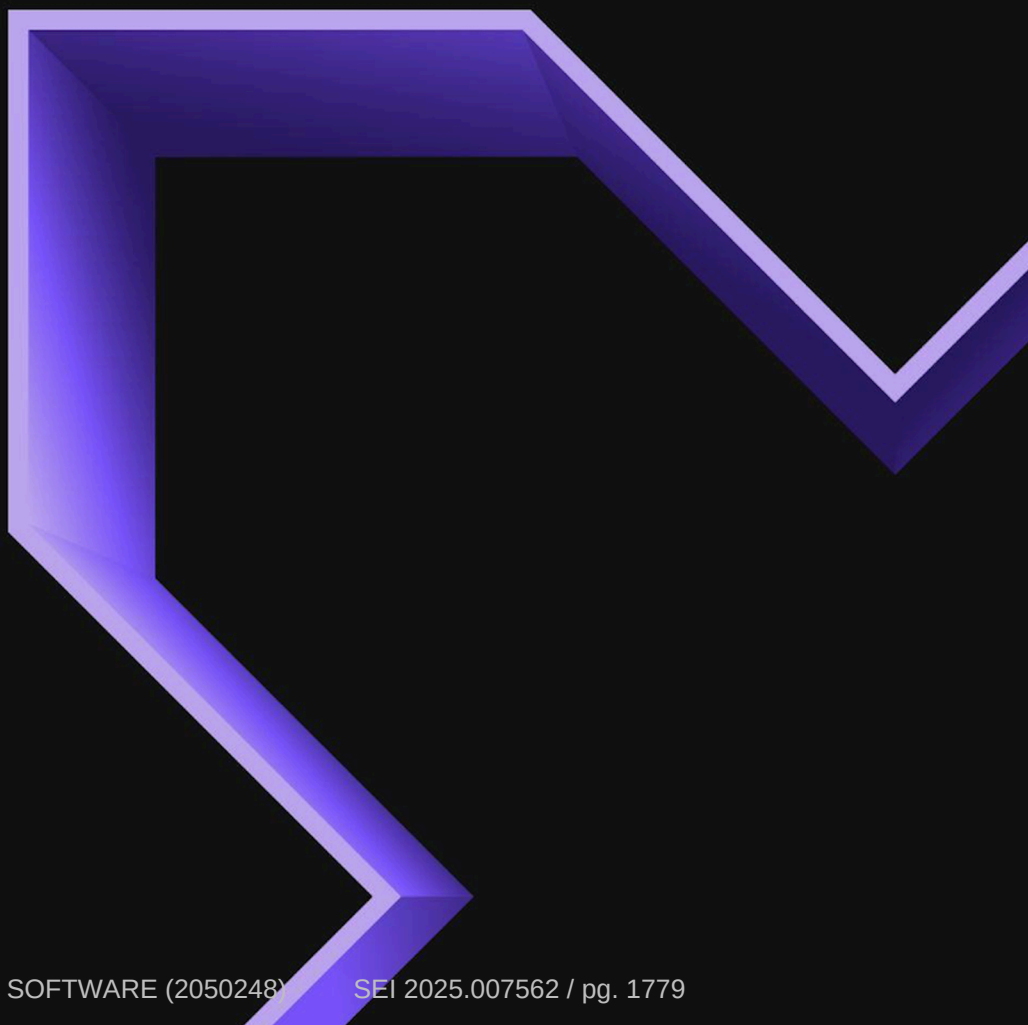
- Any deletion requests are delayed by the number of days in the protection policy
- Encrypted data written to ExaGrid does not delete or change previous backups in the repository
- Landing Zone data that is encrypted does not delete or change previous backups in the repository
- Set delayed deletion in 1 day increments from 0 days to 30 days
- Protects against loss of any and all retained backups including monthlies and yearlies
- Two-Factor Authentication (2FA) protects changes to Time-Lock setting
  - Only Security Officer role is allowed to approve changes to Time-Lock setting
  - 2FA with Login/Password and system generated QR code protects all accounts
- Separate password for primary site versus second site ExaGrid
- Separate backup staff and security staff roles and passwords
- **Alarm on Delete**
  - Alarm on large delete: A value can be set as a threshold by the backup administrator (default is 50%) and if a delete is more than the threshold, system will raise an alarm, only Admin role can clear this alarm.
  - A threshold can be configured, by individual share, based on backup pattern. (The default value is 50% for every share). When a delete request comes to the system, the ExaGrid system will honor the request and delete the data. If RTL is enabled, the data will be retained for the RTL policy (for the number of days set by an organization). When RTL is enabled, organizations will be able to recover the data using the PITR (Point-In-Time-Recovery).
  - If an organization gets false positive alarm frequently, the Admin role can adjust the threshold value from 1-99% to avoid more false alarms.
- Alarm on data deduplication ratio change
  - If primary storage is encrypted and sent to the ExaGrid from the backup application or if the threat actor encrypts the data on the ExaGrid Landing Zone, ExaGrid will see significant drop in the deduplication ratio being achieved and will send an alarm. The data in the Repository Tier remains protected.

ExaGrid reserves the right to change specifications or other product information without notice. ExaGrid and the ExaGrid logo are trademarks of ExaGrid Systems, Inc. All other trademarks are the property of their respective holders. ©2023 ExaGrid Systems, Inc. All rights reserved.

Flow Microsegmentation Guide

Flow Network Security (formerly Flow Microsegmentation) 6.5

September 13, 2024



NUTANIX

Contents

Security Policies....4

Types of Policies....5

Security Policy Model....7

Requirements....9

Enabling Microsegmentation....10
Disabling Microsegmentation....10

Built-in Categories for Security Policies....11

Services....12
Creating a Service....12

Addresses....13
Creating an Address....13

Allowing Discovered Traffic....14

Application Security Policy Configuration....17
Creating an Application Security Policy....17
Modifying an Application Security Policy....22
Applying an Application Security Policy....22
Monitoring an Application Security Policy (Visualizing Network Flows)....23
Deleting an Application Security Policy....24

Isolation Environment Policy Configuration....26
Creating an Isolation Environment Policy....27
Modifying an Isolation Environment Policy....29
Applying an Isolation Environment Policy....29
Monitoring an Isolation Environment Policy (Visualizing Network Flows)....29
Deleting an Isolation Environment Policy....30

Quarantine Policy Configuration....31
Configuring the Quarantine Policy....31

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1780

Quarantining a VM..... 33
Removing a VM from the Quarantine.....33

VDI Policy Configuration..... 34
Creating a VDI Policy.....34
Default VDI Policy..... 38
Configuring Active Directory Domain Services..... 38
Modifying the VDI Policy.....40
Applying the VDI Policy..... 40
Monitoring the VDI Policy..... 41
Deleting the VDI Policy.....41

Applying Filtering and Grouping to a Security Policy.....42

Exporting and Importing Security Policies..... 46

Copyright.....47

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1781

SECURITY POLICIES

Traditional data centers use firewalls to implement security checks at the perimeter—the points at which traffic enters and leaves the data center network. Such perimeter firewalls are effective at protecting the network from external threats. However, they offer no protection against threats that originate from within the data center and spread laterally, from one compromised machine to another.

The problem is compounded by virtualized workloads changing their network configurations and hosts as they start, stop, and migrate frequently. For example, IP addresses and MAC addresses can change as applications are shut down on one host and started on another. Manual enforcement of security policies through traditional firewalls, which rely on network configurations to inspect traffic, cannot keep up with these frequent changes and are error-prone.

Network-centric security policies also require the involvement of network security teams that have intimate knowledge of network configuration in terms of VLANs, subnets, and other network entities.

Nutanix Flow includes a policy-driven security framework that inspects traffic within the data center. The framework works as follows:

- Security policies inspect traffic that originates and terminates within a data center and help eliminate the need for additional firewalls within the data center.
- The framework uses a workload-centric approach instead of a network-centric approach. Therefore, it can scrutinize traffic to and from VMs no matter how their network configurations change and where they reside in the data center. The workload-centric, network-agnostic approach also enables the virtualization team to implement these security policies without having to rely on network security teams.
- Security policies are applied to categories (a logical grouping of VMs) and not to the VMs themselves. Therefore, it does not matter how many VMs are started up in a given category. Traffic associated with the VMs in a category is secured without administrative intervention, at any scale.
- Prism Central offers a visualization-based approach to configuring policies and monitoring the traffic to which a given policy applies.
- Using Prism Central, you can configure syslog monitoring by forwarding Flow logs to an external syslog server. For details, see Configuring Syslog Monitoring in the *Prism Central Admin Center Guide*.

> **Note:** Nutanix Flow supports only AHV hypervisor; security policies can not be applied to VMs running on other hypervisors.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1782

TYPES OF POLICIES

The types of policies in Prism Central and their use cases are described here.

Table 1: Types of Policies

Policy Type	Use Case
Application Security Policy	Use an application security policy when you want to secure an application by specifying allowed traffic sources and destinations. This method of securing an application is typically called *application ring fencing*. For example, use an application security policy when you want to allow only those VMs in the categories `department: engineering` and `department: customersupport` (the allowed sources) to communicate with an issue tracking tool in the category `AppType: IssueTracker` (the secured application), and you want the issue tracking tool to be able to send traffic only to an integrated customer relationship management application in the category `AppType: CRM`. The secured application itself can be divided into tiers by the use of categories (the built-in AppTier category). For example, you can divide the issue tracking tool into web, application, and database tiers and configure tier-to-tier rules. For more information, see Application Security Policy Configuration on page 17.
Isolation Environment Policy	Use an isolation environment policy when you want to block all traffic, regardless of direction, between two groups of VMs identified by their category. VMs within a group can communicate with each other. For example, use an isolation environment policy when you want to block all traffic between VMs in the category `Environment: sandbox` and VMs in the category `Environment: production`, and you want to allow all the VMs within each of those categories to communicate with each other. For more information, see Isolation Environment Policy Configuration on page 26.
Quarantine Policy	Use a quarantine policy when you want to isolate a compromised or infected VM and optionally want to subject it to forensics. For more information, see Quarantine Policy Configuration on page 31.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1783

Policy Type	Use Case
VDI Policy	Use a VDI policy when you want to secure your VDI environment. For more information, see VDI Policy Configuration on page 34

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1784

SECURITY POLICY MODEL

Application-centricity

The security policy model uses an application-centric policy language instead of the more complex, traditional network-centric policy language. Configuring an application security policy involves specifying which VMs belong to the application you want to protect and then identifying the entities or networks, in the inbound and outbound directions, with which you want to allow communication.

All the entities in an application security policy are identified by the categories to which they belong and not by their IP address, VLAN, or other network attributes. After a VM is associated with a category and the category is specified in a security policy, traffic associated with the VM is monitored even if it migrates to another network or changes its IP address.

The default options for allowing traffic on the inbound and outbound directions are also inherently application centric. For application security policies, the default option for inbound traffic is **Allowed List**, which means that **Allowed List** is usually the recommended option for inbound traffic. The default option can be changed to **Allow All** traffic. The default option in the outbound direction allows the application to send traffic to all destinations, but you can configure a destination **Allowed List** if desired.

For forensic quarantine policies, the default option in both directions is **Allowed List**, but you can **Allow All** traffic in both directions. For strict quarantine policies, no traffic is allowed in either direction.

All the VMs within a category can communicate with each other. For example, in a tiered application, regardless of how you configure tier-to-tier rules, the VMs within a given tier can communicate with each other.

Allowed List-Based Policy Expression

An application security policy is expressed in terms of the categories and subnets with which you want the application to communicate and therefore, by extension, the traffic you want to allow. A more granular policy expression can be achieved by specifying which protocols and ports can be used for communication.

Any category or subnet that is not in the allowed list is blocked. You cannot specify the categories and subnets you want to block because the number of such entities are typically much larger and grow at a much higher rate than the categories and subnets with which an application should be allowed to communicate. Expressing a policy in terms of allowed traffic results in a smaller, tighter policy configuration that can be modified, monitored, and controlled more easily.

Enforcement Modes

All policies, whether associated with securing an application, isolating environments, or quarantining VMs, can be run in the following modes:

Monitor Mode
: Allows all traffic, including traffic that is not allowed by the policy. This mode enables you to visualize both allowed and disallowed traffic and fine-tune the policy before applying it.

Enforce Mode
: Blocks all traffic that is not allowed by the policy.

You can switch a policy between these two modes as many times as you want.

Automated Enforcement

A policy uses categories to identify the VMs to which it must apply. This model allows the automatic enforcement of a policy to VMs regardless of their number and network attributes. Connectivity between Prism Central and a registered AHV cluster is required only when creating and modifying policies, or when changing the mode of operation (applied or monitoring) of a policy. Policies are applied to the VMs in a cluster even if the cluster temporarily loses network connectivity with the Prism Central instance with which it is registered. New policies and changes are applied to the cluster when connectivity is restored.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1785

Priorities Between Policies

Prism Central does not provide a way for you to specify priorities between policies of a single type. For example, you cannot prioritize one security policy over another. There is no limit to the number of inbound and outbound rules that you can add to a security policy, allowing you to define all of an application's security requirements in a single policy. This makes priorities between policies unnecessary.

However, priorities exist between the different policy types. Quarantine policies have the highest priority followed by isolation environment policies, and application security policies, in that order. The VDI Policy takes the last precedence, for example, if an application security is protecting a VM, it cannot simultaneously be protected with the VDI policy.

Isolation environment rules take precedence over application security rules, so make sure that isolation environment policies and application security policies are not in conflict. An isolation environment rule and an application security rule are said to be in conflict if they apply to the same traffic (a scenario that is encountered when VMs in one of the categories in the isolation environment send traffic to an application in the other category, and some or all of that traffic is either allowed or disallowed by the application security policy). The effect that an isolation environment policy has on a conflicting application security policy depends on the mode in which the isolation environment policy is deployed, and is as follows:

- If the isolation environment policy is in the applied mode, it blocks all traffic to the application, including the traffic that is allowed by the application security policy.
- If the isolation environment policy is in the monitoring mode, it allows all traffic to the application, including any traffic that is disallowed by the application security policy.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1786

REQUIREMENTS

The Security Policies feature has the following requirements:

- The feature is supported only on AHV clusters running AOS 5.6 or later and AHV version 20170830.115 or later.
- The Prism Central instance must be hosted on one of the AHV clusters registered with it. The AHV cluster that hosts the Prism Central instance must be running AOS 5.6 or later.
- The host must have at least 1 GB of additional memory for each Prism Central VM hosted on it.
- If you are running a Prism Central scale-out instance, all the VMs in the Prism Central cluster must be powered on.
- The AHV hosts must be allowed to communicate with the Prism Central VMs over TCP port 9446. Keeping the port open enables the hosts to send the Prism Central VMs connection tracking data. Prism Central uses that data to show network flows.
- Flow supports only TCP, UDP, or ICMP traffic.

Caution:

- When Flow is enabled, a Kafka container is automatically created on the cluster where Prism Central is hosted. The container is used to store data that is required for flow visualization to work and must not be deleted.
- Cross cluster live migration of guest VMs that are part of Flow security policy is not supported.
- Security Policies are not supported for VMs that are on the advanced networking stack. An alert is raised for VMs that are part of both VPC and Flow policy, and Flow policies are not enforced for VMs on VPCs.
- Overlapping or conflicting policy configuration is not supported and might cause unintended interruption of network services.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1787

ENABLING MICROSEGMENTATION

Microsegmentation is disabled by default. Before you can configure and use application security policies, isolation environment policies, and quarantine policies, you must enable the feature. The feature requires a Flow license. If you have not installed a Flow license, you can try the feature for a period of 60 days. After this period expires, you will be required to install the license to continue using the feature.

Before you begin

Ensure that you meet Microsegmentation requirements.

About this task

To enable microsegmentation, do the following:

Procedure

1. Log on to the Prism Central web console.
2. Click the collapse menu ("hamburger") button on the left of the main menu and then select **Prism Central Settings** to display the Settings page.
3. Click **Microsegmentation** from the Settings menu (on the left).
   The **Enable Microsegmentation** dialog box is displayed.
4. To determine whether the registered clusters are capable of supporting microsegmentation, do the following:
   a. Click **View Cluster Capability**, and then review the results of the capability checks that Prism Central performed on the registered clusters.
   b. Click **Back**.
5. Select the **Enable Microsegmentation** check box.
6. Click **OK**.

Disabling Microsegmentation

Prism Central web console provides you the ability to disable the microsegmentation feature.

About this task

To disable microsegmentation, do the following:

Procedure

1. Log on to the Prism Central web console.
2. Click the gear icon in the main menu and then select **Microsegmentation** in the **Settings** page.
3. Click **Disable Microsegmentation**.
   A confirmation message appears.
4. Click **Disable** to confirm disabling the microsegmentation feature.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1788

BUILT-IN CATEGORIES FOR SECURITY POLICIES

Prism Central includes built-in categories that you can use in application security policies and isolation policies. It also includes a built-in category for quarantining VMs.

Table 2: Built-In Categories

Category	Description
AppTier	Add values for the tiers in your application (such as web, application_logic, and database) to this category and use the values to divide the application into tiers when configuring a security policy.
AppType	Associate the VMs in your application with the appropriate built-in application type such as Exchange and Apache_Spark. You can also update the category to add values for applications not listed in this category.
Environment	Add values for environments that you want to isolate from each other and then associate VMs with the values.
Quarantine	Add a VM to this category when you want to quarantine the VM. You cannot modify this category. The category has the following values: Strict Use this value when you want to block all inbound and outbound traffic. Forensic Use this value when you want to block all inbound and outbound traffic except the traffic to and from categories that contain forensic tools.
ADGroup	This category is managed by ID Based Security (ID Firewall). Each ADGroup value represents an imported group from Active Directory. To add or remove values to use in Flow policies use the **ID Based Security** configuration page (**Prism Central Settings** > **Flow** > **ID Based Security**). The category values may be used in VDI policies, see VDI Policy Configuration on page 34 for details.
ADGroup:Default	This category is applied to the VDI VMs of the AD group when the VM inclusion criteria is set and allows you to apply a default set of rules for the VDI VMs (without the requirement of user logons).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1789

SERVICES

Service is a group of protocol-port combination. You can use any of the default services or create a custom service. The ability to use the service entities in the policy creation workflow reduces any manual configuration error and enables reusability of available entities.

- To create or update a custom service, see Creating a Service on page 12.
- To view the list of available services (built-in and custom services), go to **Network & Security** > **Security Policies** > **Services**.

Creating a Service

About this task

To create a custom service, do the following.

Procedure

1. Log on to the Prism Central web console.
2. Click the collapse menu ("hamburger") button on the left of the main menu and go to **Network & Security** > **Security Policies** > **Services**.
3. Click **Create Service Group**.
4. Enter a name and description for the service.
5. Select the **Protocol** from the drop-down menu and enter the port number or port range in the **Port** field.

   You can add multiple protocol-port combinations in a single service. To add more protocol-port combination, click **Add Row** and specify the required values.
6. Click **Save** to save the service.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1790

ADDRESSES

Address is a way to group one or many IP addresses or ranges. You can create an address entity and use that address entity while creating policies. The ability to use the addresses in the policy creation work flow reduces any manual configuration error and enables reusability of available entities.

- To create or update an Address, see Creating an Address on page 13.
- To view the list of available addresses, go to **Network & Security** > **Security Policies** > **Addresses**.

Creating an Address

About this task

To create an Address, do the following.

Procedure

1. Log on to the Prism Central web console.
2. Click the collapse menu ("hamburger") button on the left of the main menu and go to **Network & Security** > **Security Policies** > **Addresses**.
3. Click **Create Address**.
4. Enter a name and description for the address.
5. Enter the IP address or a IP range in the **Subnet** field.

   You can add multiple subnets in a single address entity. To add more subnets, click **Add Row** and specify the required values.
6. Click **Save** to save the address.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1791

ALLOWING DISCOVERED TRAFFIC

About this task

A generic policy in the enforced mode discovers traffic intended to reach the secured entities. When the policy is in the enforced mode, by default the system does not allow the discovered traffic to reach the secured entities. To process the discovered traffic, you update the policy to manually allow the discovered traffic. Later, the traffic is subjected to the configured rules that is defined in the policy. To allow the discovered traffic, follow these steps:

Procedure

1. Log on to Prism Central.
2. Select **Infrastructure** application from the Application Switcher Function, and navigate to **Network & Security** > **Security Policies**

   The **Security Policies** page appears.
3. In the **Security Policies** page, select the policy.

   The policy page shows the discovered traffic in the **Inbounds** and **Outbounds**.
4. Click **Update**.

   The **Update Security Policy** page appears.
5. Click **Next**.

   - In the **Inbounds > Discovered** or **Outbounds > Discovered** section, hover over the traffic source and click **Allow Traffic**.

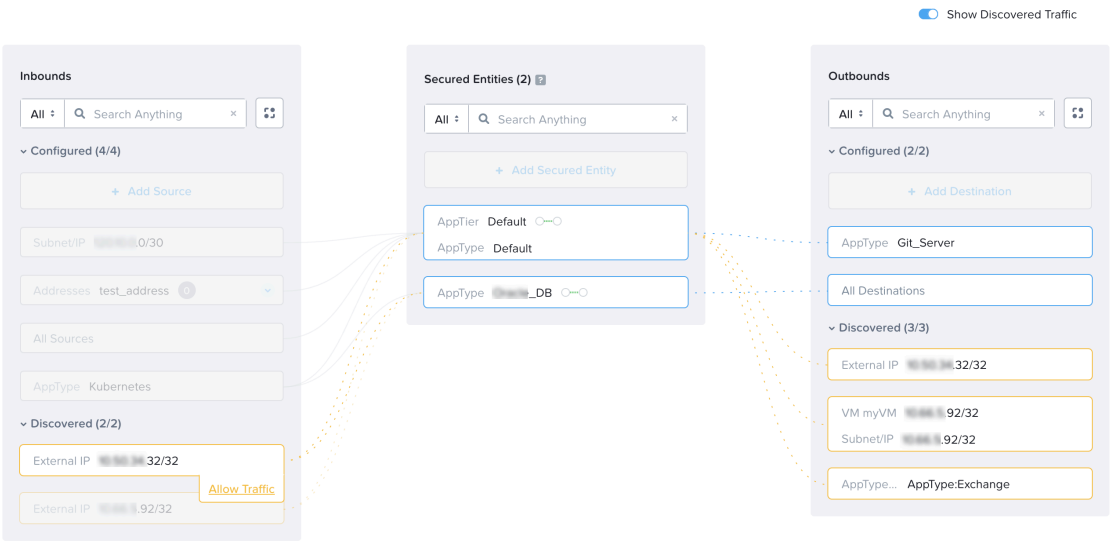


Figure 1: Discovered Traffic - Visual View

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1792

6. In the **Allow Traffic** page, select the source of the discovered traffic and choose a service.

   Show All Traffic: Shows a consolidated list of sources trying to reach all AppTiers (secured VMs).

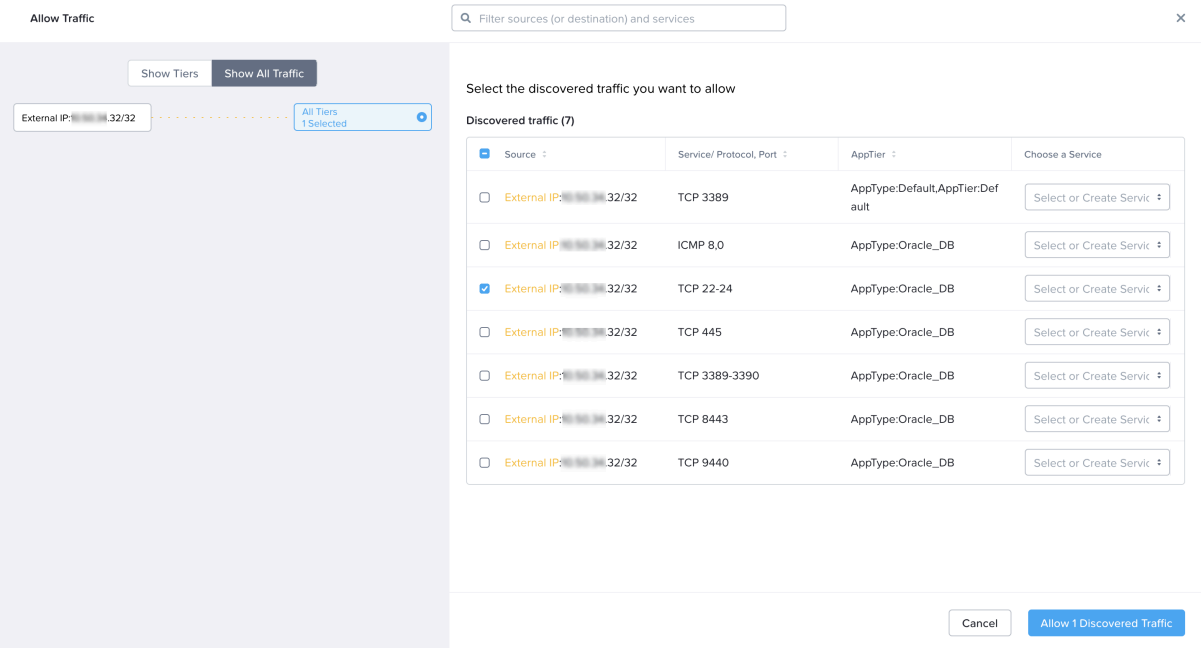


Figure 2: Allow Traffic - Show All Traffic

Show Tiers: Shows a source trying to reach different AppTypes within an AppTier.

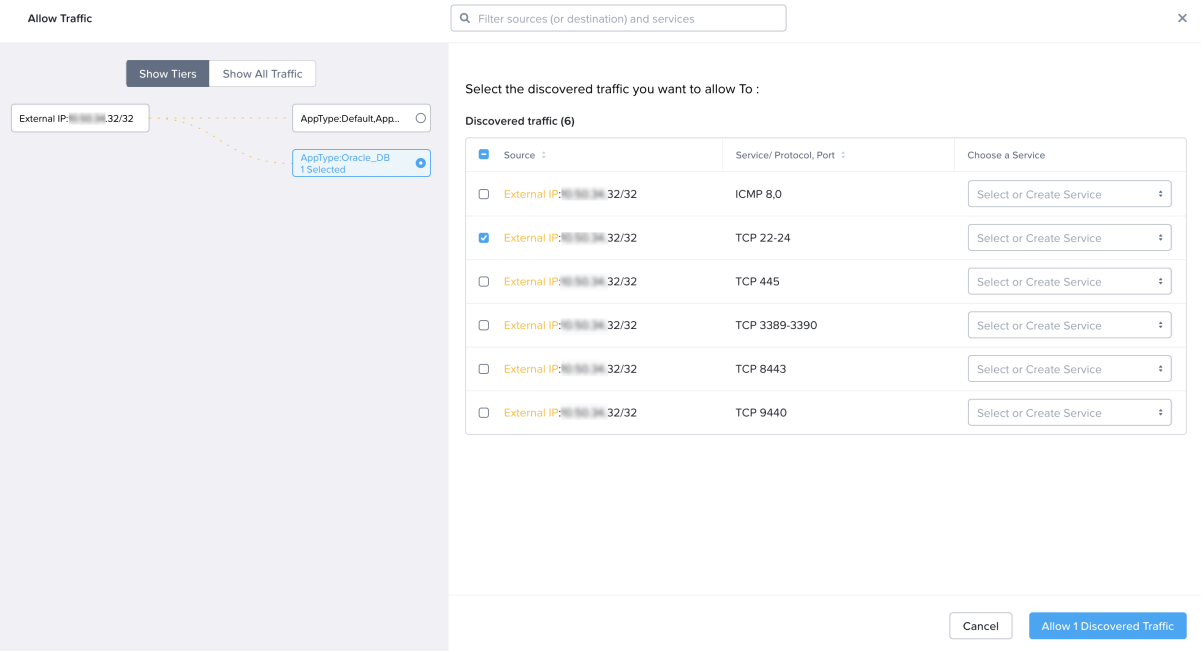


Figure 3: Allow Traffic - Show Tiers

You can select more than one traffic source. If a required service is not present in the drop-down, you can create a new service. See Creating a Service on page 12 for more information.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1793

7. Click **Allow Discovered Traffic** and click **Next**.
8. In the **Review** page, select a policy mode and click **Confirm** to complete updating the security policy.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1794

APPLICATION SECURITY POLICY CONFIGURATION

Creating an Application Security Policy

Before you begin

- Create the categories you need and associate the VMs that you want to protect with those categories. You might be required to create categories for the following purposes. Some categories or category values are required while others are optional:
  - Every security policy must be associated with a value in the AppType category, so make sure that you update the AppType category with appropriate values if the built-in values do not work for you. For information about this category and its values, see Category Details View in the *Prism Central Infrastructure Guide*.
  - If you need to apply the policy to an application in a specific environment (for example, development, test, or production) or an application at a specific location, create the category you need and apply it to the application. Prism Central includes a built-in Environment category that you can use or update with values of your own. You can also create your own categories.
  - If you want to specify categories for traffic sources and destinations instead of allowing all inbound and outbound traffic, create those categories and apply them to the traffic sources and destinations.
  - If you want to divide the application into tiers in a security policy, add tiers to the AppTier category. The AppTier category has a built-in `default` value, but you can update the category to add values of your choice.

  For information about categories and their values, see Category Management in the *Prism Central Infrastructure Guide*.
- Security policy configuration might require more time than the default session timeout allows you. You might want to increase the session timeout so that you do not lose a configuration that is left unattended while you perform associated tasks such as referring to this documentation. For more information, see Configuring Prism Central UI Settings in the *Prism Central Admin Center Guide*.

About this task

To secure an application, do the following:

1.

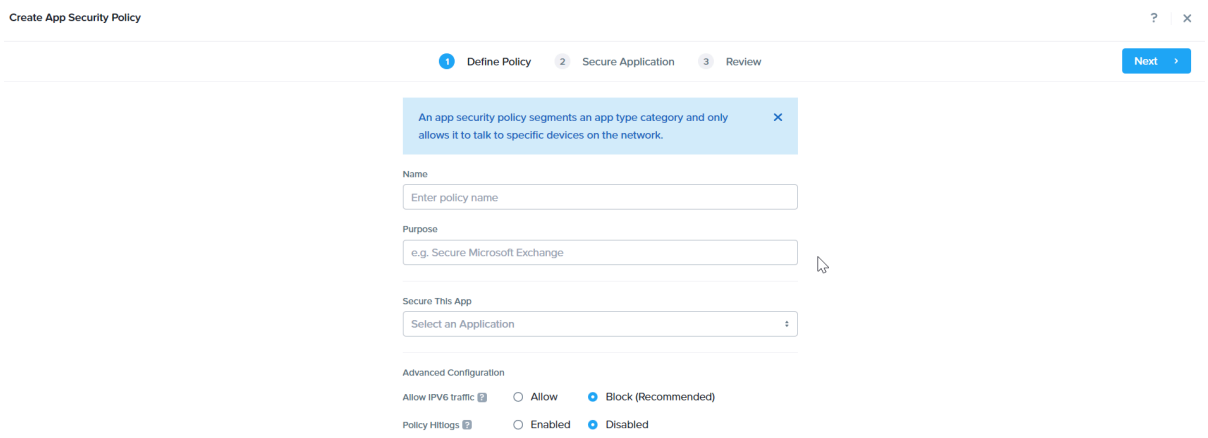
Procedure

1. Log on to Prism Central.
2. Select **Infrastructure** application from the Application Switcher Function, and navigate to **Network & Security** > **Security Policies**The **Security Policies** page appears.
3. In the **Security Policies** page, click **Create Security Policy**, and then click **Secure an Application**. The **Create App Security Policy** page is displayed.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1795

4. On the **Define Policy** tab, do the following in the indicated fields, and then click **Next**:

Figure 4: Define Policy Tab



a. **Name**: Enter a name for the security policy.

b. **Purpose**: Describe the purpose of the security policy.

c. **Secure This App**: Select the type of application that you want to secure.

The **Secure This App** list displays available values in the AppType category. It uses the format `AppType: value`, where value represents a type of application. Every application that you want Prism Central to secure must be associated with a value from the built-in AppType category. The AppType category includes values for frequently encountered applications, such as Exchange and Hadoop. The AppType category also includes a built-in `default` value that you can use if your application cannot be associated with one of the other built-in values. You can also update the `AppType` category to add a value of your choice. For information about categories and their values, see Category Management in the *Prism Central Infrastructure Guide*.

d. If you want to filter the VMs by an additional category, select **Filter the app type by category**, and then enter the name of the category in the text box that is displayed.

This option enables you to apply the policy to an additional category. For example, if you are configuring a policy for an application in the category `AppType: Exchange`, this option enables you to further restrict the policy to specific locations (such as `Location: US` and `Location: EU`) or environments (such as `Environment: Production`, `Environment: Development`, and `Environment: Test`).

e. Optionally, in the **Advanced Configuration** section, select the **Allow** radio button to allow **IPv6 traffic**. The policy rules apply to IPv4 traffic only and all IPv6 traffic is blocked by default.

> **Note:** If you choose to block IPv6 traffic, the IPv6 traffic remains blocked even in the monitoring mode.

f. Optionally, click the toggle button against **Policy Hit Logs** to log traffic flow hits on the policy rules.

You can configure syslog monitoring for the policy hit logs for Flow. For details, see Configuring Syslog Monitoring in the *Prism Central Admin Center Guide*.

> **Note:** Policy hit logs are not generated if both source and destination are in inbound or outbound category.

5. In the **Securing an App** dialog box, review the schematic that illustrates the flow of traffic through a secured app, and then click **OK, Got it!**
The **Secure Application** tab is displayed. The schematic on this tab can be divided into three areas of configuration: the **Inbound** side, (for adding traffic source allowlist), the application at the center (for

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1796

configuring inbound, outbound, and tier-to-tier rules), and the **Outbound** side (for adding traffic destination allowlist).

6. On the **Secure Application** tab, do the following, and then click **Next**:

   a. On the application at the center of the tab, do the following in the indicated fields:

   - If you want to divide the application into tiers (such as a web tier, an application tier, and a database tier) and configure tier-to-tier rules, first configure the application as described in this step, and then configure inbound and outbound rules. This approach ensures that the individual tiers are available when you want to configure inbound and outbound rules at the tier level. Skip this step if you want to treat the application as a single entity in the security policy.

     To divide your application into tiers and create tier-to-tier rules, do the following:

     1. On the application, click **Set Rules on App Tiers, Instead**.

        > **Note:** After you click **Set Rules on App Tiers, Instead**, the link text, **Set rules on the whole app, instead**, is displayed in its place. Click **Set rules on the whole app, instead** if you want to discard the tiered configuration and return to configuring rules on the application as a whole.

     2. Click **Add Tier**, and then select a tier.

        Repeat this step to add as many tiers as you require. The following figure shows an application with a web tier, an application tier, and a database tier:

     3. To delete a tier, pause over the tier you want to delete and click the delete button that is displayed.
     4. Click **Set Rules Within App**.

        > **Note:** When configuring tier-to-tier rules, two modes are made available to you through the buttons **Set Rules to & from App** and **Set Rules Within App**. The **Set Rules to & from App** option enables you to add application tiers and to specify allowed inbound and outbound traffic. The **Set**

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1797

Rules Within App option enables you to specify tier-to-tier rules within the application. These buttons enable you to switch between the two modes.

5. Click each tier in the application and click **Yes** or **No** to specify whether or not you want to allow the VMs in the tier to communicate with each other.
6. Configure a tier-to-tier rule as follows:
    1. Click the source tier (for example, if the tiers are WebTier and AppTier and you want to configure a tier-to-tier rule from WebTier to AppTier, click the source tier, WebTier).
    2. Click the plus sign that is displayed on the destination tier (in this example, click the destination tier, AppTier). The **Create Tier to Tier Rule** dialog box
    3. Enter a description for the rule.

        Note: The policy rule description is captured in the policy hitlog data.

        - Policy hitlog must be enabled
        - Rule description is added to the hitlog only for allowed traffic

    4. In **Service Details**, click **Allow all traffic** to allow all types of traffic or click **Select a service** to choose any default or custom service.
    5. Click **Save**.

    Configure tier-to-tier rules for as many source and destination tiers as you want.

b. To add traffic sources, on the **Inbound** side of the **Secure Application** tab, do the following:

- From the drop-down list, select one of the following options:
    - **Allow All**: Allows traffic from all sources.
    - **Allowed List Only**: Allows traffic only if the traffic originates from entities on the security policy's source allowlist. This option is the default option. If this option is selected, you must also configure the source allowlist by clicking **Add Source**.
- Click **Add Source**, and then do the following:
    1. Select one of the following options from the drop-down list:
        - **Category**: Allows traffic only if that traffic originates from entities that are in the selected category.
        - **Subnet/IP**: Allows traffic only if that traffic originates from entities that are in the selected subnet.
        - **Addresses**: Allows traffic only if the traffic originates from the entities that are in the selected address.
    2. Enter the value in the text box, and then click **Add**.

        When entering the name of a category, a list of matching names is displayed, and you can select the name you want to specify. The subnet mask must be specified in the CIDR format.

        When entering the address, a list of available address group names appears. Select the address group or you can create a new address group.
    3. To add another category, subnet or address, click **Add Source**. Add as many another category, subnet or address as you want to allow.

    Each entry in this list represents a stream of inbound traffic.

c. To add traffic destinations, on the **Outbound** side, do the following:

- From the drop-down list, select one of the following options:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1798

- **Allow All**: Allows traffic to all destinations. This option is the default option.
- **Allowed List Only**: Allows traffic only if the traffic is destined for entities on the security policy's destination allowlist. If this option is selected, you must also configure the destination allowlist by clicking **Add Destination**.

- Click **Add Destination**, and then do the following:
  1. Select one of the following options from the drop-down list:
     - **Category**: Allows traffic only if that traffic is destined for entities in the selected category.
     - **Subnet/IP**: Allows traffic only if that traffic is destined for entities in the selected subnet.
     - **Addresses**: Allows traffic only if the traffic originates from the entities that are in the selected address.
  2. Enter the value in the text box and then click **Add**.

     When entering the name of a category, a list of matching names is displayed, and you can select the name you want to specify. The subnet mask must be specified in the CIDR format.

     When entering the address, a list of available address group names appears. Select the address group or you can create a new address group.
  3. To add another category, subnet or address, click **Add Destination**. Add as many categories, subnets or address as you want to allow.

  Each entry in this list represents a stream of outbound traffic.

- To specify the protocols that you want to allow from each stream of inbound and outbound traffic, do the following:
  1. If you added application tiers and configured tier-to-tier rules, first click **Set Rules to & from App**.
  2. Click the traffic source or traffic destination (a category or subnet if you have configured a allowlist or **All Sources** if you have chosen to allow all sources) for which you want to create a rule.
  3. Click the plus icon that appears on the application (if you are treating the application as a single entity) or application tier (if you have divided the application into tiers). The **Create Inbound Rule** or **Create Outbound Rule** dialog box appears.
  4. Enter a description for the rule.
  5. In **Service Details**, click **Allow all traffic** to allow all types of traffic or click **Select a service** to choose any default or custom service.
  6. Click **Save**.

After you configure a rule, a dotted line appears between the two endpoints of the rule. Point to the dotted line to show the list of ports that the rule allows.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1799

7. On the **Review** tab, review the security policy configuration, and then do one of the following:

   - If you want to apply the configuration, select **Enforce** and click **Apply**.

     Applying a security policy enforces the security policy on the application, and traffic from entities that are not defined as sources in the policy is blocked.

   - If you want to save the configuration and monitor how the security policy works, select **Monitor** and click **Save and Monitor**.

     When a policy is in the monitoring state, the application continues to receive all traffic, but disallowed traffic is highlighted on the monitoring page. Traffic is not blocked until the policy is enforced.

     Note: A policy that you have chosen to save and monitor can be applied from the policy update page.

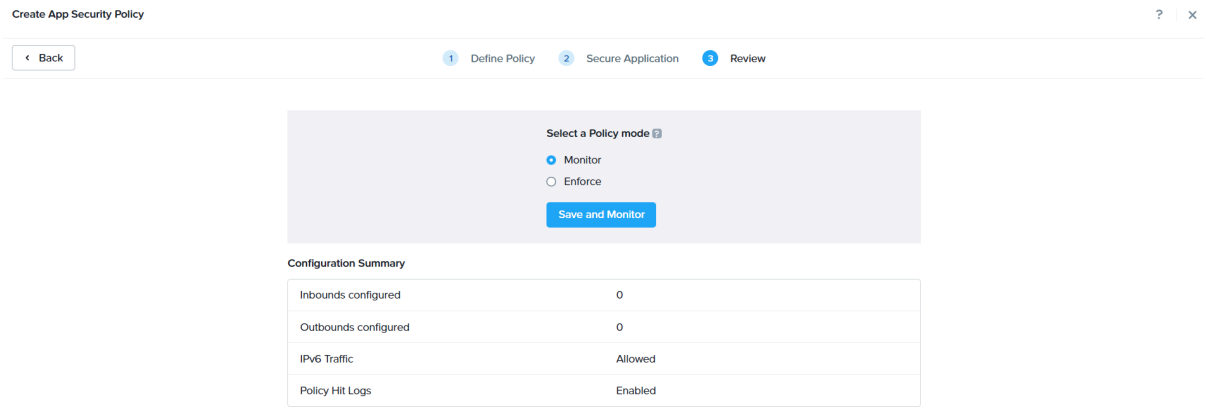


Figure 5: Review

Modifying an Application Security Policy

About this task

To modify a security policy, do the following:

Procedure

1. In the **Security Policies** page, select the policy that you want to modify, click **Actions**, and then click **Update**.
2. Make the changes you want and then apply or save and monitor the policy.

   The update options are the same as those for creating a policy. For information about the options, see Creating an Application Security Policy on page 17.

Applying an Application Security Policy

Applying a security policy enforces the security policy on the application, and any traffic from sources that are not allowed is blocked.

About this task

To apply a security policy, do the following:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1800

Procedure

1. In the **Security Policies** page, select the policy that you want to apply, click **Actions**, and then click **Apply**.
2. Confirm by typing **Apply** in the dialog box, and then click **OK**.

Monitoring an Application Security Policy (Visualizing Network Flows)

About this task

When a policy is in the monitoring state, the application continues to receive all traffic, but disallowed traffic is highlighted on the monitoring page. Traffic is not blocked until the policy is applied.

To monitor a security policy, do the following:

Procedure

1. In the **Security Policies** page, select the policy that you want to monitor, click **Actions**, and then click **Monitor**.
2. Confirm by typing **Monitor** in the dialog box, and then click **OK**.
   Allowed network flows and disallowed network flows are shown on the monitoring page, as shown in the following figure. Allowed flows are depicted with a blue dotted line and disallowed network flows are depicted with a red dotted line:

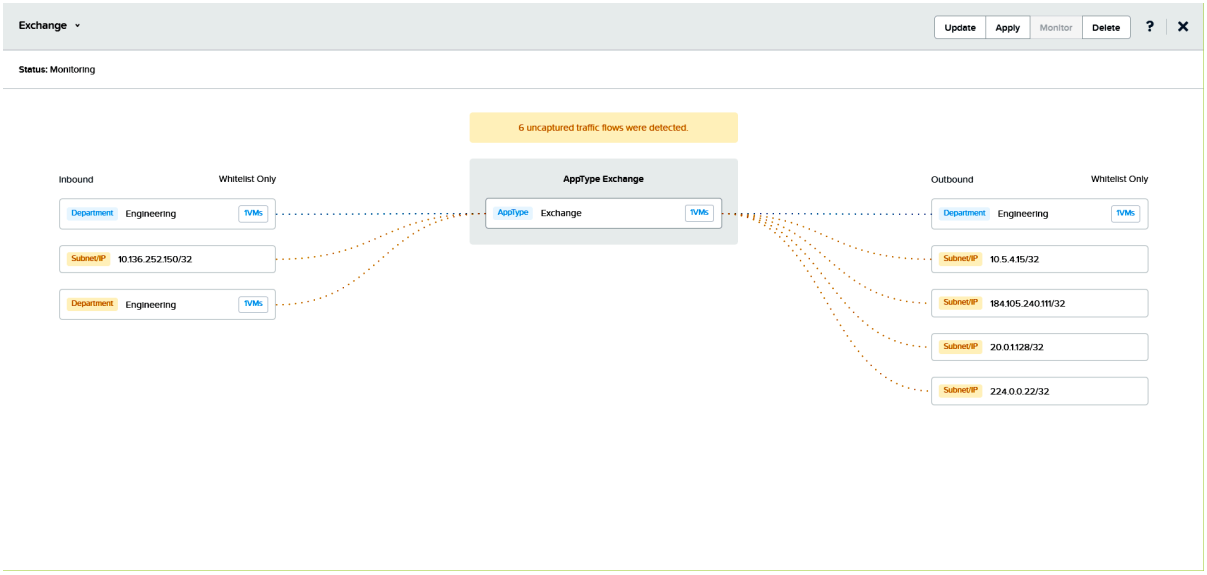


Figure 6: Monitoring Page for an Application Security Policy

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1801

3. To show a preview of the network flow in a tooltip, pause over the dotted line that depicts the network flow in the diagram.
   A tooltip similar to the following is displayed. The tooltip shows a graph for each connection:

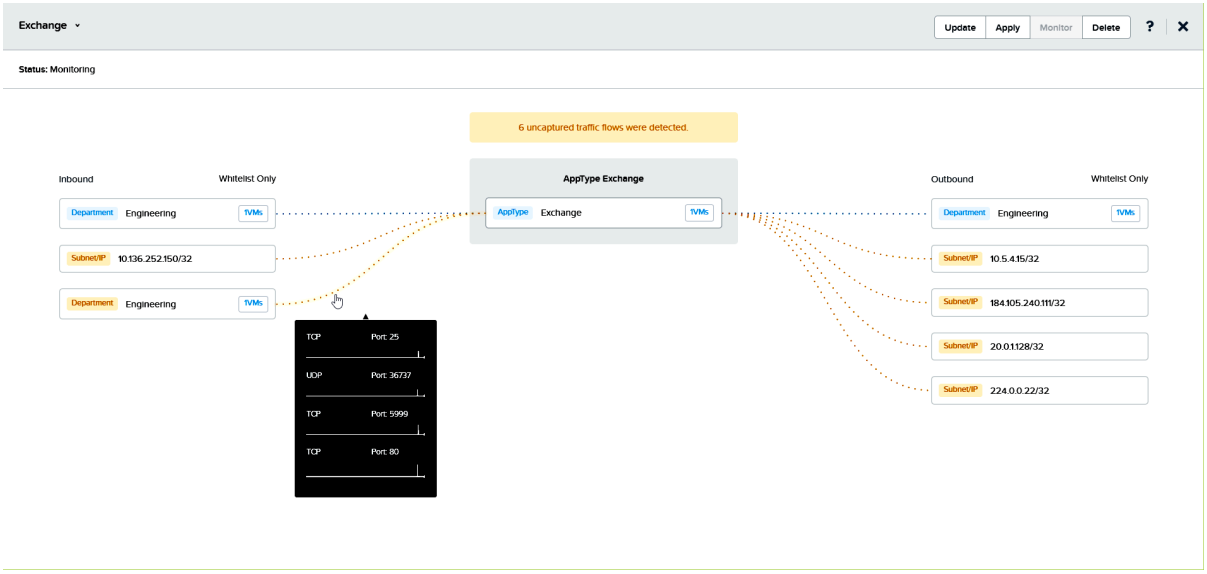


Figure 7: Tooltip Showing a Preview of the Network Flow

4. To see a graph of a network flow, click the dotted line that depicts the network flow in the visualization.
   A more detailed graph of the network flows is displayed, as shown in the following figure:

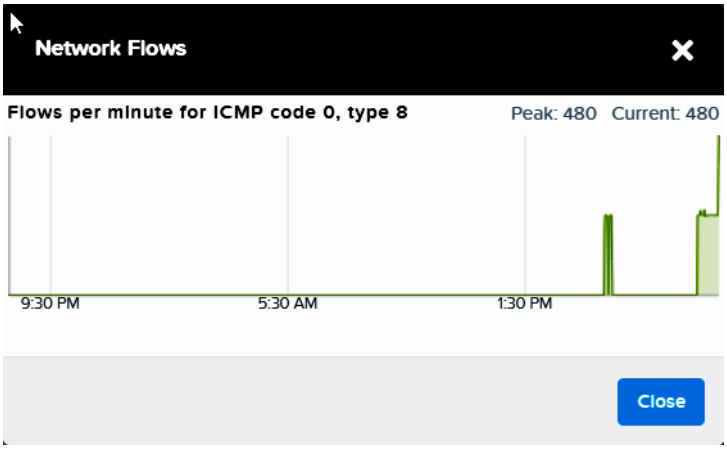


Figure 8: Network Flows Graph

5. To block unwanted flows, click **Update**, and then update the policy. For information about updating an application security policy, see Modifying an Application Security Policy on page 22.

6. To apply the policy, click **Apply**.
   Applying a policy enforces the policy and traffic from sources that are not allowed is blocked.

Deleting an Application Security Policy

About this task

To delete an application security policy, do the following:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1802

Procedure

1. In the **Security Policies** page, select the policy that you want to delete.
   You can select multiple policies and delete them all at once.
2. Click **Delete** in the **Actions** menu.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1803

ISOLATION ENVIRONMENT POLICY CONFIGURATION

An isolation environment identifies two groups of VMs by category, and it blocks communications between the groups.

You can also specify an additional category to restrict the scope of the isolation environment to that category.

For example, consider that you have an `application` category with values `app1` and `app2` and that you have associated some VMs with `application: app1` and some VMs with `application: app2`. Also, consider that these same VMs are distributed between two sites, and have accordingly been associated with values site1 and site2 in a category named location (`location: site1` and `location: site2`).

In this example, you might want to block communications between the VMs in the two locations. Additionally, you might want to restrict the scope of the policy to VMs in category `application: app1`. In other words, `app1` VMs in `site1` cannot communicate with `app1` VMs in `site2`. The following diagram illustrates the desired outcome. The red connectors illustrate blocked traffic. The green connectors illustrate allowed traffic.

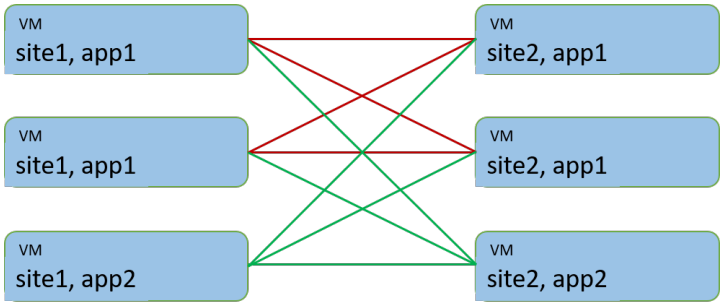


Figure 9: Applications Across Sites

You can configure an isolation policy for this by creating the following categories and isolation policy in Prism Central:

Table 3: Sample Configurations For Categories and the Isolation Policy

Entity	Values
Categories	• **Name**: `application` • **Values**: `app1` and `app2` • **Name**: `location` • **Values**: `site1` and `site2`

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1804

Entity	Values
Isolation Policy	• **Name**: `eng_isolation_policy_across_sites` • **Description**: Isolate engineering VMs across sites • **Isolate This Category**: `location: site1` • **From This Category**: `location: site2` • **Apply the isolation only within a subset of the data center**: `application: app1`

Layer 2 Isolation

Flow supports Layer 2 isolation to enable filtering of the layer 2 packets across all isolated entities. When an isolation policy is applied between two category-based VM groups, all ingress and egress traffic (broadcast, unknown-unicast, and multicast traffic) is dropped at the destination VM group.

Note:

- If VMs are part of both isolation policy and quarantine policy, the quarantine policy takes priority of processing over the isolation policy. For example, if VMs with category app1 are isolated from VMs with category app2 using an isolation policy, the traffic between these VM groups are not dropped if the VM groups are also part of a quarantine forensic policy that allows communication between these VMs. In this case, since the quarantine forensics policy matches the VMs, and this policy allows the traffic, the isolation policy is not enforced.
- IPv6 traffic between isolated VMs is blocked by default with the introduction of layer 2 isolation.

Creating an Isolation Environment Policy

An isolation environment policy identifies two groups of VMs and blocks communications between the groups. The two groups are identified by category. You can specify an additional category to restrict the scope of the policy to that category.

About this task

To create an isolation environment, do the following:

Procedure

1. Log on to Prism Central.
2. Select **Infrastructure** application from the Application Switcher Function, and navigate to **Network & Security** > **Security Policies**The **Security Policies** page appears.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1805

3. In the **Security Policies** page, click **Create Security Policy**, and then click **Isolate Environments**. The **Create Isolation Policy** page appears.

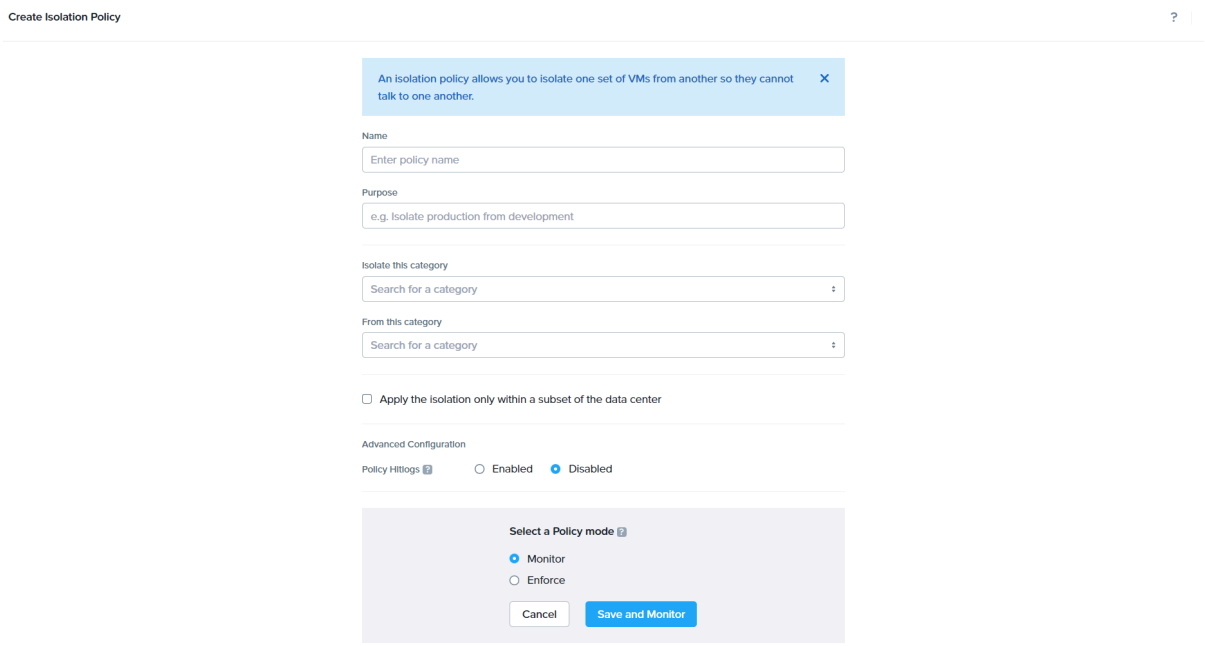


Figure 10: Create Isolation Policy

4. Do the following in the indicated fields:

   - **Name**: Enter a name for the isolation policy.
   - **Purpose**: Describe the purpose of the isolation policy.
   - **Isolate this category**: Type the name of one of the two categories that you want to isolate from each other.

     Matching names appear in a list as you type. You can click the name of the category you want.
   - **From this category**: Type the name of other category.
   - **Apply the isolation only within a subset of the data center**. If you want to restrict the scope of the policy to a specific category of VMs, select this check box, type the name of the category in the text box, and select the category from the list of matches.

     If you isolate VMs in category `Environment: Production` from VMs in category `Environment: Staging`, and you restrict the scope of the policy to VMs in the category `Environment: Dev`, Prism Central applies the isolation policy to the following groups:

     - VMs that are in both `Environment: Production` and `Environment: Dev`
     - VMs that are in both `Environment: Staging` and `Environment: Dev`.
   - **IPv6 Traffic**. Optionally, in the **Advanced Configuration** section, select the **Allow** radio button to allow **IPv6 traffic**. The policy rules apply to IPv4 traffic only and all IPv6 traffic is blocked by default.
   - **Policy Hit Logs**. Optionally, click the toggle button against **Policy Hit Logs** to log traffic flow hits on the policy rules. You can configure syslog monitoring for the policy hit logs for Flow. For details, see Configuring Syslog Monitoring in the *Prism Central Admin Center Guide* for details.

     Note: Policy hit logs are not generated if both source and destination are in inbound or outbound category.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1806

5. Do one of the following:

   » Click **Apply Now** to apply the isolation environment.

   » Click **Save and Monitor** to save the configuration and place the isolation environment in the monitoring mode.

   You can switch between the monitoring and applied states by selecting the isolation environment on the **Security Policies** page and clicking the appropriate option in the **Actions** menu.

Modifying an Isolation Environment Policy

About this task

To modify an isolation environment, do the following:

Procedure

1. In the **Security Policies** page, select the isolation policy that you want to modify, click **Actions**, and then click **Update**.
2. Make the changes you want and then apply or save and monitor the policy.

   The update options are the same as those for creating a policy. For information about the options, see Creating an Isolation Environment Policy on page 27.

Applying an Isolation Environment Policy

Applying an isolation environment policy enforces the policy on the specified categories, and any traffic between the categories is blocked.

About this task

> **Note:** Changing the state of an isolation environment policy affects the functioning of any conflicting application security policies. For more information, see Priorities Between Policies on page 8.

To apply an isolation environment policy, do the following:

Procedure

1. In the **Security Policies** page, select the policy, click **Actions**, and then click **Apply**.
2. Confirm by typing **Apply** in the dialog box, and then click **OK**.

Monitoring an Isolation Environment Policy (Visualizing Network Flows)

About this task

The VMs in the two categories in an isolation environment policy are allowed to communicate with each other when the policy is in the monitoring state. Traffic is blocked only during the time the policy is applied.

> **Note:** Changing the state of an isolation environment policy affects the functioning of any conflicting application security policies. For more information, see Priorities Between Policies on page 8.

To monitor a security policy, do the following:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1807

Procedure

1. In the **Security Policies** page, select the policy, click **Actions**, and then click **Monitor**.
2. Confirm by typing **Monitor** in the dialog box, and then click **OK**.
   The monitoring page shows the flows between the two categories.
3. To view information about a particular network flow, pause over the flow.
   A tooltip similar to the following is displayed:

Figure 11: Monitoring Page for an Isolation Environment Policy

Deleting an Isolation Environment Policy

About this task

To delete an isolation environment policy, do the following:

Procedure

1. In the **Security Policies** page, select the policy.
   You can select multiple policies to delete them all at once.
2. Click **Delete** in the **Actions** menu.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1808

QUARANTINE POLICY CONFIGURATION

Prism Central includes a system-defined quarantine policy that enables you to perform the following tasks:

- Completely isolate an infected VM that must not have any traffic associated with it.
- Isolate an infected VM but specify a set of forensic tools that can communicate with the VM.

For these use cases, Prism Central includes built-in categories that are included in the system-defined quarantine policy.

> **Note:** You cannot create a quarantine policy. However, you can modify existing (system-defined) quarantine policy.

Prism Central also enables you to monitor the quarantine policy before applying it.

The quarantine policy cannot be deleted.

Configuring the Quarantine Policy

In the built-in quarantine policy, you specify categories that can communicate with VMs that have been added to the **Quarantine: Forensics** category.

About this task

To configure the quarantine policy, do the following;

Procedure

1. Log on to Prism Central.
2. Select **Infrastructure** application from the Application Switcher Function, and navigate to **Network & Security** > **Security Policies**The **Security Policies** page appears.
3. In the **Security Policies** page, select **Quarantine**, and then click **Update** in the **Actions** menu.
4. Optionally, in the **Advanced Configuration** under the **Define Policy** tab, do the following.
   a. Select the **Allow** radio button to allow **IPv6 traffic**. The policy rules apply to IPv4 traffic only and all IPv6 traffic is blocked by default. You can configure the allow option for both **Forensic** and **Strict** modes.
   b. Optionally, click the toggle button against **Policy Hit Logs** to log traffic flow hits on the policy rules.
      You can configure syslog monitoring for the policy hit logs for Flow. For details, see Configuring Syslog Monitoring in the *Prism Central Admin Center Guide* . You can enable the policy hit log option for both **Forensic** and **Strict** modes.

      > **Note:** Policy hit logs are not generated if both source and destination are in inbound or outbound category.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1809

5. On the **Add Forensic Tools** tab, do the following, and then click **Next**:

   a. To specify the categories that contain forensic tools, on the **Inbound** and **Outbound** sides of the policy diagram, do the following:

      - From the drop-down list, select one of the following options:

        - **Allow All**: Allows traffic associated with all sources or destinations.
        - **Allowed List Only**: Allows traffic only if the traffic is associated with the categories and subnets on the allowlist. This option is the default option. If this option is selected, you must also configure the allowlist by clicking **Add Source** or **Add Destination**.

      - Click **Add Source** or **Add Destination**, and then do the following:

        1. Select one of the following options from the drop-down list:

           - **Category**: Allows traffic to or from the specified category.
           - **Subnet/IP**: Allows traffic to or from the specified subnet.
           - **Addresses**: Allows traffic only if the traffic originates from the entities that are in the selected address.

        2. Enter the value in the text box, and then click **Add**.

           When entering the name of a category, a list of matching names is displayed, and you can select the name you want to specify. The subnet mask must be specified in the CIDR format.

           When entering the address, a list of available address group names appears. Select the address group or you can create a new address group.

        3. To add another category, subnet or address, click **Add Source** or **Add Destination**. Add as many category, subnet or address as you want to allow.

   b. To specify the protocols and ports over which the forensic tools can communicate with the VMs in the forensic category, do the following:

      - 1. On the **Inbound** and **Outbound** sides of the policy diagram, click a category or subnet (if you have configured a allowed list) or **All Sources** (if you have chosen to allow all sources) for which you want to create a rule.
        2. Click the plus icon that appears on the **Quarantine: Forensic** category. The **Create Inbound Rule** or **Create Outbound Rule** dialog box
        3. Enter a description for the rule.

           Note: The policy rule description is captured in the policy hitlog data.

           - Policy hitlog must be enabled
           - Rule description is added to the hitlog only for allowed traffic

        4. In **Service Details**, click **Allow all traffic** to allow all types of traffic or click **Select a service** to choose any default or custom service.
        5. Click **Save**.

   After you configure a rule, a dotted line appears between the two endpoints of the rule. Point to the dotted line to show the list of ports that the rule allows.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1810

6. On the **Review** tab, do one of the following:

   » Click **Apply Now** to apply the quarantine policy.

   » Click **Save and Monitor** to save the configuration and place the quarantine policy in the monitoring mode.

   You can switch between the monitoring and applied states by selecting **Quarantine** on the **Security Policies** page and clicking the appropriate option in the **Actions** menu.

Quarantining a VM

You quarantine a VM by adding the VM to a quarantine category.

About this task

To add an infected VM to a quarantine category, do the following:

Procedure

1. In the VMs dashboard **List** tab (see VMs Summary View in the *Prism Central Infrastructure Guide*), select the infected VM, click **Actions**, and then click **Quarantine VMs**.
2. Under Quarantine Method, click one of the following options:

   » **Strict.** Isolates the VM from all traffic. No exceptions can be made for forensics.

   » **Forensic.** Isolates the VM from all traffic except traffic from categories specified in the built-in quarantine policy. The allowed categories contain forensic tools that enable you to perform forensics on the VM.

   For VMs added to the strict quarantine, a red icon is displayed in the name column.
3. Click **Quarantine**.

Removing a VM from the Quarantine

About this task

To remove a VM from the quarantine, do the following:

Procedure

1. In the VMs dashboard **List** tab (see VMs Summary View in the *Prism Central Infrastructure Guide*), select the VM that you want to remove from the quarantine, click **Actions**, and then click **Unquarantine VMs**.

   You can select multiple VMs and remove them from the quarantine in a single step.
2. In the **Unquarantine VMs** dialog box, click **Unquarantine**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1811

VDI POLICY CONFIGURATION

The **VDI Policy** is based on identity-based categorization of the VDI VMs using Active Directory group membership. Configuring VDI policy includes adding an Active Directory domain that is used for the ID firewall (**ID Based Security**) and configuring a service account for the domain.

ID Based Security

ID firewall is an extension to Flow that allows you to write security policies based on users and groups in an Active Directory domain in which your VDI VMs are attached. When using ID firewall, you can import groups from Active Directory into Prism Central as categories (in the category key ADGroup), and then write policies around these categories, just as you would for any other category. A new type of policy has been added for this purpose - the **VDI Policy**. ID firewall takes care of automatically placing VDI VMs in the appropriate categories on detecting user logons into the VM hosted on Nutanix infrastructure associated with Prism Central, thus allowing user and group based enforcement of Flow policies.

- See Configuring Active Directory Domain Services on page 38 to import user groups for identity-based security policies.
- See Creating a VDI Policy on page 34 to create a VDI policy.
- See Default VDI Policy on page 38 configuration to define a default VDI policy.

Note:

- It is recommended to disable credential caching on VDI VMs for Flow ID Firewall. The Flow ID Firewall checks the domain controller events for logon attempts. If the VM connection to the domain controller is not available, a user is able to logon (if credential caching enabled) but no event is generated on the domain controller inhibiting the ID Firewall to detect the logon.
- To disable credential caching, see *Interactive logon: Number of previous logons to cache (in case domain controller is not available)* on *Microsoft* documentation website.
- A basic assumption of VDI Policies is that a single end-user is logged on to each desktop VM at a point in time. As a result, if multiple users log into a single desktop VM at once, the security posture of the VM may change in unpredictable ways. Please ensure that for predictable behavior, only one user is logged into the desktop VMs at a time.

Creating a VDI Policy

ID firewall integrates Nutanix Flow with Microsoft Active Directory (AD), such that the groups in the AD can be imported into Prism Central as categories. These imported categories can then be used in the VDI policy as target groups, inbound traffic, and outbound traffic. Prism Central automatically places VMs inside the imported AD group categories when user logons are detected on VMs that are part of the Active Directory domain and also present on Nutanix managed clusters, thus applying security policies based on user group membership.

Before you begin

Note:

- Flow Network Security does not support LDAPS encrypted connections on port 636. Therefore, to use VDI policies, configure an unencrypted port 389 for LDAP connection.
- Flow ID firewall is supported only for AHV host compatible with AOS version 5.17 and above and Prism Central version 5.17 and above.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1812

- Flow ID firewall does not detect user logoffs. The policy applied to a VM is kept applied until next user logon on the same VM.
- VMs with an **AppType** category assignment do not get categorized by **ID Based Security**.
- You can use the Default VDI Policy on page 38 to apply a default set of rules for the VDI VMs (without the requirement of user logons).
- Since a VM user can be a member of multiple ADGroups that are mapped into Prism Central from Active Directory, when a user logs on, a VM may be placed in multiple ADGroups at once. This is the correct behavior, and the policy applied to the VM will be a union of the respective combination of inbounds and outbounds across all ADGroups the VM is placed into.

- If not already available, configure an Active Directory domain that is used for ID firewall, see Configuring Active Directory Domain Services on page 38.
- Configure a service account with required configuration for the Active Directory domain, see Configure Service Account for ID Firewall on page 39.

About this task

To secure a VDI environment, do the following:

Procedure

1. Log on to Prism Central.
2. Select **Infrastructure** application from the Application Switcher Function, and navigate to **Network & Security** > **Security Policies**The **Security Policies** page appears.
3. In the **Security Policies** page, click **Create Security Policy**. Select **Secure VDI Groups (VDI Policy)** and click **Create**.

   You can create only one VDI policy for securing applications through ID Firewall.

   The **Define Policy** page is displayed.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1813

4. On the **Define Policy** tab, do the following in the indicated fields, and then click **Next**:

   a. The **Policy Name** and **Purpose** fields are auto-populated.

   b. Select either **Include all VMs** or **Include VMs by name** as the **VDI VM Filter**.

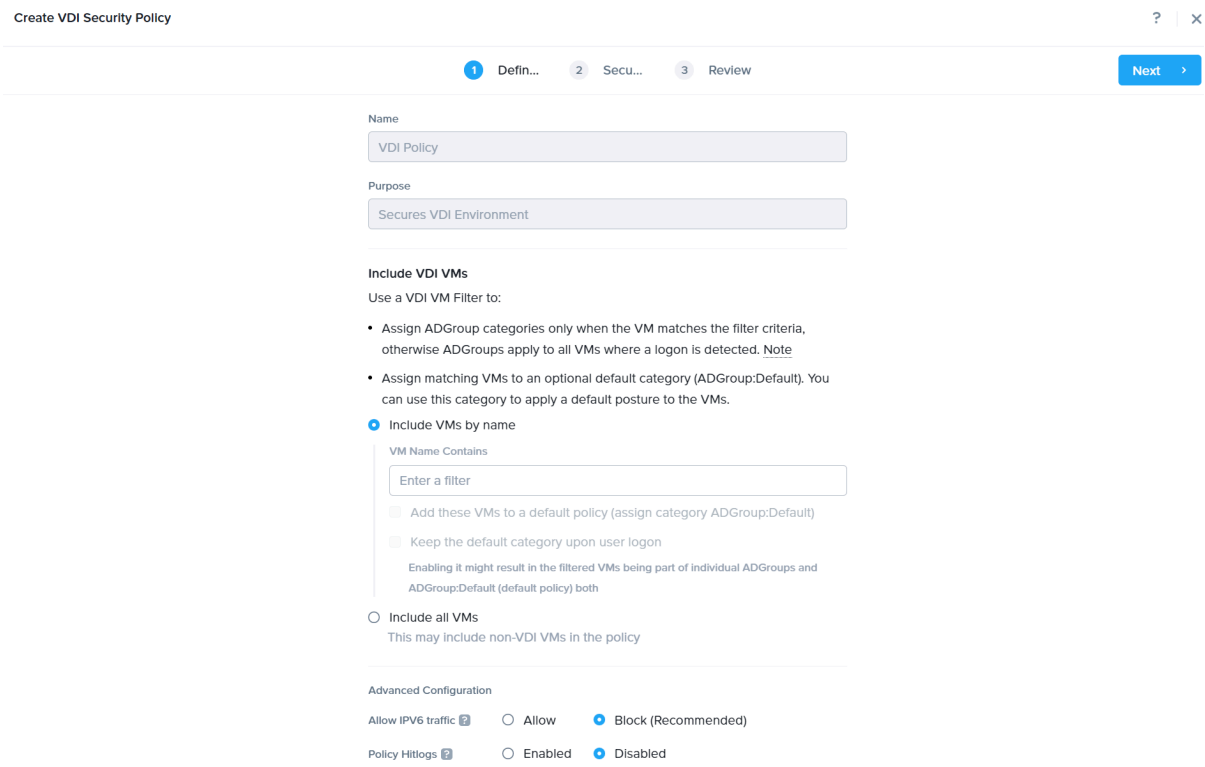


Figure 12: Define Tab

You can use the VDI VM Filter for the following scenarios.

- **Include VMs by name** - Select **Include VMs by name** and enter the matching criteria in the **VM Name Contains** field. Select the **Assign matching VMs to an optional default category (ADGroup:Default)** check-box to apply a default posture to the VMs, see Default VDI Policy on page 38 for details. Optionally, select the **Keep the default category upon user logon** check-box to preserve the default category even after user logon.

  Note:

  - Assign ADGroup categories only when the VM matches the filter criteria, otherwise ADGroups apply to all VMs where a logon is detected.
  - VMs with an AppType category assigned is never categorized with an ADGroup.
  - While updating the VDI policy, if inclusion criteria is changed to exclude and then re-include previously included VMs (that were previously logged on and categorized), upon re-inclusion the

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1814

previous categories will not be applied; consecutively, a new logon must occur for the VM for categories to apply.

- **Include all VMs** - Select **Include all VMs** to include all the VMs in the AD group in the policy. Note that non-VDI VMs will also be included in the policy if **Include all VMs** option is selected.

a. Optionally, in the **Advanced Configuration** section, select the **Allow** option to allow **IPv6 traffic**. The policy rules apply to IPv4 traffic only and all IPv6 traffic is blocked by default.

> **Note:** If you choose to block IPv6 traffic, the IPv6 traffic remains blocked even in the monitoring mode.

b. Optionally, turn on the **Policy Hit Logs** option to log traffic flow hits on the policy rules.

You can configure syslog monitoring for the policy hit logs for Flow. For details, see Configuring Syslog Monitoring in the *Prism Central Admin Central Guide*.

> **Note:** Policy hit logs are not generated if both source and destination are in inbound or outbound category.

5. In the **Secure AD Groups** tab, do the following in the indicated fields and click **Next**.

a. For **Inbound Traffic**, click **+ Add Source** and enter the category or subnets that the VDI group can receive the traffic from, as the source.

b. For each **VDI ADGroup**, click **+Add AD Group** to select the AD groups (categorized VDI VMs) that you want to secure. You can click **Import all AD Groups** to add all imported ADGroup categories to the VDI policy.

c. For **Outbound Traffic**, click **+ Add Destination** and enter the category or subnets that the VDI group can send the traffic to, as the destination.\

> **Note:** If you have not used the default VDI option in *Step 2b*, ensure that you add all of your Active Directory domain controllers as part of this step, using either categories or subnets, for each ADGroup.

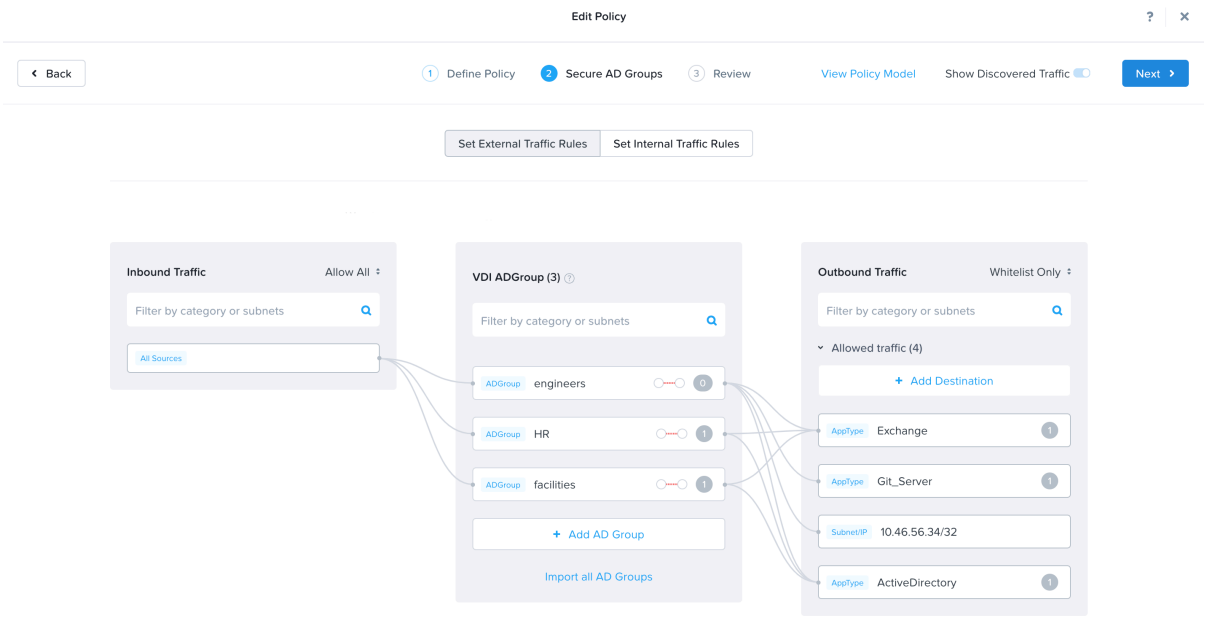


Figure 13: Secure AD Groups Tab

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1815

6. Do one of the following:

   » Click **Apply Now** to apply the VDI Policy.

   » Click **Save and Monitor** to save the configuration.

   You can switch between the monitoring and applied states on the **Security Policies** page and clicking the appropriate option in the **Actions** menu.

Default VDI Policy

The Default VDI policy feature allows you to apply a default set of rules as defined by the desktop administrator for VDI VMs and users. There are two primary use cases for Default VDI Policy (**ADGroup:Default**).

- To ensure that a VDI VM is secure even before a user logs on to the VDI VM.
- To enable access to common network resources without the need to add the resources to every tier of a VDI policy.

You can define a default VDI policy at the time of creating a new VDI policy, or by updating any existing VDI policy. See *Step 2b* of the VDI Policy Configuration topic for details.

Configuring Active Directory Domain Services

Active Directory Domain Services configuration is used to import user groups for identity based security policies.

Before you begin

- Microsegmentation must be enabled to be able to use the ID Firewall feature. For more information, see Enabling Microsegmentation on page 10.
- You must allow WMI access from Prism Central to all the Active Directory Domain Controllers in your network firewall and Active Directory firewall.
- Active Directory Requirements:
  - Minimum supported domain functional level in Active Directory is Windows Server 2008 R2.
  - ID Firewall checks the membership of Security Groups only, Distribution Groups are not supported.
  - NTP must be configured on Active Directory and Prism Central.
  - DNS must be configured on Prism Central if you want to use host name for domain controllers.

About this task

To configure an Active Directory domain, do the following.

Procedure

1. Log on to the Prism Central web console.
2. Click the collapse menu ("hamburger") button on the left of the main menu and then select **Prism Central Settings** to display the Settings page.
3. Click **ID Based Security** from the Settings menu (on the left).
   The **ID Based Security** page is displayed. This page allows you to **Add New Domain** or use an **Existing AD**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1816

4. If you select **Use Existing AD** in step 3, do the following in the indicated fields:

   a. Click the **Manually Add Domain Controller** button, then click **+ Domain Controller**.

   b. Enter the **IP Address** or **Host Name** of the domain controllers that you want to monitor for user logons events. You must add all the domain controllers associated with your Active Directory manually.

      Click **+** and add each domain controller individually, then click the blue check mark icon to save.

      > **Note:** DNS must be configured on Prism Central for the host name option to work.

5. If you select **Add New Domain** in step 3, a set of fields is displayed. Do the following in the indicated fields:

   a. **Name**: Enter a directory name.

      This is a name you choose to identify this entry; it need not be the name of an actual directory.

   b. **Domain**: Enter the domain name.

      Enter the domain name in DNS format, for example, nutanix.com.

   c. **Directory URL**: Enter the LDAP address of the directory, including the port number.

   d. **Service Account Username**: Enter the service account user name in the *`user_name@domain.com`* format that you want Prism Central to use to detect logons and query user and group information from Active Directory.

      > **Caution:** Do not use the Domain Admin account as the service account considering the security best practices. Create a new domain user and grant it required permissions as described in Configure Service Account for ID Firewall on page 39.

      A service account is a special user account that an application or service uses to interact with the Active Directory. Enter your Active Directory service account credentials in this (username) and the following (password) field.

      > **Note:** Ensure that you update the service account credentials here whenever the service account password changes or when a different service account is used.

   e. **Service Account Password**: Enter the service account password.

   f. When all the fields are correct, click the **Save** button (lower right).

      ID Firewall uses the service account for ID based security with additional requirements, see Configure Service Account for ID Firewall on page 39.

   Once saved, the **Referenced AD Groups** section is displayed. You can add a new user group by clicking **+ Add User Group** and edit the auto-generated **Category Value**. After the active directory configuration is complete, you can create the VDI Policy, see Creating a VDI Policy on page 34

6. Select **Add Inclusion Criteria** under **Manage the VM Inclusion Criteria** to specify which VMs are assigned to AD Group categories upon user logon based on VM name.

   > **Note:** It is recommend that users add inclusion criteria if at all possible to prevent any unintended categorizations.

   > **Note:** The VMs with AppType category assigned cannot be categorized by ID Based Security.

Configure Service Account for ID Firewall

Active Directory service account in Prism Central is used for connectivity with the Active Directory domain services. ID Firewall also uses the same service account for ID based security.

To configure a service account for ID firewall, do the following.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1817

1. Create a new user in the Active Directory.
2. Add the user to the **Distributed COM Users** group and the **Event Log Readers** domain groups.
3. Start the **dcomcnfg.exe** utility and go to **Component Services** > **Computers** > **My Computer** > **DCOM Config**.
4. Right-click on **Windows Management and Instrumentation** and select **Properties** from the menu.
5. Switch to **Security** tab, select **Customize** option in the **Access Permissions** section and then click **Edit**.
6. Add the user and grant **Local Access** and **Remote Access** permissions to the user. Click **OK** to confirm changes.
7. Run the `WMIMGMT.msc` command to start **Windows Management Instrumentation** snap-in.
8. Right-click on **WMI control (local)** and select **Properties** from the menu.
9. Switch to **Security** tab and expand **Root** tree.
10. Select **CIMV2** in the expanded tree and click **Security**.
11. Go to **Advanced** > **Add** > **Principal** and enter the user name.
12. Change scope by selecting **This namespace and subnamespaces** in the **Applies to** drop-down menu.
13. Click the check-box to grant the **Enable Account** and **Remote Enable** permissions. Click **OK** to confirm changes.
14. Restart the `winmgmt` service.

    ```
    C:\> net stop winmgmt
    C:\> net start winmgmt
    ```

    Alternatively, reboot the domain controller.
15. Repeat step 3 to step 14 on every domain controller.

Modifying the VDI Policy

About this task

To modify the VDI policy, do the following:

Procedure

1. In the **Security Policies** page, select the policy, click **Actions**, and then click **Update**.
2. Make the changes you want and then apply or save and monitor the policy.

   The update options are the same as those for creating a policy. For information about the options, see Creating a VDI Policy on page 34.

Applying the VDI Policy

Applying the VDI policy enforces the policy on the specified categories (VDI AD groups), and any traffic between the categories is blocked.

About this task

To apply the VDI policy, do the following:

Procedure

1. In the **Security Policies**page, select the policy, click **Actions**, and then click **Apply**.
2. Confirm by typing **Apply** in the dialog box, and then click **OK**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1818

Monitoring the VDI Policy

About this task

The VMs in VDI AD Groups in the VDI policy are allowed to communicate with each other when the policy is in the monitoring state. Traffic is blocked only during the time the policy is applied.

To monitor a security policy, do the following:

Procedure

1. In the **Security Policies**page, select the policy, click **Actions**, and then click **Monitor**.
2. Confirm by typing **Monitor** in the dialog box, and then click **OK**.

Deleting the VDI Policy

About this task

To delete the VDI policy, do the following:

Procedure

1. In the **Security Policies** page, select the VDI policy.
2. Click **Delete** in the **Actions** menu.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1819

APPLYING FILTERING AND GROUPING TO A SECURITY POLICY

You can apply different types of filters to view results based on properties like source , destination, category, ports, and more. You can also group related rule attributes together for easier visualization of connection flows. Grouping and Filtering work together to provide an intuitive view for the security policy.

About this task

To apply filtering and grouping to a security policy, do the following.

Procedure

1. Log on to the Prism Central web console.
2. Click the collapse menu ("hamburger") button on the left of the main menu and go to **Policies** > **Security**. The **Policies** page is displayed.
3. Click any policy to view the inbound, application, and outbound configuration.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1820

4. To view specific rule properties, do one of the following.

   » In the **Search** box, search for the required string using the default **All** filter.

   » Click the filter drop-down menu to search the policy based on any of the following filter types.

   Category
   : search category name and value

   Address
   : search address and subnet IP address

   Subnet IP
   : search subnet IP address

   Service
   : search service name

   Rule Description
   : search rule description

   Ports (TCP/UDP)
   : search TCP/UDP ports and services

   ICMP
   : search ICMP ports and services

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1821

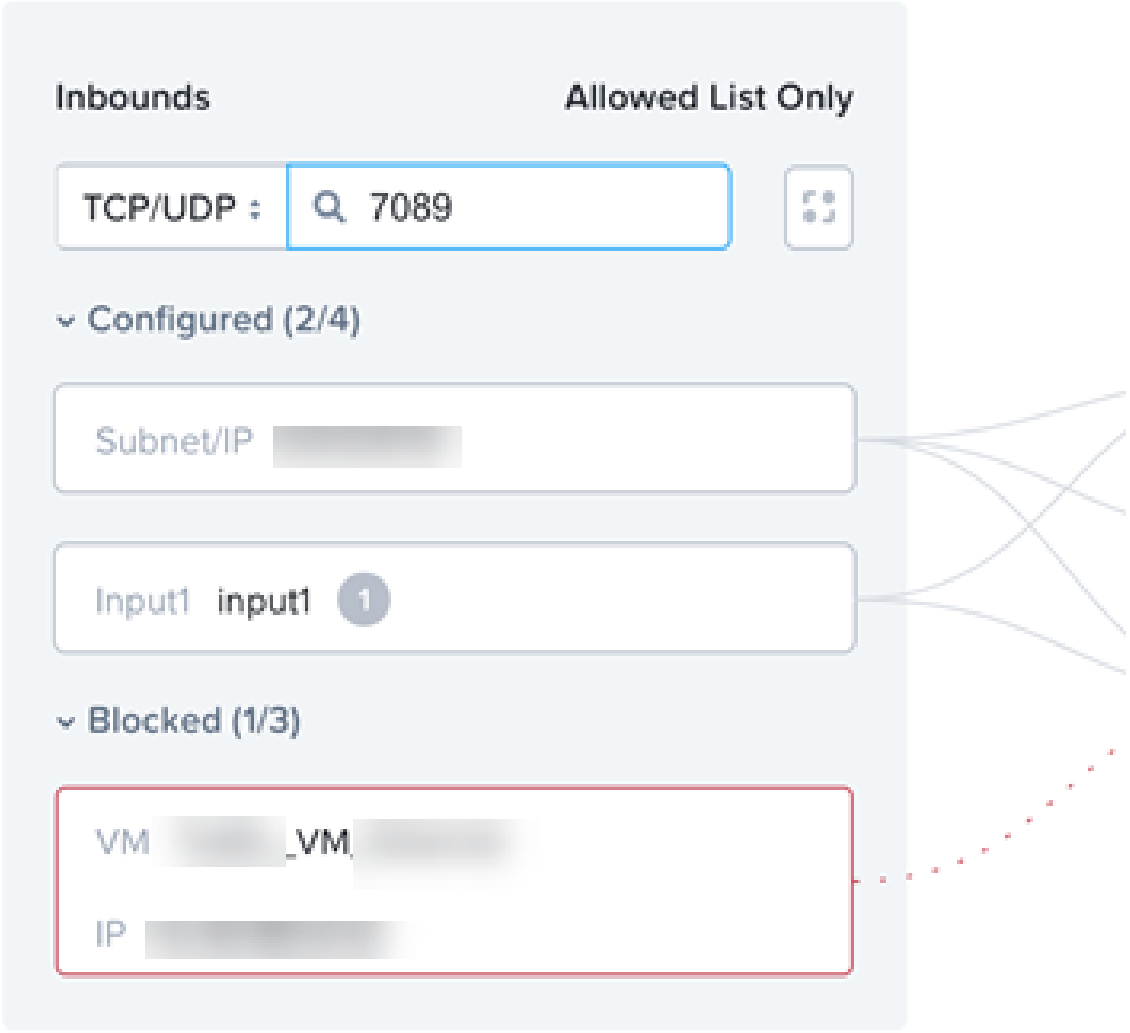


Figure 14: Filtering Policies

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1822

5. To group related rule entities together, click the group icon.

   The group option organizes related rule attributes like subnet IP, categories, and service in distinct boxes. Also, the connection flows for all the entities in a group are displayed as a single connection flow. To view all the entities belonging to a group, click the down-arrow icon to expand the group.

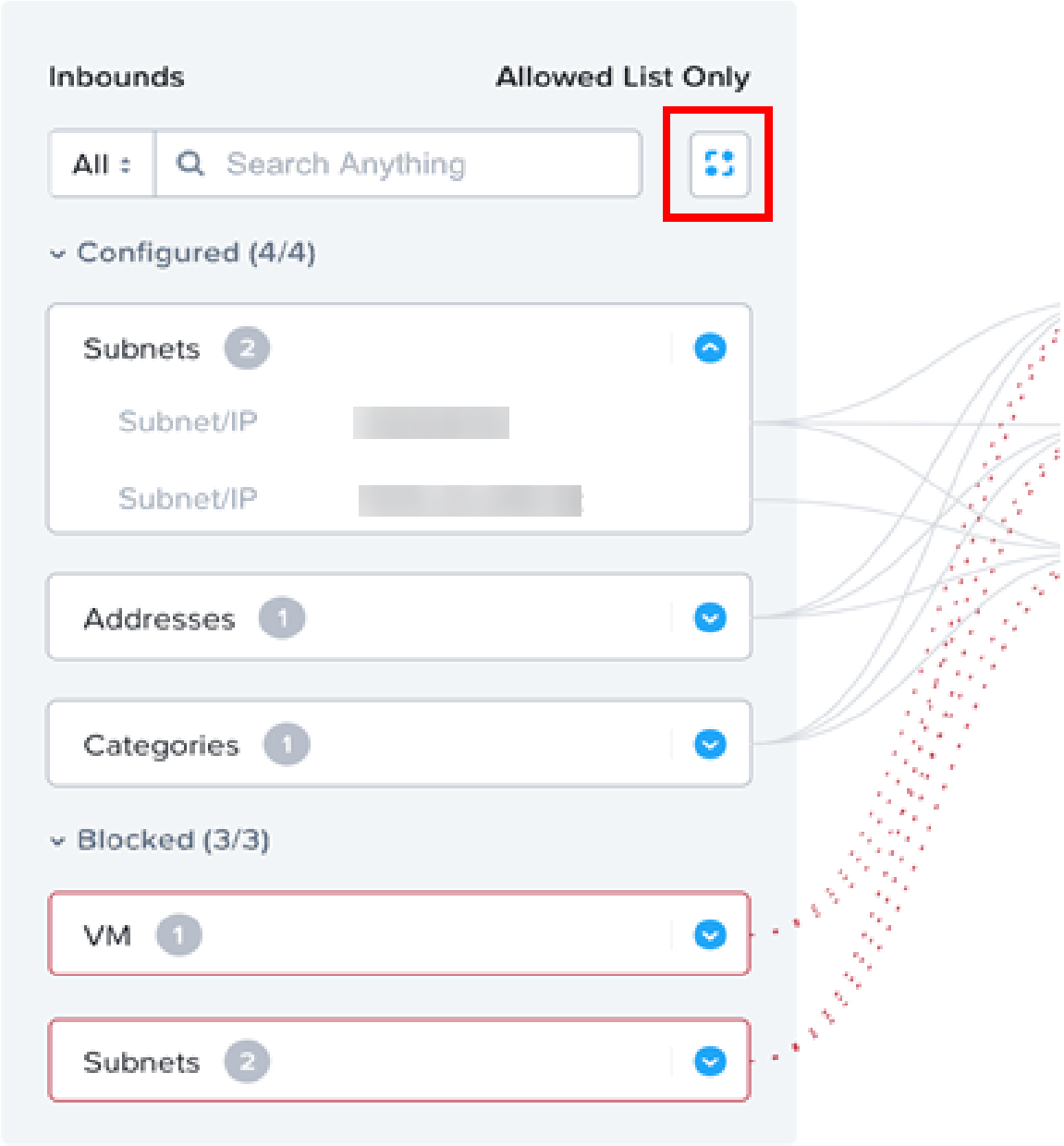


Figure 15: Filtering Policies

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1823

EXPORTING AND IMPORTING SECURITY POLICIES

Prism Central allows you to export and import security policies for the following security administration aspects.

- Have a snapshot of a working security configuration so that system can be restored to the desired state when needed.
- Ability to apply security policies as templates. This scenario is useful in ROBO environments (disaster recovery deployments) where the datacenters are being managed by multiple Prism Central instances.

Exporting Security Policies

To export or import security policy, do the following in the **Security Policies** page.

> **Note:** For VDI policy, the inclusion criteria and default VDI category settings are not included in the export process. You must set these manually after an import if required.

- Click the **Export & Import** drop down menu.
- To export the security policies, select **Export Security Policy**. The security policies binary file is downloaded.
- To import any previously exported security policies binary file, select **Import Security Policy**, then click **Browse** to select the binary file. Click **Import**. The security policies are imported.

> **Note:** Existing policies are overridden with new policies. Policies that are not part of this import are deleted.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1824

COPYRIGHT

Copyright 2024 Nutanix, Inc.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Nutanix and the Nutanix logo are registered trademarks of Nutanix, Inc. in the United States and/or other jurisdictions. All other brand and product names mentioned herein are for identification purposes only and may be trademarks of their respective holders.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1825

ExaGrid Tiered Backup Storage

Fastest Backups

Fastest Recoveries

Unparalleled, Cost-effective Scale-out

Comprehensive Security and Ransomware Recovery

ExaGrid Tiered Backup Storage

Security, Reliability, and Redundancy

ExaGrid Reliability and Redundancy Architecture

ExaGrid's architecture and implementation have multiple facets of reliability and redundancy protecting the customer's data at every step, allowing organizations to make informed vendor selections. Organizations using backup storage to hold their invaluable backup data should carefully consider how the solution is architected for reliability and redundancy. Compromises in a product's architecture or implementation may reduce product cost, but those savings are quickly dwarfed by the risk and real cost to an organization of a loss of some or all backup data.

Retention Time-Lock for Ransomware Recovery

Retention Time-Lock is a revolutionary approach to protecting backup retention data to enable fast and easy recovery from ransomware.

- ExaGrid's two-tier architecture includes a network-facing tier and a non-network-facing tier. ExaGrid alone controls the non-network-facing tier, creating a tiered air gap
- Backups are written to the network-facing-tier for fast backup performance. The most recent backups are kept in their full undeduplicated form for fast restores
- Data is adaptively deduplicated (for storage cost efficiency) into the non-network-facing tier for long-term retention data. Organizations can have as many days, weeks, months, or years of retention as they require. There is no limit to the number of version retention copies that can be saved
- If data is deleted in the network-facing tier, that data is not deleted in the non-network-facing Repository Tier for a set period of time. This allows for all data to be recoverable after a ransomware attack or other security event
- If encrypted data is sent to the network-facing tier, or if any of its data is encrypted, ExaGrid's repository tier is protected as all the deduplication objects are immutable because they are never modified

ExaGrid assumes the threat actors/hackers will take control of the backup application or the backup storage and will issue delete commands for all backups. ExaGrid has the only non-network-facing Tiered Backup Storage solution (a tiered air gap) with delayed deletes and immutable deduplication objects. This unique approach ensures when a ransomware attack occurs, data can be easily recovered or VMs booted from the ExaGrid Tiered Backup Storage system. Not only can the most recent primary storage data be restored, but all retained backups remain intact.

ExaGrid issues an alert upon on large delete attempts above the set threshold and also on data deduplication ratio change due to encryption. These act as an early warning detection of an attack.

For a more in-depth look at the Retention Time-Lock feature, please download the ExaGrid Retention Time-Lock for Ransomware Recovery data sheet.

Server Hardware and Platform Software

RAID6 Internal Storage with Consistency Checking

All ExaGrid internal storage is accessed using an industry-leading PCIe RAID controller configured to RAID6 (e.g. double-parity) with a global "hot spare" disk. In normal operation, your data is additionally protected because the RAID controller does consistency checking of the data on its disks in the background, correcting any disk media errors using the parity disks.

Because there are two parity disks, each ExaGrid appliance can tolerate the simultaneous loss of up to two disk drives. The first lost disk drive will automatically initiate a parity rebuild operation using the global hot spare. Administrators and (optionally) ExaGrid customer support are informed via alerts of the failure. A replacement disk drive is dispatched quickly, typically allowing replacement of the failed disk the next business day. Loss of the second disk does not result in loss of data since the remaining parity disk allows for data regeneration; providing more time for the important task of replacing the failed disk(s). Over 90% of ExaGrid 's customer have alerts also sent to the ExaGrid Health Reporting system.

Flash-Backed RAID Cache

The industry-leading PCIe RAID controller has an onboard volatile memory writeback cache that is backed up to non-volatile flash memory when system power is lost or interrupted.

Redundant Power Supplies

All ExaGrid models include redundant power supplies monitored by the system software, producing an alert and optionally an e-mail notification of any power supply issues. When Health Monitoring (see below) is enabled, ExaGrid customer support is made aware of the issue and can immediately arrange for the shipment of a replacement power supply. Power supplies, like disk drives, are hot-swappable.

Securing Data on the WAN

Replication of deduplicated backup data can be encrypted when transferred between ExaGrid sites using 256-bit AES, which is a FIPS PUB 140-2 Approved Security Function. This eliminates the need for a VPN to perform encryption across the WAN.

Encryption at Rest

ExaGrid offers FIPS 140-2 Validated hardware-based disk encryption on all SEC models. Self-encrypting hard disks with RAID controller-based key management and access control secures your data during the storage process.

- Uses FIPS 140-2 Validated Self-Encrypting Drives (SEDs) to ensure that data at rest is always efficiently encrypted with 256-bit AES and is never in the clear on the disk storage. All data, configuration settings, etc. are encrypted
- Drive theft protection – The drives cannot be read outside of the host system where encryption was enabled

Up to Date with Industry Standards

- ExaGrid supports IPv6
- ExaGrid is up to date with industry security features in Rocky Linux

Operating System Patches

Current ExaGrid server platform software is based on the Rocky Linux distribution. We release critical and relevant OS security patches as a part our regular ExaGrid software releases. Relevant CVEs will be included at least quarterly, with critical fixes included more quickly.

ExaGrid Software

Management Interfaces

- ExaGrid software is managed through a web interface and will, by default, accept connections from a web browser on both ports 80 (HTTP) and 443 (HTTPS). ExaGrid software supports disabling HTTP for environments that require HTTPS (secure) only. When using HTTPS, ExaGrid's certificate can be added to web browsers, or a user's certificates can be installed onto ExaGrid servers via the web interface or provided by a SCEP server
- Windows Active Directory (AD) domain credentials can be used to control access to the ExaGrid management interface, providing authentication and authorization to the web GUI
- Two-factor Authentication (2FA) can be required for any user (local or Active Directory) using any industry-standard OAUTH-TOTP application. 2FA is turned on by default is for both the Admin and Security Officer roles and any login without 2FA will create a warning prompt and an alarm for greater security.
- Role-Based Access Control using local or Active Directory credentials and Admin and Security Officer roles are fully compartmentalized

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1827

  - ***Backup Operator*** role for day-to-day operations has limitations such as no deletion of shares
  - ***Security Officer*** role protects sensitive data management and approval is required for any changes to the Retention Time-Lock policy, deletion of share, and to approve the viewing of or changes to root access
  - ***Admin*** role is like a Linux super-user – allowed to do any administrative operation (limited users given this role) Admins cannot complete sensitive data management action (such as deleting data/shares) without the Security Officer's approval
  - Adding these roles to users can only be done by a user that already has the role – so a rogue admin cannot bypass Security Officer approval of sensitive data management actions
  - Key operations require Security Officer approval to protect against internal threats, such as share deletes and de-replication (when a rogue admin turns off replication to remote site)
- Automatic user interface logout after a period of inactivity
- Although access via SSH is not necessary for user functions, some support operations can only be provided over SSH. ExaGrid secures SSH by allowing it to be disabled, allowing access via randomly generated passwords, or customer-supplied passwords, or only SSH key pairs
- Security checklist for quick and easy implementation of best practices
- Each ExaGrid server runs a proper firewall and a customized Linux distribution that opens just the ports and runs just the services necessary for receiving backups, web-based GUI, and ExaGrid-to-ExaGrid replication

Share Access

- Common Internet File System (CIFS) – SMBv2, SMBv3
- Network File System (NFS) – Versions 3 and 4
- Veeam Data Mover – SSH for command and control and Veeam-specific protocol for data movement over TCP
- Veritas OpenStorage Technology protocol (OST) – ExaGrid specific protocol over TCP
- Oracle RMAN channels using CIFS or NFS
- S3 Object Storage via https

For CIFS and Veeam Data Mover, AD integration allows using domain credentials for share and management GUI access control (authentication and authorization). For CIFS, NFS, and OST protocls, additional access control is provided via an IP whitelist. For each share, at least one IP address/mask pair is provided, with either multiple pairs or subnet mask used to broaden access. It is recommended that only the backup servers that regularly access a share are placed in a share's IP whitelist.

For Veeam shares using the Veeam Data Mover, access control is provided by username and password credentials, or is provided via an SSH key, and entered into both the Veeam and ExaGrid configuration. These can be AD credentials, or local users configured on the ExaGrid site. The Veeam Data Mover is automatically installed from the Veeam server onto the ExaGrid server over SSH. The Veeam Data Mover runs in an isolated environment on the ExaGrid server which limits system access, has no root privileges, and runs only when activated by Veeam operations.

Backup Data Checksums with Automatic Repair

As backup data is deduplicated, checksums are added to the deduplicated data as it is placed into the portion of the ExaGrid storage referred to as the Repository Tier. These end-to-end checksums cover the deduplicated backup data itself, and are used to verify the backup data during processing and as it is read from disk. The deduplicated backup data can optionally be replicated to a remote site; these checksums are used to validate the replicated data as well. During backup restore operations on shares that have been replicated to a DR site, the rare case of an invalid checksum is automatically handled by using the deduplicated data kept at the DR site.

External syslogging and SNMP

ExaGrid software can be configured to send operational information to an external syslog receiver and/or SNMP server for further integration into enterprise management systems. Examples of operational information sent to a syslog receiver include web access audits, configuration audits, hardware issues, significant software events, etc.

Deduplicated Metadata Transactional Consistency

Metadata that tracks all of the deduplicated data is kept in a database and on internal storage. Software techniques are used to ensure transactional integrity of all metadata changes, including flushing filesystem pages into the flash-backed RAID controller's onboard cache. The data flow of deduplicated backup data is protected end-to-end by the combination of checksums (above) and metadata transactional consistency.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1828

Logging Filesystem

Backup data is kept in the ExaGrid internal storage on an industry-standard logging filesystem where file activity is logged for integrity and quick repair after an unclean shutdown.

Internal Database Backups and Self-Describing Metadata

The database used to keep metadata that tracks deduplicated data is periodically dumped to internal storage. These dumps are used to quickly restore the metadata database in the case of massive failure. The database dumps are used as an optimization; the metadata kept on disk is self-describing and can be used to completely rebuild the deduplicated data in the internal repository both at the local and remote ExaGrid sites.

Replication and Inter-server Security

Replication of deduplicated backup data from one site to another can be optionally encrypted using internally-managed keys. The ExaGrid software uses a combination of Kerberos, TLS and SSH with 256-bit AES keys, which is a FIPS PUB 140-2 Approved Security Function, to secure all communications between ExaGrid servers in a site. A unique Kerberos domain is configured per site, and all sites have trust relationships automatically configured and enforced between them. All API communications are authenticated using Kerberos to ensure that commands and data cannot be tampered with while traversing the network.

Insulation from Ransomware

When ransomware strikes, it is critical to have backups insulated from the malicious encryption/damage since they may be your last line of defense. In addition to ExaGrid's Retention Time-Lock (see above), ExaGrid helps insulate backups from ransomware in the following ways:

- Comprehensive access security
  - ExaGrid shares can be accessed only from designated backup/media servers. While those servers may also be subject to rampant ransomware, the fewer servers that have access to your backups, the better. If those servers are affected by ransomware, ExaGrid's Retention Time-Lock will allow full recovery of any and all retained backups.
  - Windows Active Directory domain credentials can be used to control access to ExaGrid shares (CIFS and Veeam Data Mover) and management GUI, requiring Windows account credentials to be authenticated and authorized before access is granted to an ExaGrid share, further reducing the chance of malicious access to backups.
  - Veeam Accelerated Data Mover shares require a separate Veeam password and are accessible only via SSH, with optional key pairs, which also reduces the chance of malicious access to Veeam backups.
  - All accounts used to manage the ExaGrid software are protected using non-default passwords. This includes the backup "admin" account, the special ExaGrid customer support account, and root access.
- ExaGrid software is updated at least quarterly with the latest appropriate CVE fixes, reducing the ways ransomware can gain access to ExaGrid servers. Software may be updated more frequently as dictated by CVE severity.
- Each ExaGrid server runs a proper firewall and a customized Linux distribution that opens just the ports and runs just the services necessary for receiving backups, web-based GUI, and ExaGrid-to-ExaGrid replication.
- Communications between ExaGrid servers is secured using Kerberos authorization and authentication, protecting from a "man in the middle" attack from malicious users or software.

Periodic Assessments Using a Network Vulnerability Scanner

A complete vulnerability assessment is run periodically against ExaGrid's software. Vulnerabilities flagged by this assessment are evaluated and tracked and mitigated as appropriate.

Windows Active Directory

ExaGrid's support for Windows Active Directory allows:

- Authentication and authorization of the ExaGrid Web GUI using Active Directory user accounts and/or groups in conjunction with role-based access control (RBAC)
- Authentication and authorization of ExaGrid CIFS shares using Active Directory user accounts and/or groups
- Authentication and authorization of ExaGrid Veeam shares using Active Directory user accounts and/or groups
- Access to all ExaGrid shares can continue to be controlled via an IP "whitelist"

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1829

Key behaviors include:

- Active Directory membership of ExaGrid Server(s) is defined and performed at the ExaGrid Site level. No need to configure each and every ExaGrid Server individually.
- Each ExaGrid Site can be joined to only a single Active Directory Domain (just like Windows computers).
- All ExaGrid Servers in a multi-server ExaGrid Site must join and belong to the same Active Directory Domain.
- Different ExaGrid Sites in a multi-site ExaGrid System can be joined to different Active Directory Domains.
- Once an ExaGrid Site is added to a domain, AD user(s) and/or groups – from any trusted AD Domain – are mapped to ExaGrid management role(s) for the Web GUI – e.g. administrator, backup operator, view only, etc. This mapping is done in the ExaGrid Web GUI. Any user can then login to the ExaGrid Web GUI with their AD account/password and will only be able to perform the management actions permitted by their assigned role – aka Role-Based Access Control (RBAC).
- Once an ExaGrid Site is added to a domain, AD user(s) and/or group(s) – from any trusted AD Domain – can be used to control access to the CIFS and/or Veeam shares in that Site. The AD user/group/password is generally configured into the backup application which then presents those credentials to ExaGrid when accessing share(s).
- If an ExaGrid Site is not in an Active Directory Domain, then a locally-managed set of "local users" can be used to control access to the ExaGrid user interface and shares, including allowing "guest" access to shares.
- Microsoft supports a wide range of characters in Active Directory usernames and passwords. However ExaGrid's user interface login is currently limited to: Active Directory usernames and passwords that contain any printable, 7-bit ASCII character including special characters and spaces.

ExaGrid Support Facilities

Health Monitoring

ExaGrid servers deliver data to ExaGrid Support (phone home) using both health reporting and alerting. Health reporting includes statistics data for trending on a daily basis and automated analysis. Data is stored on secure ExaGrid servers with trending databases used to determine the overall health over time. Health reports are sent to ExaGrid using https, or secure FTP or e-mail (with some decrease in depth of analysis). Alerts are momentary notification that could indicate actionable events, including hardware failures, communications issues, potential misconfiguration, etc. ExaGrid Support promptly receives these alerts via e-mail from ExaGrid Support servers.

Secure Remote Support Access

ExaGrid Support provides a secure remote access solution so customer support engineers can provide unattended monitoring and corrective action on customer ExaGrid servers. Using a secure outbound TLS connection, tunnels are connected back into ExaGrid servers. The tunnels are secured using the highest security ECDHE and AES cipher suites, use certificate pinning for authentication, and can utilize an HTTP proxy.

Internal Database Backups and Self-Describing Metadata

The database used to keep metadata that tracks deduplicated data is periodically dumped to internal storage. These dumps are used to quickly restore the metadata database in the case of massive failure. The database dumps are used as an optimization; the metadata kept on disk is self-describing and can be used to completely rebuild the deduplicated data in the internal repository both at the local and remote ExaGrid sites.

ExaGrid reserves the right to change specifications or other product information without notice. ExaGrid and the ExaGrid logo are trademarks of ExaGrid Systems, Inc. All other trademarks are the property of their respective holders. ©2024 ExaGrid Systems, Inc. All rights reserved.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1830

ExaGrid's Value and Functionality for the Digital Operational Resilience Act (DORA)

EXAGRID®
Tiered Backup Storage

Table of Contents

What is the Digital Operational Resilience Act (DORA)? 3
Continuously Monitor Security 4
ExaGrid's User Interface Entry Screen 5
ExaGrid's Comprehensive Security Shield 6
Security, Reliability, and Redundancy 7
Retention Time-Lock for Ransomware Recovery 13

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1832

What is the Digital Operational Resilience Act (DORA)?

The Digital Operational Resilience Act (DORA) is a EU regulation that entered into force on 16 January 2023 and will apply as of 17 January 2025.

According to the European Insurance and Occupational Pensions Authority (EIOPA) website:
DORA aims at strengthening the IT security of financial entities such as banks, insurance companies, and investment firms, and making sure that the financial sector in Europe is able to stay resilient in the event of a severe operational disruption. DORA brings harmonisation of the rules relating to operational resilience for the financial sector applying to 20 different types of financial entities and ICT third-party service providers.

Organisations will need to:

1. Provide employee training
2. Manage and secure supply chain security
3. Comply with regulations for incident reporting
4. Follow a security-first approach
5. Continuously monitor security
6. Be able to recover from an attack such as ransomware

ExaGrid Tiered Backup Storage includes all of the advanced and required security features to ensure a security-first approach to backup/data protect storage including:

- All data in transit to the disaster recovery site is encrypted
- Optional data encryption at rest – at the drive level
- Ransomware recovery with
  - Non-network-facing tier (tiered air gap), delayed deletes, immutable data objects
- RBAC – Role-based Access Control
- Security Officer Role
- Two Factor Authentication – 2FA
- TLS certificates
- Secured https://
- SMB signing
- IP based whitelist
- SSH key support
- Many other security features

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1833

Continuously Monitor Security

ExaGrid continuously monitors in the following ways:

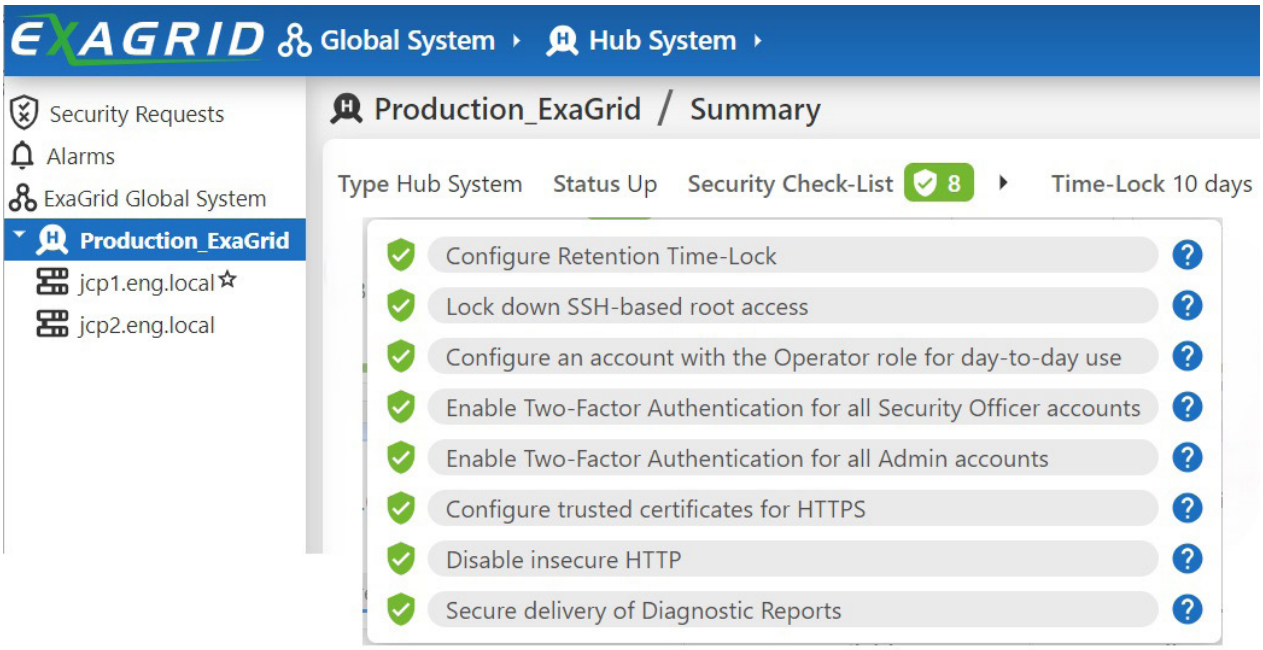
- Entry user interface screen highlights if security features are active or inactive
- ExaGrid system alerts IT staff for any change or security feature not enabled by generating an audit event that can be monitored via remote syslogging
- ExaGrid's customer support monitors via optional Health Reporting where customers' alerts and alarms are sent as a second set up eyes to monitor if key security features are disabled
- ExaGrid system alerts on early attack detection:
  - Alert on large delete (outside of set threshold) to identify a potential attack
  - Alert on deduplication ratio change to identify a potential attack where primary data is being encrypted

There is a wide range of security products that can prevent an attack, however, if an attack occurs that the last line of defense is the backup storage so that all data can be recovered to bring up operations, keep the business going, and keep all employees productive.

ExaGrid Tiered Backup Storage has a unique architecture with a front-end Landing Zone and tiered repository. The repository is not network facing. Threat actors cannot see or access the non-network-facing Repository Tier. In addition, ExaGrid employs a delayed delete policy such that any data deleted in the front end Landing Zone is not deleted in the Repository Tier until after *X* days. This approach is called Retention Time-Lock (RTL). This ensures that all data is protected and available for recovery after a ransomware attack. All objects in the Repository Tier are immutable. There is a detailed description of RTL later in this document.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1834

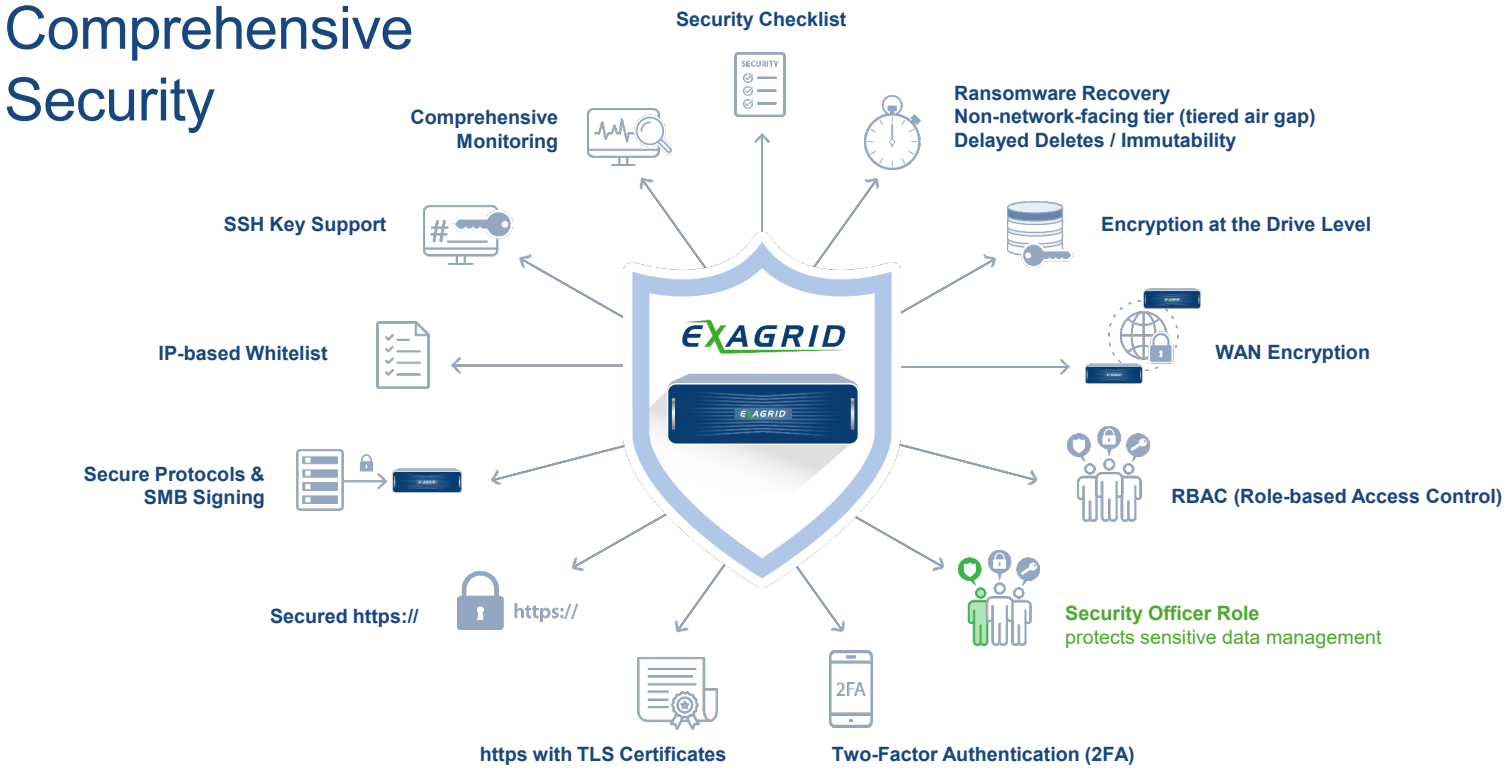
ExaGrid's User Interface Entry Screen



ExaGrid's user interface entry screen shows security status to ensure that all security features are properly enabled.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1835

ExaGrid's Comprehensive Security Shield



ExaGrid has all the security features that IT staff are asking for in backup storage.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1836

Security, Reliability, and Redundancy

ExaGrid Reliability and Redundancy Architecture

ExaGrid's architecture and implementation have multiple facets of reliability and redundancy protecting the customer's data at every step, allowing organizations to make informed vendor selections. Organizations using backup storage to hold their invaluable backup data should carefully consider how the solution is architected for reliability and redundancy. Compromises in a product's architecture or implementation may reduce product cost, but those savings are quickly dwarfed by the risk and real cost to an organization of a loss of some or all backup data.

Retention Time-Lock for Ransomware Recovery

Retention Time-Lock is a revolutionary approach to protecting backup retention data to enable fast and easy recovery from ransomware.

- ExaGrid's two-tier architecture includes a network-facing tier and a non-network-facing tier. ExaGrid alone controls the non-network-facing tier, creating a tiered air gap
- Backups are written to the network-facing tier for fast backup performance. The most recent backups are kept in their full undeduplicated form for fast restores
- Data is adaptively deduplicated (for storage cost efficiency) into the non-network-facing tier for long-term retention data. Organizations can have as many days, weeks, months, or years of retention as they require. There is no limit to the number of version retention copies that can be saved
- If data is deleted in the network-facing tier, that data is not deleted in the non-network-facing Repository Tier for a set period of time. This allows for all data to be recoverable after a ransomware attack or other security event
- If encrypted data is sent to the network-facing tier, or if any of its data is encrypted, ExaGrid's repository tier is protected as all the deduplication objects are immutable because they are never modified

ExaGrid assumes the threat actors/hackers will take control of the backup application or the backup storage and will issue delete commands for all backups. ExaGrid has the only non-network-facing Tiered Backup Storage solution (a tiered air gap) with delayed deletes and immutable deduplication objects. This unique approach ensures when a ransomware attack occurs, data can be easily recovered or VMs booted from the ExaGrid Tiered Backup Storage system. Not only can the most recent primary storage data be restored, but all retained backups remain intact.

ExaGrid issues an alert upon large delete attempts above the set threshold and also on data deduplication ratio change due to encryption. These act as an early warning detection of an attack.

See page #13 for a more detailed description of ExaGrid's Retention Time-Lock for Ransomware Recovery.

Server Hardware and Platform Software

RAID6 Internal Storage with Consistency Checking

All ExaGrid internal storage is accessed using an industry-leading PCIe RAID controller configured to RAID6 (e.g. double-parity) with a global "hot spare" disk. In normal operation, your data is additionally protected because the RAID controller does consistency checking of the data on its disks in the background, correcting any disk media errors using the parity disks.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1837

Because there are two parity disks, each ExaGrid appliance can tolerate the simultaneous loss of up to two disk drives. The first lost disk drive will automatically initiate a parity rebuild operation using the global hot spare. Administrators and (optionally) ExaGrid customer support are informed via alerts of the failure. A replacement disk drive is dispatched quickly, typically allowing replacement of the failed disk the next business day. Loss of the second disk does not result in loss of data since the remaining parity disk allows for data regeneration; providing more time for the important task of replacing the failed disk(s). Over 90% of ExaGrid 's customer have alerts also sent to the ExaGrid Health Reporting system.

Flash-Backed RAID Cache

The industry-leading PCIe RAID controller has an onboard volatile memory writeback cache that is backed up to non-volatile flash memory when system power is lost or interrupted.

Redundant Power Supplies

All ExaGrid models include redundant power supplies monitored by the system software, producing an alert and optionally an e-mail notification of any power supply issues. When Health Monitoring (see below) is enabled, ExaGrid customer support is made aware of the issue and can immediately arrange for the shipment of a replacement power supply. Power supplies, like disk drives, are hot-swappable.

Securing Data on the WAN

Replication of deduplicated backup data can be encrypted when transferred between ExaGrid sites using 256-bit AES, which is a FIPS PUB 140-2 Approved Security Function. This eliminates the need for a VPN to perform encryption across the WAN.

Encryption at Rest

ExaGrid offers FIPS 140-2 Validated hardware-based disk encryption on all SEC models. Self-encrypting hard disks with RAID controller-based key management and access control secures your data during the storage process.

- ExaGrid supports IPv6
- ExaGrid is up to date with industry security features in Rocky Linux
- ExaGrid uses FIPS 140-2 Validated Self-Encrypting Drives (SEDs) to ensure that data at rest is always efficiently encrypted with 256-bit AES and is never in the clear on the disk storage. All data, configuration settings, etc. are encrypted
- Drive theft protection – The drives cannot be read outside of the host system where encryption was enabled

Operating System Patches

Current ExaGrid server platform software is based on the Rocky Linux distribution. We release critical and relevant OS security patches as a part our regular ExaGrid software releases. Relevant CVEs will be included at least quarterly, with critical fixes included more quickly.

ExaGrid Software

Management Interfaces

- ExaGrid software is managed through a web interface and will, by default, accept connections from a web browser on both ports 80 (HTTP) and 443 (HTTPS). ExaGrid software supports disabling HTTP for environments that require HTTPS (secure) only. When using HTTPS, ExaGrid's certificate can be added to web browsers, or a user's certificates can be installed onto ExaGrid servers via the web interface or provided by a SCEP server
- Windows Active Directory (AD) domain credentials can be used to control access to the ExaGrid management interface, providing authentication and authorization to the web GUI

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1838

- Two-factor Authentication (2FA) can be required for any user (local or Active Directory) using any industry-standard OAUTH-TOTP application. 2FA is turned on by default is for both the Admin and Security Officer roles and any login without 2FA will create a warning prompt and an alarm for greater security.
- Role-Based Access Control using local or Active Directory credentials and Admin and Security Officer roles are fully compartmentalized
  - ***Backup Operator*** role for day-to-day operations has limitations such as no deletion of shares
  - ***Security Officer*** role protects sensitive data management and approval is required for any changes to the Retention Time-Lock policy, deletion of share, and to approve the viewing of or changes to root access
  - ***Admin*** role is like a Linux super-user – allowed to do any administrative operation (limited users given this role) Admins cannot complete sensitive data management action (such as deleting data/shares) without the Security Officer's approval
  - Adding these roles to users can only be done by a user that already has the role – so a rogue admin cannot bypass Security Officer approval of sensitive data management actions
  - Key operations require Security Officer approval to protect against internal threats, such as share deletes and de-replication (when a rogue admin turns off replication to remote site)
- Automatic user interface logout after a period of inactivity
- Although access via SSH is not necessary for user functions, some support operations can only be provided over SSH. ExaGrid secures SSH by allowing it to be disabled, allowing access via randomly generated passwords, or customer-supplied passwords, or only SSH key pairs
- Security checklist for quick and easy implementation of best practices
- Each ExaGrid server runs a proper firewall and a customized Linux distribution that opens just the ports and runs just the services necessary for receiving backups, web-based GUI, and ExaGrid-to-ExaGrid replication

Share Access

- Common Internet File System (CIFS) – SMBv2, SMBv3
- Network File System (NFS) – Versions 3 and 4
- Veeam Data Mover – SSH for command and control and Veeam-specific protocol for data movement over TCP
- Veritas OpenStorage Technology protocol (OST) – ExaGrid specific protocol over TCP
- Oracle RMAN channels using CIFS or NFS
- S3 Object Storage via https

For CIFS and Veeam Data Mover, AD integration allows using domain credentials for share and management GUI access control (authentication and authorization). For CIFS, NFS, and OST protocls, additional access control is provided via an IP whitelist. For each share, at least one IP address/mask pair is provided, with either multiple pairs or subnet mask used to broaden access. It is recommended that only the backup servers that regularly access a share are placed in a share's IP whitelist.

For Veeam shares using the Veeam Data Mover, access control is provided by username and password credentials entered into both the Veeam and ExaGrid configuration. These can be AD credentials, or local users configured on the ExaGrid site. The Veeam Data Mover is automatically installed from the Veeam server onto the ExaGrid server over SSH. The Veeam Data Mover runs in an isolated environment on the ExaGrid server which limits system access, has no root privileges, and runs only when activated by Veeam operations.

Backup Data Checksums with Automatic Repair

As backup data is deduplicated, checksums are added to the deduplicated data as it is placed into the portion of the ExaGrid storage referred to as the Repository Tier.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1839

These end-to-end checksums cover the deduplicated backup data itself, and are used to verify the backup data during processing and as it is read from disk. The deduplicated backup data can optionally be replicated to a remote site; these checksums are used to validate the replicated data as well. During backup restore operations on shares that have been replicated to a DR site, the rare case of an invalid checksum is automatically handled by using the deduplicated data kept at the DR site.

External syslogging and SNMP

ExaGrid software can be configured to send operational information to an external syslog receiver and/or SNMP server for further integration into enterprise management systems. Examples of operational information sent to a syslog receiver include web access audits, configuration audits, hardware issues, significant software events, etc.

Deduplicated Metadata Transactional Consistency

Metadata that tracks all of the deduplicated data is kept in a database and on internal storage. Software techniques are used to ensure transactional integrity of all metadata changes, including flushing filesystem pages into the flash-backed RAID controller's onboard cache. The data flow of deduplicated backup data is protected end-to-end by the combination of checksums (above) and metadata transactional consistency.

Logging Filesystem

Backup data is kept in the ExaGrid internal storage on an industry-standard logging filesystem where file activity is logged for integrity and quick repair after an unclean shutdown.

Internal Database Backups and Self-Describing Metadata

The database used to keep metadata that tracks deduplicated data is periodically dumped to internal storage. These dumps are used to quickly restore the metadata database in the case of massive failure. The database dumps are used as an optimization; the metadata kept on disk is self-describing and can be used to completely rebuild the deduplicated data in the internal repository both at the local and remote ExaGrid sites.

Replication and Inter-server Security

Replication of deduplicated backup data from one site to another can be optionally encrypted using internally-managed keys. The ExaGrid software uses a combination of Kerberos, TLS and SSH with 256-bit AES keys, which is a FIPS PUB 140-2 Approved Security Function, to secure all communications between ExaGrid servers in a site. A unique Kerberos domain is configured per site, and all sites have trust relationships automatically configured and enforced between them. All API communications are authenticated using Kerberos to ensure that commands and data cannot be tampered with while traversing the network.

Insulation from Ransomware

When ransomware strikes, it is critical to have backups insulated from the malicious encryption/damage since they may be your last line of defense. In addition to ExaGrid's Retention Time-Lock (see above), ExaGrid helps insulate backups from ransomware in the following ways:

- Comprehensive access security
  - ExaGrid shares can be accessed only from designated backup/media servers. While those servers may also be subject to rampant ransomware, the fewer servers that have access to your backups, the better. If those servers are affected by ransomware, ExaGrid's Retention Time-Lock will allow full recovery of any and all retained backups.
  - Windows Active Directory domain credentials can be used to control access to ExaGrid shares (CIFS and Veeam Data Mover) and management GUI, requiring Windows account credentials to be authenticated and authorized before access is granted to an ExaGrid share, further reducing the chance of malicious access to backups.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1840

  - Veeam Accelerated Data Mover shares require a separate Veeam password and are accessible only via SSH, with optional key pairs, which also reduces the chance of malicious access to Veeam backups.
  - All accounts used to manage the ExaGrid software are protected using non-default passwords. This includes the backup "admin" account, the special ExaGrid customer support account, and root access.

- ExaGrid software is updated at least quarterly with the latest appropriate CVE fixes, reducing the ways ransomware can gain access to ExaGrid servers. Software may be updated more frequently as dictated by
  CVE severity.
- Each ExaGrid server runs a proper firewall and a customized Linux distribution that opens just the ports and runs just the services necessary for receiving backups, web-based GUI, and ExaGrid-to-ExaGrid replication.
- Communications between ExaGrid servers is secured using Kerberos authorization and authentication, protecting from a "man in the middle" attack from malicious users or software.

Periodic Assessments Using a Network Vulnerability Scanner

A complete vulnerability assessment is run periodically against ExaGrid's software. Vulnerabilities flagged by this assessment are evaluated and tracked and mitigated as appropriate.

Windows Active Directory

ExaGrid's support for Windows Active Directory allows:

- Authentication and authorization of the ExaGrid Web GUI using Active Directory user accounts and/or groups in conjunction with role-based access control (RBAC)
- Authentication and authorization of ExaGrid CIFS shares using Active Directory user accounts and/or groups
- Authentication and authorization of ExaGrid Veeam shares using Active Directory user accounts and/or groups
- Access to all ExaGrid shares can continue to be controlled via an IP "whitelist"

Key behaviors include:

- Active Directory membership of ExaGrid Server(s) is defined and performed at the ExaGrid Site level. No need to configure each and every ExaGrid Server individually.
- Each ExaGrid Site can be joined to only a single Active Directory Domain (just like Windows computers).
- All ExaGrid Servers in a multi-server ExaGrid Site must join and belong to the same Active Directory Domain.
- Different ExaGrid Sites in a multi-site ExaGrid System can be joined to different Active Directory Domains.
- Once an ExaGrid Site is added to a domain, AD user(s) and/or groups – from any trusted AD Domain – are mapped to ExaGrid management role(s) for the Web GUI – e.g. administrator, backup operator, view only, etc. This mapping is done in the ExaGrid Web GUI. Any user can then login to the ExaGrid Web GUI with their AD account/password and will only be able to perform the management actions permitted by their assigned role – a.k.a. Role-Based Access Control (RBAC).
- Once an ExaGrid Site is added to a domain, AD user(s) and/or group(s) – from any trusted AD Domain – can be used to control access to the CIFS and/or Veeam shares in that Site. The AD user/group/password is generally configured into the backup application which then presents those credentials to ExaGrid when accessing share(s).
- If an ExaGrid Site is not in an Active Directory Domain, then a locally-managed set of "local users" can be used to control access to the ExaGrid user interface and shares, including allowing "guest" access to shares.
- Microsoft supports a wide range of characters in Active Directory usernames and passwords. However ExaGrid's user interface login is currently limited to: Active Directory usernames and passwords that contain any printable, 7-bit ASCII character including special characters and spaces.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1841

ExaGrid Support Facilities

Health Monitoring

ExaGrid servers deliver data to ExaGrid Support (phone home) using both health reporting and alerting. Health reporting includes statistics data for trending on a daily basis and automated analysis. Data is stored on secure ExaGrid servers with trending databases used to determine the overall health over time. Health reports are sent to ExaGrid using https, or secure FTP or email (with some decrease in depth of analysis). Alerts are momentary notification that could indicate actionable events, including hardware failures, communications issues, potential misconfiguration, etc. ExaGrid Support promptly receives these alerts via e-mail from ExaGrid Support servers.

Secure Remote Support Access

ExaGrid Support provides a secure remote access solution so customer support engineers can provide unattended monitoring and corrective action on customer ExaGrid servers. Using a secure outbound TLS connection, tunnels are connected back into ExaGrid servers. The tunnels are secured using the highest security ECDHE and AES cipher suites, use certificate pinning for authentication, and can utilize an HTTP proxy.

Internal Database Backups and Self-Describing Metadata

The database used to keep metadata that tracks deduplicated data is periodically dumped to internal storage. These dumps are used to quickly restore the metadata database in the case of massive failure. The database dumps are used as an optimization; the metadata kept on disk is self-describing and can be used to completely rebuild the deduplicated data in the internal repository both at the local and remote ExaGrid sites.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1842

Retention Time-Lock for Ransomware Recovery

Ransomware attacks are on the rise, becoming disruptive and potentially very costly to businesses. No matter how meticulously an organization follows best practices to protect valuable data, the attackers seem to stay one step ahead. They maliciously encrypt primary data, take control of the backup application and delete the backup data.

Protection from ransomware is a primary concern for organizations today. ExaGrid offers a unique approach to ensuring that attackers cannot compromise the backup data.

The challenge is how to protect the backup data from being deleted while at the same time allow for backup retention to be purged when retention points are achieved. If you retention lock all of the data, you cannot delete the retention points and the storage costs become untenable. If you allow retention points to be deleted to save storage, you leave the system open for hackers to delete all data.

ExaGrid's unique approach is called Retention Time-Lock (RTL). It prevents the threat actors/hackers from deleting the backups and allows for retention points to be purged. The result is a strong data protection and recovery solution at a very low cost of storage.

ExaGrid is Tiered Backup Storage with a front-end disk-cache Landing Zone and separate Repository Tier containing all retention data. Data is written directly to the "network facing" ExaGrid disk-cache Landing Zone. Then it is tiered into a "non-network-facing" long-term retention repository where it is stored as deduplicated data objects to reduce the storage cost of long-term retention data. As data is tiered to the Repository Tier, it is deduplicated and stored in a series of objects and metadata. As with other object storage systems, the ExaGrid objects and metadata never change allowing only for the creation of new objects or deletion of old objects when retention is reached.

ExaGrid's approach to ransomware allows organizations to set up a time lock period that governs the processing of any delete requests in the Repository Tier as that tier is not network facing and not accessible to hackers. The combination of a non-network-facing tier, a delayed deletion for a period of time and objects that never change are the elements of the ExaGrid Retention Time-Lock solution. For example, if the time lock period for the Repository Tier is set to 10 days, then when delete requests are sent to the ExaGrid from a backup application that has been compromised or from a hacked CIFS or other communications protocols, the data in the Repository Tier is time-locked for up to 10 days against any deletion. The data in the Landing Zone will be deleted or encrypted, however, the Repository Tier data is not deleted upon an external request for the configured period of time. When a ransomware attack is identified, simply put the ExaGrid system into a new recover mode and then restore any and all backup data to primary storage. The time lock period is separate and in addition to the days, week, months and year or retention that is set by the backup application and stored by ExaGrid in the retention repository.

The solution provides a retention lock, but only for an adjustable period of time as it delays the deletes. ExaGrid chose not to implement Retention Time-Lock forever because the cost of the storage would be unmanageable. ExaGrid already has the long term backup retention so it would be redundant to have a separate store with retention lock. The 10-day default policy for delayed deletes only takes an additional 10% of storage space. ExaGrid allows the delay of deletes from 1 day to 30 days.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1843

Recovery Process – 5 Easy Steps

- Invoke recover mode
  - Retention Time-Lock clock is stopped with all deletes put on hold indefinitely until data recovery operation is complete
- Contact assigned level 2 ExaGrid customer support engineer
  - The backup administrator can carry out the recovery using the ExaGrid GUI, but since this is not a common operation, we suggest contacting ExaGrid customer support
- Determine the time of the event so you can plan restore
- Determine which backup on the ExaGrid completed deduplication before the event
- Perform restore from that backup using the backup application

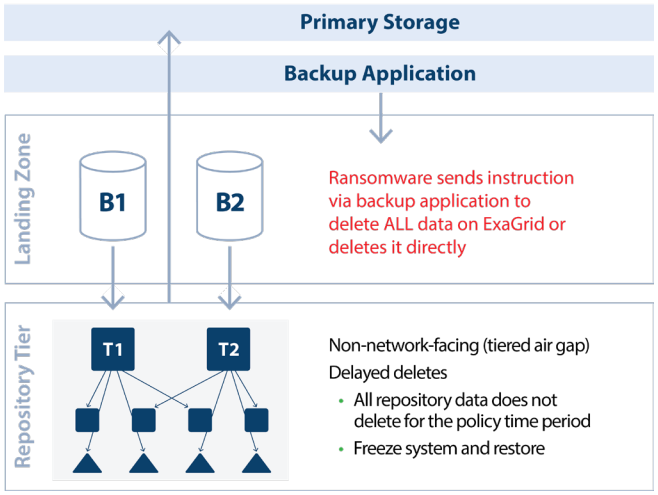
ExaGrid advantages are:

- Manage a single system instead of multiple systems for both backup storage and ransomware recovery
- Unique second Retention Tier that is only visible to ExaGrid software not to the network
- Data is not deleted as delete requests are delayed and therefore ready to recover after a ransomware attack
- Weekly, monthly, yearly and other purges still occur to keep storage costs in line with the retention periods
- The 10-day default policy for delayed deletes only takes an additional 5% to 10% of storage space
- Storage does not grow forever and stays within the backup retention period set to keep storage costs down
- All retention data (most recent backups and all retention) is preserved and is not deleted

Example Scenarios

- Data is deleted in the ExaGrid disk-cache Landing Zone via the backup application or by hacking the communication protocol. Since the Retention Tier data has a delayed delete time lock, the objects are still intact and available to restore. When the ransomware event is detected, simply put the ExaGrid in a new recover mode and restore. You have as much time to detect the ransomware attack as the time lock was set for on the ExaGrid. If you had the time lock set for 10 days, then you have 10 days to detect the ransomware attack and put the ExaGrid system in the new recover mode for restoring data.

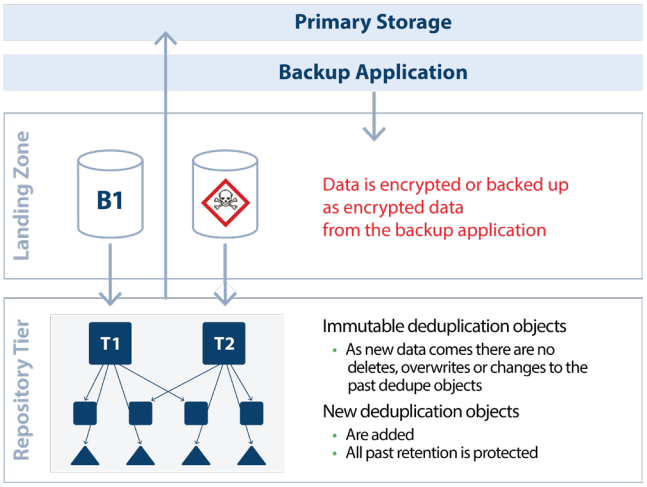
Deletion Protection of Backup Data on ExaGrid



Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1844

- Data is encrypted in the ExaGrid disk-cache Landing Zone or is encrypted on the primary storage and backed up to ExaGrid such that ExaGrid has encrypted data in the Landing Zone and deduplicates it into the Repository Tier. The data in the Landing Zone is encrypted. However, all previously deduplicated data objects never change (immutable), so they are never impacted by the newly arrived encrypted data. ExaGrid has all previous backups before the ransomware attack that can be restored immediately. In addition to being able to recover from the most recent deduplicated backup, the system still retains all the backup data according to the retention requirements.

Encryption Protection of Backup Data on ExaGrid



Features:

- Any deletion requests are delayed by the number of days in the protection policy
- Encrypted data written to ExaGrid does not delete or change previous backups in the repository
- Landing Zone data that is encrypted does not delete or change previous backups in the repository
- Set delayed deletion in 1 day increments from 0 days to 30 days
- Protects against loss of any and all retained backups including monthlies and yearlies
- Two-Factor Authentication (2FA) protects changes to Time-Lock setting
  - Only Security Officer role is allowed to approve changes to Time-Lock setting
  - 2FA with Login/Password and system generated QR code protects all accounts
- Separate password for primary site versus second site ExaGrid
- Separate backup staff and security staff roles and passwords
- **Alarm on Delete**
  - Alarm on large delete: A value can be set as a threshold by the backup administrator (default is 50%) and if a delete is more than the threshold, system will raise an alarm, only Admin role can clear this alarm.
  - A threshold can be configured, by individual share, based on backup pattern. (The default value is 50% for every share). When a delete request comes to the system, the ExaGrid system will honor the request and delete the data. If RTL is enabled, the data will be retained for the RTL policy (for the number of days
    set by an organization). When RTL is enabled, organizations will be able to recover the data using the PITR (Point-In-Time-Recovery).
  - If an organization gets false positive alarm frequently, the Admin role can adjust the threshold value from 1-99% to avoid more false alarms.
- **Alarm on Data Deduplication Ratio Change**
  - If primary storage is encrypted and sent to the ExaGrid from the backup application or if the threat actor encrypts the data on the ExaGrid Landing Zone, ExaGrid will see significant drop in the deduplication ratio being achieved and will send an alarm. The data in the Repository Tier remains protected.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1845

United States 100 Campus Drive / Marlborough, MA 01752 / (800) 868-6985
United Kingdom 200 Brook Drive / Green Park, Reading, Berkshire RG2 6UB / +44 (0) 1189 497 051
Singapore 1 Raffles Place, #20-61 / One Raffles Place Tower 2 / 048616 / +65 6808 5574

ExaGrid reserves the right to change specifications or other product information without notice. ExaGrid and the ExaGrid logo are trademarks of ExaGrid Systems, Inc. All other trademarks are the property of their respective holders.

©2024 ExaGrid Systems, Inc. All rights reserved.

ExaGrid Tiered Backup Storage

Technical Specifications

Application Support – All ExaGrid Appliances

Backup Applications, Utilities, and Methods

- Acronis Backup & Recovery
- Arcserve Backup, D2D, UDP
- Arctera Backup Exec
- Arctera System Recovery
- Bacula Enterprise
- BridgeHead
- Commvault
- Commvault Cloud (Metallic)
- Dell NetWorker
- HYCU
- IBM Storage Protect (TSM)
- IBM i and LaserVault ViTL
- Idera SQL Safe
- MongoDB Ops Manager
- NetBackup
- OpenText Data Protector
- Oracle RMAN
- POSIX-compliant TAR files
- Quest LiteSpeed
- Quest NetVault
- Red Gate SQL Backup
- Rubrik
- SQL Dumps
- Veeam Data Platform
- Veeam Backup for Microsoft365
- Zerto

Site Configurations

- Scalable from 10TB to 6PB full backup (32TB to 12.09PB raw) with 32 servers in a single system with Retention Time-Lock (RTL) enabled for ransomware recovery
- Hub-and-spoke architecture
- Mix and match different size/age appliance models (mixing appliances in a system with and without encryption at rest is not supported)
- Multi-hop for a tertiary copy
- ExaGrid systems (one hub and up to 15 spokes)
- Standard IP WAN connection between sites
- WAN encryption for secure data transfer
- Bandwidth throttling for WAN efficiency

Appliance Configurations

ExaGrid Model	EX10	EX20	EX36	EX54	EX81	EX84	EX135*	EX189*
Chassis	2U	2U	2U	2U	2U	2U	2U	2U
Chassis Depth	26.8 inches/680 mm					34.65 inches/880 mm		
Full Backup	10TB	20TB	36TB	54TB	81TB	84TB	135TB	189TB
Disks	8	8	12	9	12	24	18	24
Disk Size	4TB	8TB	8TB	18TB	18TB	8TB	18TB	18TB
Memory	16 GiB	32 GiB	64 GiB	64 GiB	128 GiB	128 GiB	192 GiB	256 GiB
CPUs / Cores	1 CPU 6 hyper-threaded cores			1 CPU 16 hyper-threaded cores				
NIC Ports	Two 1GbE; up to two optional 10Gbe or 25GbE ports			Two 1GbE; up to four optional 10Gbe or 25GbE ports				

All Servers: Intel or AMD processors / Enterprise SAS drives / FIPS 140-2 Self-Encrypting SAS drives for all SEC systems / RAID6 with hot spare / Redundant fans / Redundant power supplies / ExaGrid software /19-inch rack-mount chassis with dedicated IPMI network port

** EX135/EX189 available with optional Cable Management Arm*

Regulatory Approvals

- CB Certificate
- CISPR 32/35
- EN 55035
- EN 55022/32
- EN 55032:2015
- EN 60950-1
- EN 6100-3 2/3/4
- EN 62368-1
- FCC Class A
- ICES-003
- IEC 60950-1
- IEC 6100-3-3
- IEC 62368-1
- EN 6100-3-2/4
- RoHS Compliant
- UKCA
- UL/CSA 60950-1
- UL/CSA 62368-1
- VCCI
- WEEE Declaration EU Directive

Environmental Requirements

	Power	Temperature	Humidity	Cooling (Operating)	Sound Power Level	In-rush Wattage
All Appliances	Frequency: 50-60 Hz / Voltage: 100-240 VAC Two NEMA 5-15R 3-prong receptacles/appliance Country kits available for international orders EX10: 144W EX20: 176W EX36: 272W EX54: 240W EX81: 300W EX84: 493W EX135: 373W EX189: 416W	10° to 35° C (50° to 95° F)	20% to 80% non-condensing	EX10: 491 BTU/hr EX20: 600 BTU/hr EX36: 928 BTU/hr EX54: 818 BTU/hr EX81: 1023 BTU/hr EX84: 1680 BTU/hr EX135: 1272 BTU/hr EX189: 1419 BTU/hr	EX84/EX135/EX189: 84 dBA Others: 82 dBA	EX10: 215W EX20: 256W EX36: 323W EX54: 291W EX81: 312W EX84: 612W EX135: 557W EX189: 605W

United States 100 Campus Drive / Marlborough, MA 01752 / (800) 868-6985
United Kingdom 200 Brook Drive / Green Park, Reading, Berkshire RG2 6UB / +44 (0) 1189 497 051
Singapore 1 Raffles Place, #20-61 / One Raffles Place Tower 2 / 048616 / +65 6808 5574

exagrid.com

ExaGrid reserves the right to change specifications or other product information without notice. ExaGrid and the ExaGrid logo are trademarks of ExaGrid Systems, Inc. All other trademarks are the property of their respective holders. ©2025 ExaGrid Systems, Inc. All rights reserved.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1847

Datasheet

NVIDIA L40S

Unparalleled AI and graphics performance for the data center.

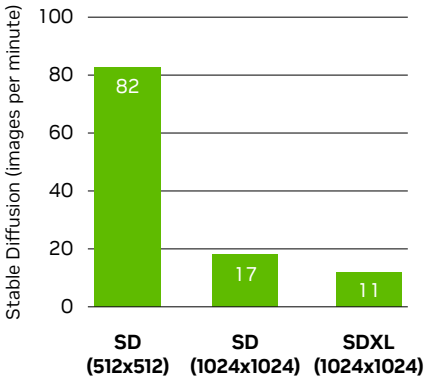
Generative AI is fueling transformative change, unlocking a new frontier of opportunities for enterprises across every industry. To transform with AI, enterprises need more compute resources, greater scale, and a broad set of capabilities to meet the demands of an ever-increasing set of diverse and complex workloads.

The NVIDIA L40S GPU is the most powerful universal GPU for the data center, delivering end-to-end acceleration for the next generation of AI-enabled applications—from **gen AI**, LLM inference, small-model training and fine-tuning to 3D graphics, rendering, and video applications.

Accelerate Next-Generation Workloads

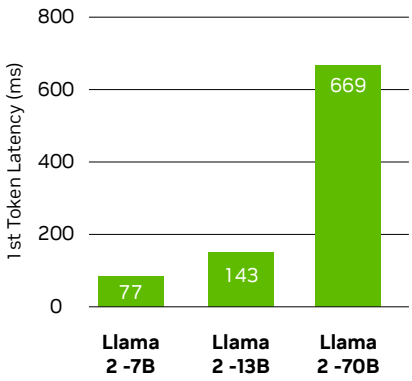
- Generative AI
- LLM inference
- LLM fine-tuning and small-model training
- NVIDIA Omniverse™ Enterprise
- Rendering and 3D graphics
- Streaming and video content

Generative AI Image Generation



Measured performance; NVIDIA L40S Stable Diffusion v2.1, TRT 8.6.1, BS:1, FP16 | Stable Diffusion XL 1.0, TRT 8.6.1, BS:1, FP16

Large Language Model (LLM) Inference



Measured performance; NVIDIA L40S Llama 2-7B/13B/70B, ISL=2048, OSL=128, BS=1: FP8.

Powered by the NVIDIA Ada Lovelace Architecture

Fourth-Generation Tensor Cores

Hardware support for structural sparsity and optimized TF32 format provides out-of-the-box performance gains for faster AI and data science model training. Accelerate AI-enhanced graphics capabilities with **DLSS** to upscale resolution with better performance in select applications.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1848

Third-Generation RT Cores

Enhanced throughput and concurrent ray-tracing and shading capabilities improve ray-tracing performance, accelerating renders for product design and architecture, engineering, and construction workflows. See lifelike designs in action with hardware-accelerated motion blur and stunning real-time animations.

Transformer Engine

Transformer Engine dramatically accelerates AI performance and improves memory utilization for both training and inference. Harnessing the power of the **Ada Lovelace fourth-generation Tensor Cores**, Transformer Engine intelligently scans the layers of transformer architecture neural networks and automatically recasts between FP8 and FP16 precisions to deliver faster AI performance and accelerate training and inference.

Data Center Ready

The L40S GPU is optimized for 24/7 enterprise data center operations and designed, built, tested, and supported by NVIDIA to ensure maximum performance, durability, and uptime. The L40S GPU meets the latest data center standards, is Network Equipment-Building System (NEBS) Level 3 ready, and features secure boot with root of trust technology, providing an additional layer of security for data centers.

Technical Specifications	
GPU Architecture	NVIDIA Ada Lovelace Architecture
GPU Memory	48GB GDDR6 with ECC
Memory Bandwidth	864GB/s
Interconnect Interface	PCIe Gen4 x16: 64GB/s bidirectional
NVIDIA Ada Lovelace Architecture-Based CUDA® Cores	18,176
NVIDIA Third-Generation RT Cores	142
NVIDIA Fourth-Generation Tensor Cores	568
RT Core Performance TFLOPS	209
FP32 TFLOPS	91.6
TF32 Tensor Core TFLOPS	183 I 366*
BFLOAT16 Tensor Core TFLOPS	362.05 I 733*
FP16 Tensor Core	362.05 I 733*
FP8 Tensor Core	733 I 1,466*
Peak INT8 Tensor TOPS	733 I 1,466*
Peak INT4 Tensor TOPS	733 I 1,466*
Form Factor	4.4" (H) x 10.5" (L), dual slot
Display Ports	4x DisplayPort 1.4a
Max Power Consumption	350W
Power Connector	16-pin

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1849

Thermal	Passive
Virtual GPU (vGPU) Software Support	Yes
vGPU Profiles Supported	See the **virtual GPU licensing guide**
NVENC I NVDEC	3x I 3x (includes AV1 encode and decode)
Secure Boot With Root of Trust	Yes
NEBS Ready	Level 3
MIG Support	No
NVIDIA® NVLink® Support	No

* With sparsity

Ready to Get Started?

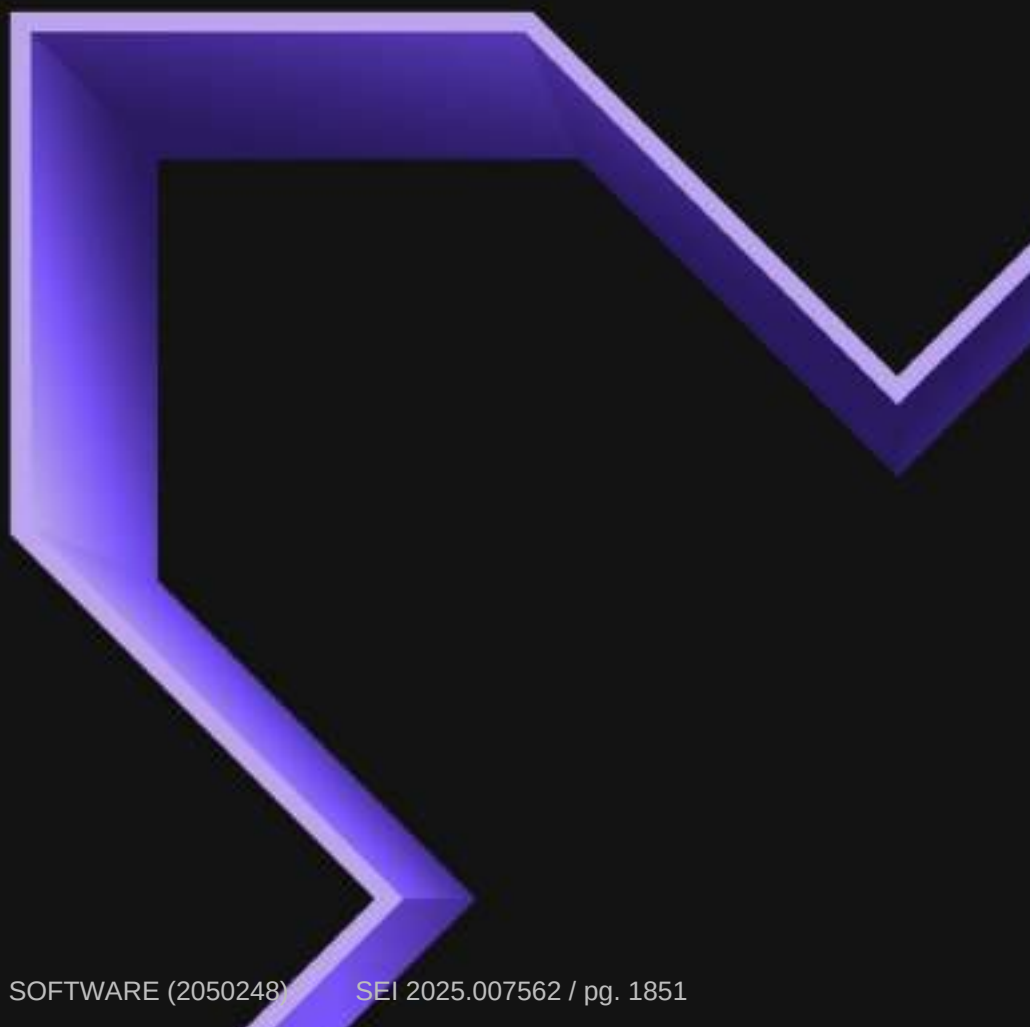
To learn more about the NVIDIA L40S, visit **www.nvidia.com/l40s**

© 2024 NVIDIA Corporation and affiliates. All rights reserved. NVIDIA, the NVIDIA logo, CUDA, HGX, NVLink, and Omniverse are trademarks and/or registered trademarks of NVIDIA Corporation and affiliates in the U.S. and other countries. Other company and product names may be trademarks of the respective owners with which they are associated. 3110647. FEB24

Prism Element Web Console Guide

Prism 7.0

January 21, 2025



NUTANIX

Contents

Help Organization.....8

Nutanix Platform Overview..... 9

Guest VM Data Management..... 9
MapReduce Tiering..... 10
Live Migration..... 10
High Availability..... 10
Virtualization Management VM High Availability..... 11
Data Path Redundancy..... 11
Cluster Components..... 12
Zeus..... 12
Zookeeper..... 12
Medusa..... 13
Cassandra..... 13
Stargate..... 13
Curator..... 13
Prism..... 13
Single-node Clusters..... 14
Two-Node Clusters..... 17
Cluster Resiliency..... 22
Failure Handling in a Nutanix Cluster..... 22
Cluster Fault Tolerance..... 25
Fault Domains in a Nutanix Cluster..... 29
Cluster Rebuild Preference..... 40
Replication Factor..... 41
Replication Factor 2..... 41
Replication Factor 3..... 42
Replication Factor 1..... 42
Degraded Node..... 45
Degraded Node Detection..... 48
Enabling Degraded Node Detection..... 49
Managing a Degraded Node..... 49
Maximum System Values..... 51
Three Node Cluster Considerations..... 52

Cluster Management..... 53

Prism Element Web Console Overview..... 53
Logging Into the Prism Element Web Console..... 54
Logging Out of the Prism Element Web Console..... 57
Main Menu..... 58
Settings Menu..... 60
Home Dashboard..... 63
Monitoring Disk Rebuild Progress..... 68
Monitoring Node Rebuild Progress..... 69
Understanding Displayed Statistics..... 70
Modifying UI Settings..... 71
Finding the AHV Version on Prism Element..... 73

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1852

Finding the AOS Version Using Prism Element..... 74
Prism Licensing..... 74
Modifying Cluster Details..... 74
Virtual IP Address Impact..... 75
iSCSI Data Services IP Address Impact..... 76
Cluster Fault Tolerance Configuration..... 76
Increasing the Cluster Fault Tolerance Level..... 76
Modifying Cluster Rebuild Preference..... 78
Software and Firmware Upgrades..... 78
Life Cycle Management (LCM)..... 79
Nutanix Cluster Check (NCC)..... 79
Use Upgrade Software in the Prism Element Web Console (Legacy 1-Click Upgrade)..... 80
View Task Status..... 89
Multi-Cluster Management..... 93
Installing Prism Central Using 1-Click Method..... 93
Registering or Unregistering a Cluster with Prism Central..... 98
Restoring Prism Central (1-Click Recovery)..... 102
CVM Memory Configuration..... 105
Increasing the Controller VM Memory Size..... 106
Resource Requirements Supporting Snapshot Frequency (Asynchronous, NearSync, and Metro)..... 107
Rebooting an AHV or ESXI Node in a Nutanix Cluster..... 107

Storage Management..... 109
Storage Components..... 109
Capacity Management..... 111
Capacity Reservation Best Practices..... 112
Cluster Resilient Capacity..... 112
Configuring a Warning Threshold for Resilient Capacity..... 113
Rebuild Capacity Reservation..... 114
Storage Efficiency..... 117
Deduplication..... 117
Compression..... 118
Erasure Coding..... 118
Storage Dashboard..... 124
Storage Overview View..... 125
Storage Diagram View..... 127
Storage Table View..... 131
Modifying a Storage Pool..... 138
Creating a Storage Container..... 138
Modifying a Storage Container..... 142
Replication Factor Configuration..... 143
Increasing the Replication Factor using CLI..... 143
Enabling Replication Factor 1..... 145
Disabling Replication Factor 1..... 146
Volume Group Configuration..... 146
Concurrent Access from Multiple Clients..... 147
Creating a Volume Group..... 147
Modifying or Deleting a Volume Group..... 149
Cloning a Volume Group..... 150
Flash Mode for Virtual Machines, Disks, and Volume Groups..... 150
Removing Flash Mode for Virtual Disks of a Volume Group..... 152
Recycle Bin..... 152
Recycle Bin Limitations and Considerations..... 153
Enabling and Disabling the Recycle Bin..... 153

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1853

Viewing Space Used by the Recycle Bin..... 154
Clearing Storage Space Used by the Recycle Bin..... 154

Network Management..... 156
Network Configuration for Cluster..... 156
Creating or Updating a Virtual Switch..... 157
Deleting a Virtual Switch..... 160
Migrating Bridges after Upgrade..... 161
MAC Address Prefix..... 164
Network Configuration for VM Interfaces..... 167
Configuring a Virtual Network for Guest VM Interfaces..... 167
Network Segmentation..... 172
Configuring Network Switch Information..... 172
Enabling LACP and LAG (AHV Only)..... 174
Creating SNMP Profiles..... 176
Modifying Switch Information..... 177
Network Visualization..... 178
Prerequisites..... 178
Network Visualizer..... 178
Viewing the Network Visualizer..... 179
Customizing the Topology View..... 180
Viewing VM Information..... 181
Viewing Host Information..... 183
Viewing Switch Information..... 185

Hardware Management..... 187
Hardware Dashboard..... 187
Hardware Overview View..... 188
Hardware Diagram View..... 188
Hardware Table View..... 194
Expanding a Cluster..... 201
Prerequisites and Requirements..... 206
Expand a Cluster with Flow Virtual Networking Enabled..... 211
Node Maintenance..... 219
Node Maintenance Mode..... 219
Viewing a Node that is in Maintenance Mode..... 223
Guest VM Status when Node is in Maintenance Mode..... 223
Repair Host Boot Disk and SSD Repair..... 224
Starting Host Boot Disk Repair..... 225
Modifying a Cluster..... 225
Adding a Disk..... 225
Removing a Disk..... 227
Removing a Node from a Cluster..... 227
Adding a Node..... 232
Compute-Only and Storage-Only Nodes Management..... 232
Compute-Only Nodes..... 232
Storage-Only Nodes..... 233
Deployment Specifications and Considerations for Compute-Only and Storage-Only Nodes..... 234
Deployment of Compute-Only Nodes..... 243
Deployment of Storage-only Nodes..... 245
Optimized Database Solution..... 245
Operation Specifications for Optimized Database Solution..... 246
Cluster Requirements for Optimized Database Solution..... 247
Licensing Requirements for Optimized Database Solution..... 249

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1854

Configuration and Operation Limits for Optimized Database Solution....249
Supported Hardware Platforms for Optimized Database Solution....250
Networking Configurations for Compute-Only Nodes in Optimized Database Solution....250
Deployment of Compute-Only and Storage-Only nodes in Optimized Database Solution....251

Nutanix Volumes....253

File Server Management....254

Data Protection....255

Health Monitoring....256
Health Dashboard....256
Configuring Health Checks....259
Configuring NCC Frequency....260
Running Checks by Using Prism Element Web Console....261
Collecting Logs by Using Prism Element Web Console....261

Virtual Machine Management....264
VM Dashboard....264
VM Overview View....265
VM Table View....266
VM Management....274
Creating a VM (AHV)....274
Managing a VM (AHV)....279
Virtual Machine Snapshots....285
Adding Multiple vGPUs to the Same VM....286
Migrating Live a vGPU-enabled VM Within the Cluster....287
VM Management through Prism Element (ESXi)....288
Creating a VM (ESXi)....289
Managing a VM (ESXi)....291
Configuring Images....295
Virtual Machine Customization....297
Customizing Linux Virtual Machines with Cloud-Init....297
Customization of Windows Virtual Machines with System Preparation....302
VM High Availability in Acropolis....304
Enabling High Availability for the Cluster....305
Nutanix Guest Tools....306
Enabling NGT and Mounting the NGT Installer in a VM....306
NGT Installation....307
Manage Bulk Operations for NGT....312
Enabling NGT and Mounting the NGT Installer on Cloned VMs....319
Automatic Regeneration of NGT Certificates....320
Upgrading NGT....321
Reconfiguring NGT....321
Uninstalling and Removing Nutanix Guest Tools....322
NGT Metrics Collection for Windows Performance Monitor....324
VM-Host Affinity Policies Defined in Prism Element....328
Configuring Legacy VM-VM Anti-Affinity Policy....328
Connect to Citrix Cloud....330
Connecting to the Citrix Cloud....330

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1855

Guest VM Cluster Configuration (AHV Only)....332
Creating a Guest VM Cluster by Directly Attaching a Volume Group (AHV Only)....332

Performance Monitoring....334
Analysis Dashboard....334
Creating an Entity Chart....336
Creating a Metric Chart....337
Chart Metrics....337
Exporting Performance Data....346

Alerts and Events....348

View Task Status....349
View Task Status Dashboard....350

System Management....352
Configuring a Filesystem Whitelist....352
Configuring Name Servers....353
Cluster Time Synchronization....353
Recommendations for Time Synchronization....353
Configuring NTP Servers....354
Configuring an SMTP Server....355
Configuring SNMP....355
Nutanix MIB....359
Configuring a Banner Page....365
Registering a Cluster to vCenter Server....366
Unregistering a Cluster from the vCenter Server....367
Managing vCenter Server Registration Changes....367
In-Place Hypervisor Conversion....368
Requirements and Limitations for In-Place Hypervisor Conversion....369
In-Place Hypervisor Conversion Process....372
Converting Cluster (ESXi to AHV)....372
Converting Cluster (AHV to ESXi)....373
Stopping Cluster Conversion....374
Internationalization (i18n)....375
Localization (L10n)....375
Changing the Language Settings....376
Hyper-V Setup....376
Adding the Cluster and Hosts to a Domain....376
Creating a Failover Cluster for Hyper-V....377
Manually Creating a Failover Cluster (SCVMM User Interface)....378
Enabling Kerberos for Hyper-V....380

Security and User Management....383

Support Services....384
Pulse Health Monitoring....384
Pulse Configuration....386
Mask Entity Names and IP Addresses....387
Pulse Health Monitoring Data Collection....387

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1856

Remote Support Connections....393
Configuring Remote Connection Using CLI....393
Controlling Remote Connections....393
Configuring HTTP Proxy....394
Accessing the Nutanix Support Portal....395
Nutanix REST API....397
Accessing the REST API Explorer....397
Determining Compatibility Between Hardware and Supported Products....398

Help Resources....399
Accessing Online Help....399
Accessing the Nutanix Next Community....400
Glossary....400

Copyright....401

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1857

HELP ORGANIZATION

This documentation is organized as follows:

- Nutanix Platform Overview on page 9 describes the Nutanix architecture.
- Cluster Management on page 53 describes how to access and use the Prism Element web console, how to apply a Nutanix cluster license, how to upgrade the cluster to a later AOS release, and how to upgrade other software components such as disk firmware.
- Multi-Cluster Management on page 93 describes how to install a VM that runs an application called *Prism Central* and how to use *Prism Central* to monitor and manage multiple clusters.
- Storage Management on page 109 describes how to monitor storage use in a Nutanix cluster and how to create storage containers.
- Hardware Management on page 187 describes how to monitor hardware configurations in a Nutanix cluster and how to expand the cluster.
- Health Monitoring on page 256 describes how to monitor the health of VMs, hosts, and disks across a Nutanix cluster.
- Virtual Machine Management on page 264 describes how to monitor status of the VMs across a Nutanix cluster.
- Performance Monitoring on page 334 describes how to monitor and analyze performance in a Nutanix cluster.
- System Management on page 352 describes how to configure various system settings such as for SNMP, NTP, and SMTP.
- Security and User Management on page 383 describes how to configure various security settings including authentication method, SSL certificates, and SSH keys. It also describes how to add, edit, and delete user accounts.
- Support Services on page 384 describes how to enable (or disable) Nutanix technical support access to your cluster, how to access the Nutanix support portal, and how to access the Nutanix REST API explorer.

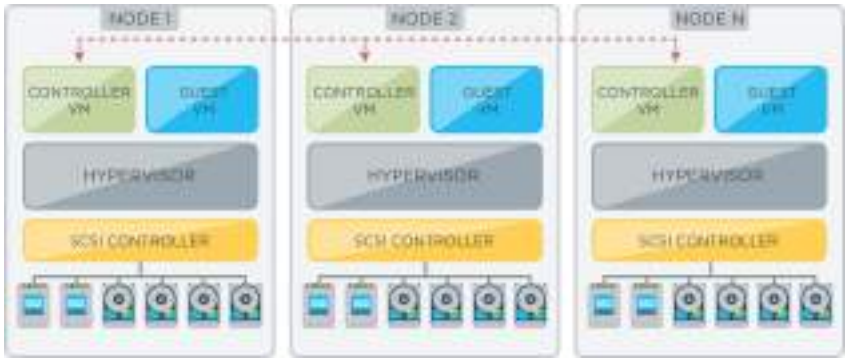
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1858

NUTANIX PLATFORM OVERVIEW

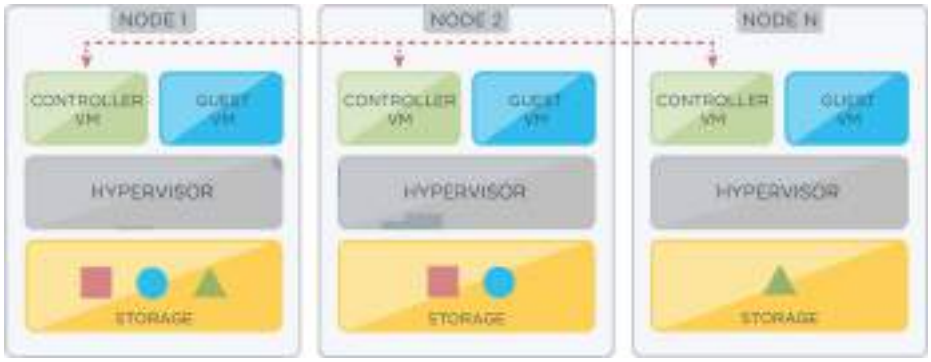
The Nutanix Enterprise Cloud Platform is a converged, scale-out compute and storage system that is purpose-built to host and store virtual machines. All nodes in a Nutanix cluster converge to deliver a unified pool of tiered storage and present resources to VMs for seamless access. A global data system architecture integrates each new node into the cluster, allowing you to scale the solution to meet the needs of your infrastructure.

The foundational unit for the cluster is a Nutanix node. Each node in the cluster runs a standard hypervisor and contains processors, memory, and local storage (SSDs and hard disks).

A Nutanix Controller VM runs on each node, enabling the pooling of local storage from all nodes in the cluster.



Guest VM Data Management



Hosts read and write data in shared Nutanix datastores as if they were connected to a SAN. From the perspective of a hypervisor host, the only difference is the improved performance that results from data not traveling across a network. VM data is stored locally, and replicated on other nodes for protection against hardware failure.

When a guest VM submits a write request through the hypervisor, that request is sent to the Controller VM on the host. To provide a rapid response to the guest VM, this data is first stored on the metadata drive, within a subset of storage called the oplog. This cache is rapidly distributed across the 10 GbE network to other metadata drives in the cluster. Oplog data is periodically transferred to persistent storage within the cluster. Data is written locally for performance and replicated on multiple nodes for high availability.

When the guest VM sends a read request through the hypervisor, the Controller VM reads from the local copy first, if present. If the host does not contain a local copy, then the Controller VM reads across the network from a host that does contain a copy. As remote data is accessed, the remote data is migrated to storage devices on the current host, so that future read requests can be local.

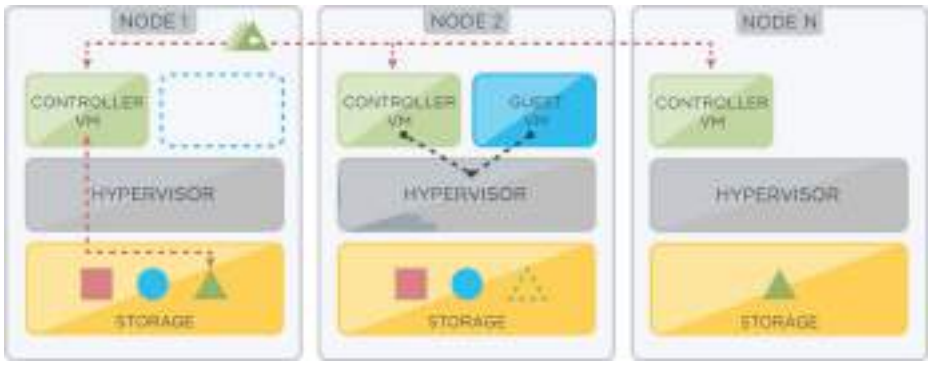
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1859

MapReduce Tiering

The Nutanix cluster dynamically manages data based on how frequently it is accessed. When possible, new data is saved on the SSD tier. Frequently-accessed, or *hot* data is kept on this tier, while *cold* data is migrated to the HDD tier. Data that is accessed frequently is again moved back to the SSD tier.

This automated data migration also applies to read requests across the network. If a guest VM repeatedly accesses a block of data on a remote host, the local controller VM migrates that data to the SSD tier of the local host. This migration not only reduces network latency, but also ensures that frequently-accessed data is stored on the fastest storage tier.

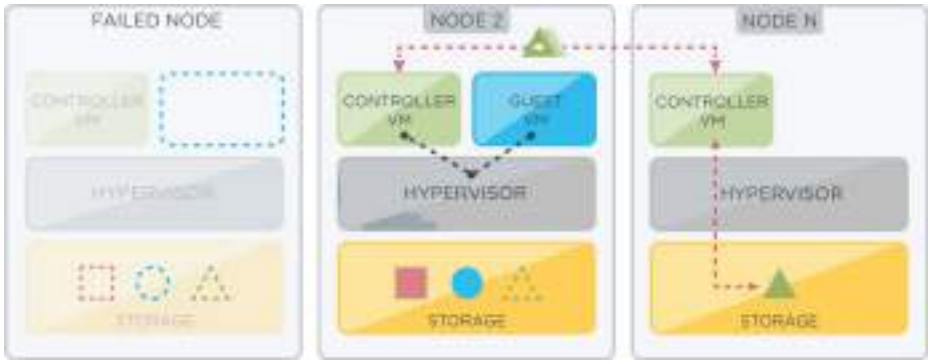
Live Migration



Live migration of VMs, whether it is initiated manually or through an automatic process like vSphere DRS, is fully supported by the Nutanix Enterprise Cloud Computing Platform. All hosts within the cluster have visibility into shared Nutanix datastores through the Controller VMs. Guest VM data is written locally, and is also replicated on other nodes for high availability.

If a VM is migrated to another host, future read requests are sent to a local copy of the data, if it exists. Otherwise, the request is sent across the network to a host that does contain the requested data. As remote data is accessed, the remote data is migrated to storage devices on the current host, so that future read requests can be local.

High Availability



The built-in data redundancy in a Nutanix cluster supports high availability provided by the hypervisor. If a node fails, all HA-protected VMs can be automatically restarted on other nodes in the cluster. The hypervisor management system, such as vCenter, selects a new host for the VMs, which may or may not contain a copy of the VM data.

If the data is stored on a node other than the VM's new host, then read requests are sent across the network. As remote data is accessed, the remote data is migrated to storage devices on the current host, so that future read requests can be local. Write requests is sent to the local storage, and also replicated on a different host. During this interaction, the Nutanix software also creates new copies of pre-existing data, to protect against future node or disk failures.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1860

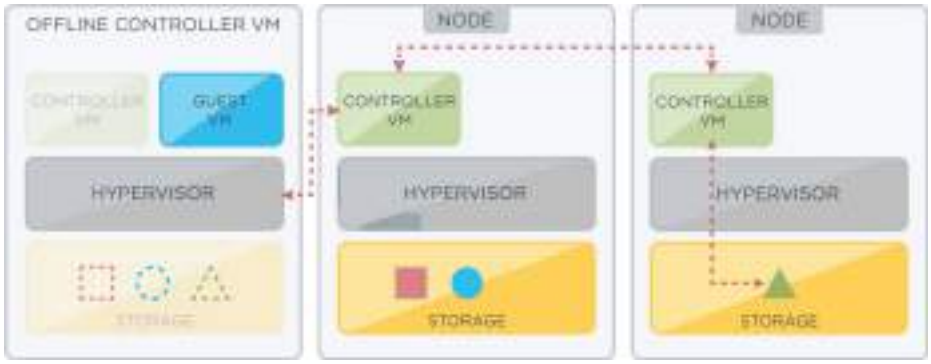
Virtualization Management VM High Availability

In virtualization management VM high availability, when a node becomes unavailable, VMs that are running on that node are restarted on another node in the same cluster.

Typically, an entity failure is detected by its isolation from the network (the failure to respond to heartbeats). Virtualization management ensures that at most one instance of the VM is running at any point during a failover. This property prevents concurrent network and storage I/O that could lead to corruption.

Virtualization management VM high availability may implement admission control to ensure that in case of node failure, the rest of the cluster has enough resources to accommodate the VMs.

Data Path Redundancy



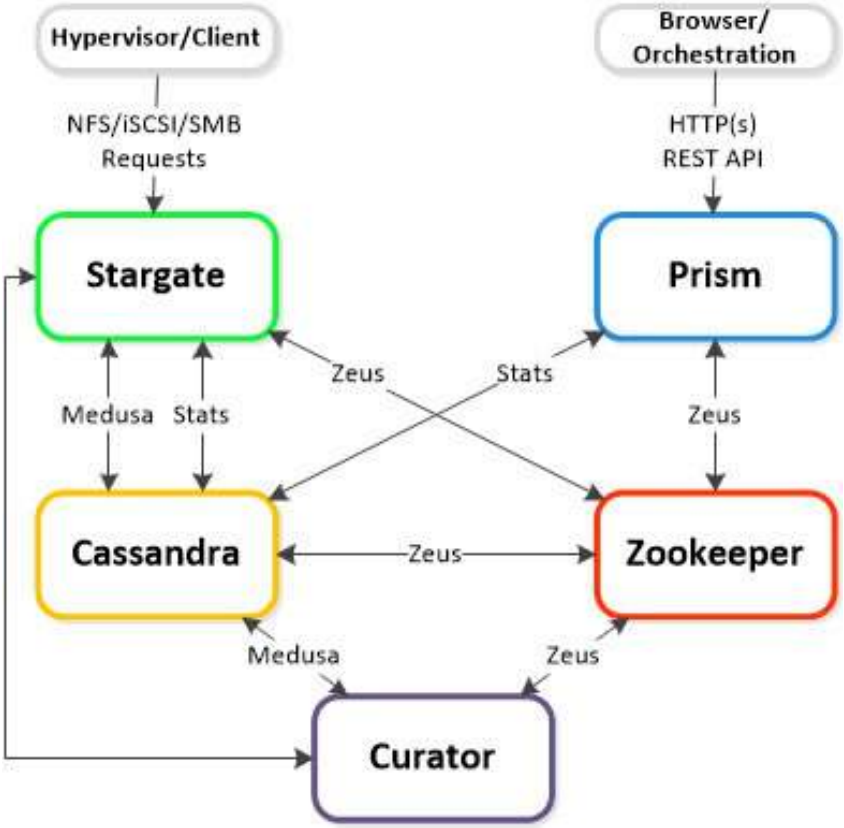
The Nutanix cluster automatically selects the optimal path between a hypervisor host and its guest VM data. The Controller VM has multiple redundant paths available, which makes the cluster more resilient to failures.

When available, the optimal path is through the local Controller VM to local storage devices. In some situations, the data is not available on local storage, such as when a guest VM was recently migrated to another host. In those cases, the Controller VM directs the read request across the network to storage on another host through the Controller VM of that host.

Data Path Redundancy also responds when a local Controller VM is unavailable. To maintain the storage path, the cluster automatically redirects the host to another Controller VM. When the local Controller VM comes back online, the data path is returned to this VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1861

Cluster Components



The Nutanix cluster has a distributed architecture, which means that each node in the cluster shares in the management of cluster resources and responsibilities. Within each node, there are software components that perform specific tasks during cluster operation.

All components run on multiple nodes in the cluster, and depend on connectivity between their peers that also run the component. Most components also depend on other components for information.

Zeus

A key element of a distributed system is a method for all nodes to store and update the cluster's configuration. This configuration includes details about the physical components in the cluster, such as hosts and disks, and logical components, like storage containers. The state of these components, including their IP addresses, capacities, and data replication rules, are also stored in the cluster configuration.

Zeus is the Nutanix library that all other components use to access the cluster configuration, which is currently implemented using Apache Zookeeper.

Zookeeper

Zookeeper runs on either three or five nodes, depending on the cluster fault tolerance that is applied to the cluster. Using multiple nodes prevents stale data from being returned to other components, while having an odd number provides a method for breaking ties if two nodes have different information.

Of these three nodes, one Zookeeper node is elected as the leader. The leader receives all requests for information and confers with the two follower nodes. If the leader stops responding, a new leader is elected automatically.

Zookeeper has no dependencies, meaning that it can start without any other cluster components running.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1862

Medusa

Distributed systems that store data for other systems (for example, a hypervisor that hosts virtual machines) must have a way to keep track of where that data is. In the case of a Nutanix cluster, it is also important to track where the replicas of that data is stored.

Medusa is a Nutanix abstraction layer that sits in front of the database that holds this metadata. The database is distributed across all nodes in the cluster, using a modified form of Apache Cassandra.

Cassandra

Cassandra is a distributed, high-performance, scalable database that stores all metadata about the guest VM data stored in a Nutanix datastore. In the case of NFS datastores, Cassandra also holds small files saved in the datastore. When a file reaches 512K in size, the cluster creates a vDisk to hold the data.

Cassandra runs on all nodes of the cluster. These nodes communicate with each other once a second using the Gossip protocol, ensuring that the state of the database is current on all nodes.

Cassandra depends on Zeus to gather information about the cluster configuration.

Stargate

A distributed system that presents storage to other systems (such as a hypervisor) needs a unified component for receiving and processing data that it receives. The Nutanix cluster has a large software component called Stargate that manages this responsibility.

From the perspective of the hypervisor, Stargate is the main point of contact for the Nutanix cluster. All read and write requests are sent across vSwitchNutanix to the Stargate process running on that node.

Stargate depends on Medusa to gather metadata and Zeus to gather cluster configuration data.

> **Tip:** If Stargate cannot reach Medusa, the log files include an HTTP timeout. Zeus communication issues can include a Zookeeper timeout.

Curator

In a distributed system, it is important to have a component that watches over the entire process. Otherwise, metadata that points to unused blocks of data could pile up, or data could become unbalanced, either across nodes, or across disk tiers.

In the Nutanix cluster, each node runs a Curator process that handles these responsibilities. A Curator master node periodically scans the metadata database and identifies cleanup and optimization tasks that Stargate or other components should perform. Analyzing the metadata is shared across other Curator nodes, using a MapReduce algorithm.

Curator depends on Zeus to learn which nodes are available, and Medusa to gather metadata. Based on that analysis, it sends commands to Stargate.

Prism

A distributed system is worthless if users can't access it. Prism provides a management gateway for administrators to configure and monitor the Nutanix cluster. This includes the nCLI and Prism Element web console.

Prism runs on every node in the cluster, and like some other components, it elects a leader. All requests are forwarded from followers to the leader using Linux iptables. This allows administrators to access Prism using any Controller VM IP address. If the Prism leader fails, a new leader is elected.

Prism communicates with Zeus for cluster configuration data and Cassandra for statistics to present to the user. It also communicates with the ESXi hosts for VM status and related information.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1863

Single-node Clusters

A traditional Nutanix cluster requires a minimum of three nodes, but Nutanix also offers the option of a two-node cluster and single-node cluster for ROBO implementations and other situations that require a lower cost option. Unlike a two-node-node cluster that provides many of the resiliency features of a three-node cluster, a single-node cluster provides lowered resiliency protections.

A single-node cluster is capable of running a limited number of user VMs. These are unlike single-node replication targets which are for replication and backup purposes.

The following table outlines features and limitations of a single-node cluster.

> **Note:** Single-node clusters are supported only on a limited set of hardware models. For more information, see Prerequisites and Requirements on page 15.

Table 1: Single-node Cluster Features

Requirements and Limitations	Description
Controller VM minimum requirements	6 vCPU and 20 GB memory
Replication factor	Replication factor 2 across drives within the same node. Replication factor 1 containers are optional. For more information about replication factor 1 containers, see Replication Factor 1 on page 42.
Hypervisors supported	AHV and ESXi
Network segmentation	You can segment the network on a single-node cluster by using Prism Element. Network segmentation for disaster recovery is supported on single-node clusters with AOS version 5.19.2 or later. Network segmentation for Backplane, Volumes, RDMA, and iSER is not supported on single-node clusters. For more information about network segmentation, see Securing Traffic Through Network Segmentation in the *Security Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1864

Requirements and Limitations	Description
Unsupported features	• Cluster expansion. For more information, see Expanding a Cluster on page 201. • Deduplication. For more information, see Deduplication on page 117. • Erasure coding. For more information, see Erasure Coding on page 118. • Volumes. For more information, see Volumes Guide. • NearSync DR and Metro Availability (asynchronous DR is supported). For more information, see Data Protection with Asynchronous Replication (One-hour or Greater RPO) and Metro Availability (ESXi and Hyper-V 2016) in *Data Protection and recovery with Prism Element*. • Capacity analysis (in Prism) • Rebuild capacity reservation. For more information, see Rebuild Capacity Reservation on page 114.

Prerequisites and Requirements

A single-node cluster is configured like a regular (three-node or more) cluster in many ways, but note the following for a single-node cluster:

- Single-node clusters are supported only on a select set of hardware models. For information about supported models, see KB 5943.
- As a best practice, Nutanix recommends configuring a maximum of five guest VMs. Ensure that the cluster platform has the minimal physical resources to cater to the compute and disk requirements. Also, ensure that the CVM resources are optimally consumed.

  Nutanix also recommends configuring backup for all the five guest VMs running on a single-node cluster to protect the guest VMs in a node failure scenario.

  > **Important:** Failing to configure backup for guest VMs may result in data loss as data cannot be recovered from a single-node cluster. The data loss can be observed when there is any meta-data inconsistency or file system corruption.

- Nutanix recommends that you schedule an appropriate maintenance window (downtime) for your single node clusters when you plan to perform any network configurations or changes thereto.
- Do not exceed a maximum of 1000 IOPS.
- Do not create a Prism Central instance (VM) in the cluster. There is no built-in resiliency for Prism Central in a single-node cluster, which means that a problem with the node takes out Prism Central with limited options to recover.
- LCM is supported for software updates, but not for firmware updates.
- Async DR is supported for 6 hour RPO only.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1865

- Use external DNS and NTP servers. Nutanix recommends that you host the DNS and NTP servers on a different cluster.
- Ensure that there is more than 1 SSD available for the system to place meta-data. In case of a Hybrid or All-Flash HCI node with 2 SSDs, if an SSD fails, the cluster goes into a read-only state as there is only one remaining SSD for the meta-data purpose.

  In the read-only mode, there are no create, read, update, or delete operations and no cluster changes. For more information about the read-only state, see Read-Only Mode on page 16. If the cluster experiences an unresponsive disk, data resilience is a risk. The Prism Central console offers an override option that allows users to continue writing to single-node clusters after it has entered read-only mode. For more information, see Overriding Read-Only Mode on page 17.

  > **Important:** In case of a Hybrid HCI node or All-Flash HCI node with more than 2 SSDs, if a disk (SSD or HDD) fails, the cluster can fill up and write IO fails if there is insufficient rebuild capacity and the other disks do not have enough available space to bring up the data to disk fault tolerance. For more information, see Resilient Capacity in *Nutanix Bible.*

- All user VMs must be shut down before upgrading a single-node cluster. If any user VMs are still running, a warning box appears.

  > **Important:** A graceful shutdown of the guest VM may not power-off the VM immediately. Based on the operating system in the guest VM and the workloads running on it, the VM could take sometime to get powered off. Therefore, wait for sometime and check if the VM is in the powered off state.

Read-Only Mode

Single-node clusters enter read-only mode when certain requirements are not met or a disk fails. An alert *A1195* is generated. For more information, see KB 8156. A yellow exclamation mark is displayed in the web console that indicates the single-node cluster has entered read-only mode.

A single node cluster can comprise either a Hybrid or All-Flash HCI Node.

The following table describes the disk failure scenarios in which a cluster enters into read-only mode:

Table 2: Read-Only Mode - Scenarios

HCI Node Type in Cluster	Failure Type	Impact on the single node cluster	Nutanix Recommendations
Hybrid with 2 SSDs All-Flash with 2 SSDs	1 SSD fails	The cluster becomes read-only as there is only 1 SSD remaining to store the meta-data.	Ensure that there is more than 1 SSD available for the system to place meta-data.
All-Flash with more than 2 SSDs	1 SSD fails	The meta-data attempts to pick another SSD in the node and get the node out of read-only state. **Note:** A read-only state exists for a brief period until the meta-data is able to pick the new SSD for its usage.	None

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1866

Overriding Read-Only Mode

About this task

This section describes how to override the read-only mode. The override operation allows the users to continue writing to single-node clusters after it has entered read-only mode. For more information about read-only mode, see Read-Only Mode on page 16.

Procedure

To override read-only mode from Prism Element web console, perform the following steps:

1. Click the yellow exclamation mark to re-enable write mode on the cluster.

Figure 1: Re-enable Write Mode Message

The system prompts you to confirm if you want to override read-only mode.

2. Click **Override** to confirm.

Note:

- To override read-only mode from nCLI, perform the following steps:
  1. Log into the cluster using your Nutanix credentials.
  2. Run the following command:

     ```
     nutanix@cvm$ ncli cluster set-operation-mode operation-mode=override
     ```

- An alert *A101057 - Cluster In Override Mode* is generated by the system. For more information, see KB-8132.

Two-Node Clusters

A traditional Nutanix cluster requires a minimum of three nodes, but Nutanix also offers the option of a two-node cluster for ROBO implementations and other situations that require a lower cost yet high resiliency option. Unlike a one-node cluster, a two-node cluster can still provide many of the resiliency features of a three-node cluster. This is possible by adding an external Witness VM in a separate failure domain to the configuration. For more information, see Configuring a Witness (Two-node Cluster) in the *Data Protection and Recovery with Prism Element* guide. Nevertheless, there are some restrictions when employing a two-node cluster. The following table outlines the features and limitations of a two-node cluster.

Note: Two-node clusters are supported only on a limited set of hardware models.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1867

Table 3: Two-Node Cluster Features

Feature	Description
Controller VM minimum requirements	6 vCPU and 20 GB memory
Replication factor	Replication factor 2 spanned over two nodes and Replication factor 4 for metadata on SSDs over two nodes. Replication factor 4 for metadata helps during a node failure scenario to quickly transition the healthy node to run in single-node mode with the metadata remaining disk fault tolerant. (Metadata in a two-node cluster is typically small, so the storage need for four copies is modest.) Replication factor 1 containers are optional. For more information about replication factor 1 containers, see Replication Factor 1 on page 42.
Single node failure effects	50% resource loss. Plan for 40% maximum disk and memory usage to avoid read-only state on the remaining node. Data is made replication factor 2 in the background so that data is resilient.
Drive failure effects	One node + one SSD failure (on other node) = read-only mode.
Hypervisors supported	AHV and ESXi
Unsupported features	• Cluster expansion • Deduplication (compression is supported) • Erasure coding • Nearsync DR and metro availability (asynchronous DR is supported) • Network segmentation

Two-Node Cluster Guidelines

A two-node cluster is configured and upgraded like a regular (three-node or more) cluster in most ways, but note the following for a two-node cluster:

- The IPv6 configuration is not supported for a two-node cluster.
- Two-node clusters are supported only on a select set of hardware models. For information about supported models, see KB 5943.
- Size your implementation for N + 1 so that in the event of a node loss (50% loss of resources) the remaining node will have sufficient resources to allow the cluster to continue functioning.
- There is a heartbeat check (ping) between the nodes every two seconds. If a successful ping does not occur within 10 seconds (5 consecutive failed tries), a failover is initiated. For more information, see Failure and Recovery Scenarios on page 20. When the cluster recovers, it must remain in healthy status for at least 15 minutes before it will failback.
- The upgrade process in a two-node cluster may take longer than the usual process because of the additional step of syncing data while transitioning between single and two node state. Nevertheless, the cluster remains operational during upgrade.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1868

- Use external DNS and NTP servers. Nutanix recommends that you host the DNS and NTP servers on a different cluster.
- Witness VM considerations
  - A Witness VM for two-node clusters requires a minimum of 2 vCPUs, 6 GBs of memory, and 25 GBs of storage.
  - The same Witness VM can be used for both Metro Availability and two-node clusters, and a single Witness VM can support up to 50 instances (any combination of two-node clusters and Metro Availability protection domains).
  - You can bring up a two-node cluster without a Witness VM being present initially, but it is recommended that the Witness VM be alive and running before starting the cluster.
  - The Witness VM may reside on any supported hypervisor, and it can run on either Nutanix or non-Nutanix hardware.

    Note: Nutanix does not support the deployment of a Witness VM on the AWS and Azure cloud platforms.
  - The Witness VM must reside in a separate failure domain, which means independent power and network connections from any cluster it is managing. This separate platform can be deployed either on premise (including as an option the Nutanix one-node replication target NX-1155) or off premise (centrally, typically where Prism Central is hosted).
  - During a node failure, the transition of a healthy node to single-node mode can take 30-60 seconds. The client VMs can experience I/O timeouts during this period. Therefore, it is recommended that the SCSI timeout of the client VM disks should be at least 60 seconds.
  - The minimum recovery point objective (RPO) for a two-node (or one-node) cluster is six hours.
  - Network latency between a two-node cluster and the Witness VM should not exceed 500 ms. (RPC timeouts are triggered if the network latency is higher.) During a failure scenario, nodes keep trying to reach (ping) the Witness VM until successful. Nodes ping the Witness VM every 60 seconds, and each Witness request has a two-second timeout, so it can tolerate up to one second of link latency.
  - Node removal is not supported, but node replacement is supported (where the node remains part of the cluster). When replacing a node, the cluster remains active but will transition to standalone mode for a brief period of time.
  - All node maintenance work flows (software upgrades, life cycle manager procedures, node and disk break-fix procedures, boot drive break-fix procedure) require that the cluster be registered with a Witness VM.
- Node or disk failures are handled as follows:
  - Node failure: When a two-node cluster is operating normally, data is replicated across the nodes. If a node fails, data is replicated across disks on the healthy node to maintain resiliency.
  - HDD failure: An HDD failure is handled in the same way as in a three-node cluster, that is data is rebuilt in the background. If there is insufficient rebuild capacity when an HDD fails, the cluster can fill up and I/O can fail.
  - SSD failure: If a node loses an SSD, the remedial action is the same as for an HDD failure, that is the cluster remains normal and data is rebuilt in the background for the disk. Occasionally, an SSD failure on one node can result in the other node in the cluster transitioning to a standalone state because the SSD failure caused a critical storage service to restart, which caused user I/O to stall. If the nodes have only a single SSD left and if either node fails, the healthy node goes into read-only state.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1869

Witness for Two-node Clusters

A two-node cluster requires a Witness VM that is located in a separate failure domain either off premise or in a different physical platform on premise. For information about how to configure a witness for a two-node cluster, see Witness Option in the *Data Protection and Recovery with Prism Element* guide.

The Witness option provides a dashboard of status information about all the registered two-node clusters. (The two-node view appears only in a 5.6 or later version of the Witness.) For information about Witness dashboard for a two-node cluster, see Witness VM Dashboard (Two-node Cluster) in the *Data Protection and Recovery with Prism Element* guide.

Failure and Recovery Scenarios

There are several potential failure scenarios between the nodes and the Witness VM. The steps for recovering from a failure depend on the nature of the failure. This section describes the steps needed (or not needed) when a failure occurs. Each failure scenario generates one or more alerts that you can review. For information about viewing alert messages, see Alerts Dashboard in *Prism Element Alerts and Events Reference Guide*.

Node Failure

When a node goes down, the live node sends a leadership request to the Witness VM and goes into single-node mode. In this mode replication factor 2 is still retained at the disk level, meaning data is copied to two disks. (Normally, replication factor 2 is maintained at the node level normally meaning data is copied to each node.) If one of the two metadata SSDs fails while in single-node mode, the cluster (node) goes into read-only mode until a new SSD is picked for metadata service. When the node that was down is back up and stable again, the system automatically returns to the previous state (replication factor 2 at the node level). No user intervention is necessary during this transition.

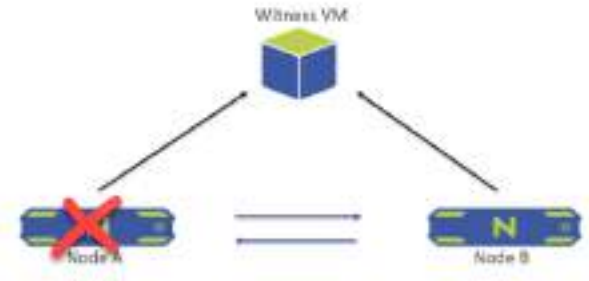


Figure 2: Failure Diagram: Node Down

Network Failure Between The Nodes

When the network connection between the nodes fails, both nodes send a leadership request to the Witness VM. Whichever node gets the leadership lock stays active and goes into single-node mode. All operations and services on the other node are shut down, and the node goes into a waiting state. When the connection is re-established, the same recovery process as in the node failure scenario begins.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1870

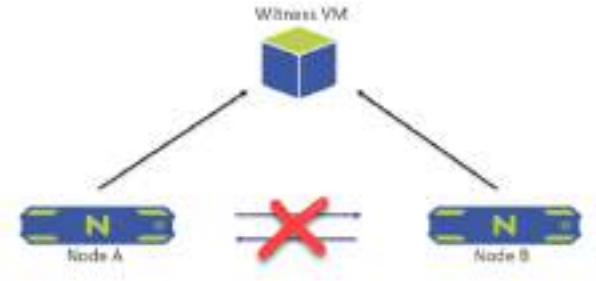


Figure 3: Failure Diagram: Node-to-Node Communication Down

Network Failure Between Node and Witness VM

When the network connection between a single node (Node A in this example) and the Witness fails, an alert is generated that Node A is not able to reach the Witness. The cluster is otherwise unaffected, and no administrator intervention is required.

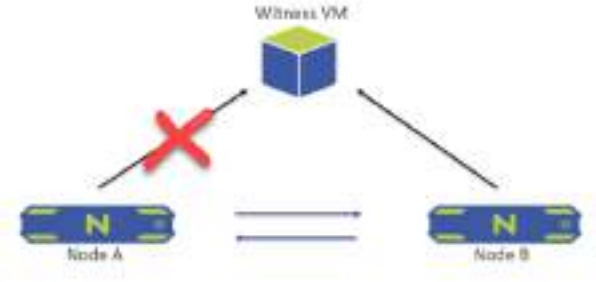


Figure 4: Failure Diagram: Node-to-Witness Communication Down

Witness VM Failure

When the Witness goes down (or the network connections to both nodes and the Witness fail), an alert is generated but the cluster is otherwise unaffected. When connection to the Witness is re-established, the Witness process resumes automatically. No administrator intervention is required.

If the Witness VM goes down permanently (unrecoverable), follow the steps for configuring a new Witness through the **Configure Witness** option of the Prism Element web console. Fore more information, see Configuring a Witness (Two-node Cluster) in the *Data Protection and Recovery with Prism Element* guide.

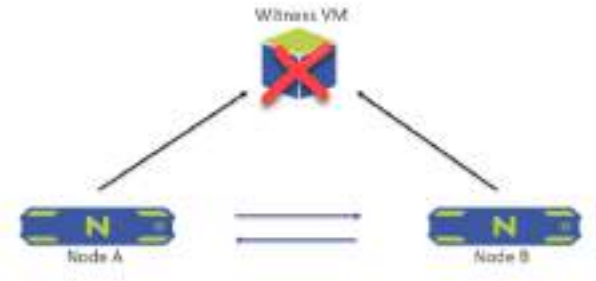


Figure 5: Failure Diagram: Witness Down

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1871

Cluster Resiliency

Nutanix AOS provides cluster resilience capability to protect your clusters from failures.

To ensure that a cluster can remain resilient during a failure, ensure that the cluster has enough free memory and vCPU capacity available for critical workloads to fail over to another node.

Failure Handling in a Nutanix Cluster

Hardware failures are a part of any datacenter lifecycle. The Nutanix architecture was designed with this inevitability in mind.

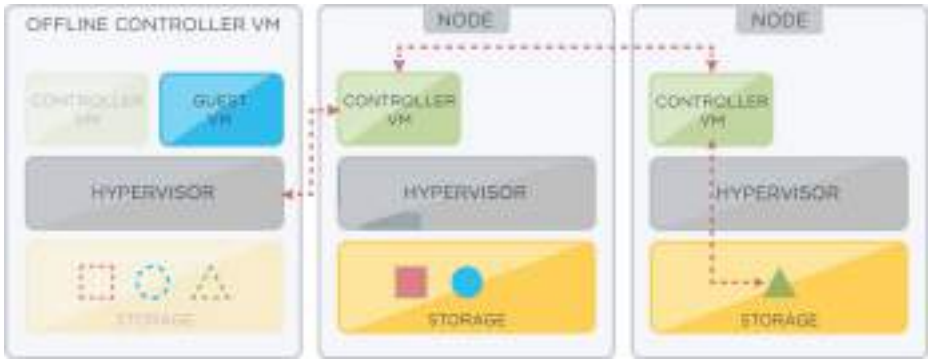
Depending on the fault tolerance of the cluster and the replication factor of the containers in the cluster, a cluster can tolerate one or two failures of a variety of hardware components while still running guest VMs and responding to commands through the management console. Many of these failures also trigger an alert through that same management console to give the administrator a chance to respond to the situation.

Nutanix provides the ability to tolerate rack failures for extended data availability, in addition to drive, node, block, and network link failure.

Node Failure

A Nutanix node is comprised of a physical host and a Controller VM. Either component can fail without impacting the rest of the cluster.

Controller VM Failure



The Nutanix cluster monitors the status of Controller VMs in the cluster. If any Stargate process fails to respond two or more times in a 30-second period, another Controller VM redirects the storage path on the related host to another Stargate. Reads and writes occur over the 10 GbE network until the missing Stargate comes back online.

To prevent constant switching between Stargates, the data path is not restored until the original Stargate has been stable for 30 seconds.

A CVM failure may include a user powering down the CVM, a CVM rolling upgrade, or any event, which might bring down the CVM. In any of these cases the storage traffic is served by another CVM in the cluster. The hypervisor and CVM communicate using a private network on a dedicated virtual switch. This means that the entire storage traffic is routed through an internal IP address on the CVM. The external IP address of the CVM is used for remote replication and for CVM to CVM communication.

In the event of a local CVM failure, the local addresses previously used by the local CVM become unavailable. In this case, the NDFS automatically detects the outage and redirects the storage traffic to another CVM in the cluster over the network. The re-routing is done transparently to the hypervisor and to the VMs running on the host. This indicates that even if a CVM is powered-off, the VMs continue to perform the I/O operations. The Nutanix Distributed File System (NDFS) is also self-healing, which means that NDFS detects when a CVM is powered-off and it automatically reboots the local CVM. Once the local CVM is available, the traffic is seamlessly transferred back to be served by the local CVM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1872

The NDFS uses replication factor and checksum to ensure data redundancy and availability in the case of a node or disk failure or corruption. In the case of a node or disk failure the data is then re-replicated among all nodes in the cluster to maintain the replication factor, which is called re-protection. Re-protection may result after a CVM is down.

What Will Users Notice?

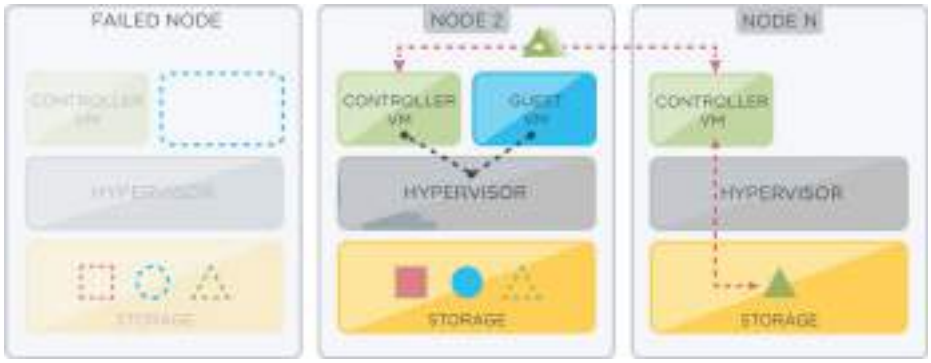
During the switching process, the host with a failed Controller VM may report that the shared storage is unavailable. Guest VMs on this host appear to *hang* until the storage path is restored. Although the primary copy of the guest VM data is unavailable because it is stored on disks mapped to the failed Controller VM, the replicas of that data are still accessible.

As soon as the redirection takes place, VMs can resume reads and writes. Performance may decrease slightly, because the IO is traveling across the network, rather than across the internal network. Because all traffic goes across the 10 GbE network, most workloads do not diminish in a way that is perceivable to users.

What Happens If Another One Fails?

A second Controller VM failure has the same impact on the VMs on the other host, which means there will be two hosts sending IO requests across the network. More importantly, however, is the additional risk to guest VM data. With two Controller VMs unavailable, there are now two sets of physical disks that are inaccessible. In a cluster with a replication factor 2, there is now a chance that some VM data extents are missing completely, at least until one of the Controller VMs resumes operation.

Host Failure



The built-in data redundancy in a Nutanix cluster supports high availability provided by the hypervisor. If a node fails, all HA-protected VMs can be automatically restarted on other nodes in the cluster.

Curator and Stargate responds to two issues that arise from the host failure. First, when the guest VM begins reading across the network, Stargate begins migrating those extents to the new host. This improves performance for the guest VM. Second, Curator notices that there is a missing replica of those extents, and instruct Stargate to begin creating a second replica.

What Will Users Notice?

Users who are accessing HA-protected VMs will notice that their VM is unavailable while it is restarted on the new host. Without HA, the VM will need to be manually restarted.

What Happens If Another One Fails?

Depending on how fully loaded the cluster is, a second host failure could leave the remaining hosts with insufficient processing power to restart the VMs from the second host. However, even in a lightly-loaded cluster, the bigger concern is additional risk to guest VM data. With two sets of physical disks that are inaccessible, there would be a chance that some VM data extents are missing completely and the IO requests are not served.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1873

Drive Failures

Drives in a Nutanix node store four primary types of data: persistent data (hot-tier and cold-tier), storage metadata, oplog, and Controller VM boot files. Cold-tier persistent data is stored in the hard-disk drives of the node. Storage metadata, oplog, hot-tier persistent data, and Controller VM boot files are kept in the SATA-SSD in drive bay one. SSDs in a dual SSD system are used for storage metadata, oplog, hot-tier persistent data according to the replication factor of system and in a RAID-1 configuration for CVM files. In all-flash nodes, data of all types is stored in the SATA-SSDs.

> **Note:** On hardware platforms that contain PCIe-SSD drives, the SATA-SSD holds only the Controller VM boot files. Storage metadata, oplog, and hot-tier persistent data reside on the PCIe-SSD.

Boot Drive Failure

Each Controller VM boots from a SATA-SSD. During cluster operation, this drive also holds component logs and related files.

A boot drive failure eventually causes the Controller VM to fail. The host does not access the boot drive directly, so other guest VMs can continue to run. Data Path Redundancy redirects the storage path to another Controller VM. For more information, see Controller VM Failure on page 22.

> **Note:** The Controller VM might restart under certain rare conditions on dual SSD nodes if a boot drive fails, or if you unmount a boot drive without marking the drive for removal and the data has not successfully migrated.

Metadata Drive Failure

The metadata *drive* (metadata spans multiple drives) serves many purposes. It holds the oplog for each host, which provides a fast response to VMs that send write requests. It is used as a persistent data tier. It is also used by the Cassandra database to provide fast read and write responses for cluster metadata. To protect against potential failure, the metadata is replicated to metadata drives in other hosts in the cluster.

Metadata is shared, and Cassandra uses up to four SSDs to store metadata. If any metadata drive fails on a host, the Controller VM restarts. Once the Cassandra process restarts, the missing metadata is retrieved from the other Controller VMs and sharded across the remaining metadata drives. When the faulty drive recovers or is replaced, metadata is stored on that drive again.

If the Cassandra process is down on a node for more than 30 minutes, the surviving Cassandra nodes detach the node from the Cassandra database so that the unavailable metadata can be replicated on other nodes. The process of healing the database takes about 30-40 minutes. If the Cassandra process restarts and remains up for 30 minutes, the procedure to detach the node is canceled if the healing procedure is still running. If the process resumes and is stable after the healing procedure is complete, the node can be manually added to the database using the nCLI command:

```
ncli> host enable-metadata-store id=host_id
```

What Will Users Notice?

Performance may decrease slightly for user VMs on the host due to the reboot and the fact that some I/O is traveling across the network. However, most workloads should not diminish in a way that is perceivable to users (other than during the reboot).

What Happens If Another One Fails?

Multiple drive failures in a single selected domain (node, block, or rack) is tolerated.

Data Drive Failure

Each node contributes data drives to the cluster storage pool. Cold-tier data is stored in HDDs, while hot-tier data is stored in SSDs for faster performance. Because the HDDs have moving parts, and outnumber any other hardware

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1874

component, this is the most likely component to experience a failure. Data is replicated across the cluster, so a single hard-disk drive failure does not result in data loss. In all-flash nodes, data of all types is stored in SSDs.

The cluster software receives a hardware alert from the host that a data drive (HDD or SSD) has failed, and immediately begin working to reduce the impact of a second failure. Curator instructs Stargate to create a second replica of any guest VM data that was stored on the drive.

> **Note:** The Controller VM restarts if a data drive fails, or if you remove a data drive without marking the drive for removal and the data has not successfully migrated.

What Will Users Notice?

For a brief period of time, guest VMs with files on the failed data drive will need to read across the network. Curator will eventually instruct Stargate to migrate the relevant data to another drive on the current host.

What Happens If Another One Fails?

In a cluster with a replication factor 2, losing two drives on different domains (node, block, or rack) means that some VM data extents could lose both replicas. Although a single drive failure does not have the same impact as a host failure, it is important to replace the failed drive as soon as possible.

Network Link Failure

The physical network adapters on each host are grouped together on the external network. This grouping of network adapters enables load balancing and failover capabilities, thus improving the performance and redundancy of the system.

In case of a network link failure, the network traffic fails over to the secondary link. This failover behavior is different for AHV and ESXi hypervisors, based on their NIC teaming and failover configuration.

For more information about hypervisor specific network link failure, see:

- Networking recommendations for ESXi
- Networking recommendations for AHV

Cluster Fault Tolerance

Cluster fault tolerance is the number of simultaneous disk or node failures a cluster can withstand within the configured fault domain while maintaining operational resilience.

Following are the types of cluster fault tolerance supported in a Nutanix cluster:

- One Node or One Disk (1N/1D)
- One Node and One Disk (1N&1D)
- Two Nodes or Two Disks (2N/2D)

Minimum Requirements

The following table lists the minimum number of nodes and replication factor required to configure the respective cluster fault tolerance.

Cluster Fault Tolerance	Replication Factor	Minimum Number of Nodes
1N/1D	2	3
1N&1D	3	3
2N/2D	3	5

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1875

One Node or One Disk Cluster Fault Tolerance

A cluster with one node or one disk (1N/1D) cluster fault tolerance can withstand the failure of either one node or one disk within the fault domain of a node, and remain resilient.

To configure 1N/1D fault tolerance, a cluster must have a minimum of three nodes to store the minimum required metadata copies to maintain resiliency and data integrity.

By default, the storage containers in a cluster with 1N/1D fault tolerance are configured with a replication factor of 2, distributing two data copies across two distinct nodes. This ensures that, in the event of a node or disk failure, at least two metadata copies remain accessible to sustain cluster operations, while at least one copy of the container data is preserved.

When you enable rack or block awareness in the cluster, the system aims to distribute three copies of metadata and two copies of container data across nodes within the configured fault domains of rack or block. This ensures that, in the event of a rack or block failure, the system retains the minimum required number of metadata and data copies across the fault domains to maintain operations.

> **Note:** If the system cannot distribute metadata and data copies across the rack or block due to node unavailability, it places the data copies on different nodes within the same fault domain.

In the event of a node or disk failure, the system automatically rebuilds the lost data on a healthy node or disk, restoring resiliency and self-healing the cluster. Therefore, when sizing the system, Nutanix recommends that you consider the spare capacity required for rebuilding operations. The spare capacity required for a cluster with 1N/1D fault tolerance is equal to the capacity of the largest node in the cluster. For more information on usable capacity, see Storage Overheads and Usable Capacity on page 28.

For information on how to configure cluster fault tolerance, see Cluster Fault Tolerance Configuration on page 76.

For information on how to increase the existing 1N/1D cluster fault tolerance of a cluster, see Increasing the Cluster Fault Tolerance Level on page 76.

One Node and One Disk Cluster Fault Tolerance

A cluster configured with one node and one disk (1N&1D) cluster fault tolerance can withstand the simultaneous failure of one node and one disk in another node, or the failure of two disks across different fault domains, and remain resilient.

To configure 1N&1D fault tolerance, a cluster must have a minimum of three nodes. A cluster with 1N&1D fault tolerance maintains three copies of metadata, locally mirrored across three different nodes, ensuring data integrity. This configuration guarantees that, in the event of a node or disk failure, enough metadata copies remain available to sustain cluster operations.

By default, storage containers in a cluster with 1N&1D fault tolerance are configured with a replication factor of 3, with three copies of data distributed across three different nodes. A Write operation is considered complete only after at least three copies of the data are successfully written. This ensures that in case of failure of a node and disk at least one copy of data remains accessible.

> **Note:** You can modify the replication factor of the storage containers to 2. However, with replication factor 2, these containers can only tolerate the failure of a single node or disk within the fault domains. Therefore, Nutanix recommends that you configure replication factor 3 for the storage containers to attain optimal cluster resiliency.

When you enable rack or block awareness, the system attempts to distribute metadata and container data across unique nodes within the configured fault domains. This ensures that, in the event of a rack or block failure, the system retains the minimum required copies of metadata and data across the fault domains to maintain operations.

> **Note:** If the system is unable to place metadata and data copies on nodes within the same rack or block due to unavailability, it places the copies on other nodes within the same configured fault domain.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1876

Adaptive Replication Factor 3

Clusters configured with 1N&1D fault tolerance utilize an adaptive mechanism to maintain operations during node downtime, whether caused by a node failure or node maintenance. During such events, the system temporarily reduces the replication factor of the containers to 2, storing only two copies of the data and marking the Write operation as complete. This ensures that the cluster can continue functioning with two active nodes. When the node is restored, the system automatically upgrades the containers to a replication factor of 3. The system also regenerates the third copy of any data written with only two copies during the downtime, fully restoring fault tolerance and data redundancy.

The cluster maintains sufficient copies of data to ensure continuous operation and service I/O even in the event of multiple failures, balancing resiliency with the overhead required for self-healing. In a steady state, the cluster maintains enough copies of data and metadata to withstand the simultaneous failure of one node and one disk. In a degraded state, when a failure has already occurred, the cluster prioritizes application availability over restoring full data resiliency.

In the event of a node failure, the system does not immediately initiate a rebuild of the data on the failed node. This ensures that the system can continue to operate, even if there is no spare capacity available for rebuilding the node, and sustain operations during the failure. In the event of a disk failure, the system rebuilds the data from the failed disk to restore resiliency and facilitate self-healing. This ensures that the system can maintain the ability to recover from disk failures, which are more likely to occur. Therefore, when sizing the system, Nutanix recommends that you consider spare capacity for rebuilding operations to account for a disk failure on a node. The spare capacity required for a cluster with 1N/1D fault tolerance is equal to the total capacity of the largest disk on every node. For more information on usable capacity, see Storage Overheads and Usable Capacity on page 28.

For information on how to configure 1N&1D cluster fault tolerance, see Cluster Fault Tolerance Configuration on page 76.

Limitations

The following limitations apply when you configure 1N&1D fault tolerance in your cluster:

- You cannot configure 1N&1D cluster fault tolerance on clusters running Hyper-V.
- You cannot increase the fault tolerance of a cluster from 1N/1D to 1N&1D; 1N&1D cluster fault tolerance must be configured when you create the cluster.
- You cannot configure 1N&1D cluster fault tolerance on clusters deployed in Nutanix Cloud Clusters (NC2) environments.
- You cannot enable erasure coding or deduplication on clusters with 1N&1D cluster fault tolerance.
- You cannot deploy compute-only or storage-only nodes on clusters with 1N&1D cluster fault tolerance.

Two Nodes or Two Disks Cluster Fault Tolerance

A cluster configured with two nodes or two disks (2N/2D) cluster fault tolerance can withstand the simultaneous failure of either two nodes or two disks within a fault domain of a node, and remain resilient.

To configure 2N/2D fault tolerance, a cluster must have a minimum of five nodes to store the minimum required metadata copies to maintain resiliency and data integrity. By default, storage containers in a cluster with 2N/2D fault tolerance are configured with a replication factor of 3, with three copies of data distributed across three different nodes.

> **Note:** You can modify the replication factor of the storage containers to 2. However, with a replication factor of 2, these containers can only tolerate the failure of a single node or disk within the fault domains. Therefore, Nutanix recommends that you configure replication factor 3 for the storage containers to attain optimal cluster resiliency.

When you enable rack or block awareness in the cluster, the system aims to distribute five copies of metadata and three copies of container data across nodes within the configured fault domains. This ensures that, in the event of a

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1877

rack or block failure, the system retains the minimum required number of metadata and data copies across the fault domains to maintain operations.

> **Note:** If the system cannot distribute metadata and data copies across the rack or block due to node unavailability, it places the data copies on different nodes within the same fault domain.

In the event of a failure, the system automatically rebuilds the lost data on a healthy node or disk, restoring resiliency and self-healing the cluster. Therefore, when sizing the system, Nutanix recommends that you consider spare capacity for rebuilding operations. The spare capacity for a cluster with 2N/2D fault tolerance is equal to the capacity of the two largest nodes in the cluster. For more information on usable capacity, see Storage Overheads and Usable Capacity on page 28.

For information on how to configure cluster fault tolerance, see Cluster Fault Tolerance Configuration on page 76.

Storage Overheads and Usable Capacity

The usable storage container capacity is the actual amount of storage space available for use within a storage container after accounting for overheads like system metadata, resiliency overheads (additional copies of data written for redundancy), and spare capacity for rebuilding the data during failures and planned maintenance. It is the effective capacity that users can access and use to store their data.

The following table shows the overheads associated with the different types of cluster fault tolerance.

Table 4: Cluster Fault Tolerance and Overheads

Cluster Fault Tolerance	Resiliency Overhead	Spare Capacity Overhead	Other System Overheads
1N/1D	1x	The capacity of the largest node in the cluster.	All flash: ~10% of raw capacity Hybrid: ~15% of raw capacity
1N&1D	2x	Total capacity of the largest disk on every node.	
2N/2D	2x	Total capacity of the two largest nodes in the cluster.	

x = Total size of application data written in the system.

The following table shows the total overheads (including resiliency overhead, spare capacity overhead, and other system overheads) based on the different types of cluster fault tolerance and the number of nodes.

> **Note:** The total overhead shown in the table is calculated assuming that the cluster is an all-flash configuration with uniform nodes, each containing 12 disks.

Table 5: Total Overhead Comparison Based On Cluster Fault Tolerance

Number of Nodes	Total Overhead (includes resiliency overhead, spare capacity overhead, and other system overheads)		
	1N/1D	1N&1D	2N/2D
3	3x	3.09x	NA

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1878

Number of Nodes	Total Overhead (includes resiliency overhead, spare capacity overhead, and other system overheads)		
	1N/1D	1N&1D	2N/2D
4	2.67x	NA	NA
5	2.50x	NA	5x
6	2.40x	NA	4.5x
7	2.33x	NA	4.2x
8	2.29x	NA	4x
9	2.25x	NA	3.86x
10	2.22x	NA	3.75x

x = Total size of application data written in the system.

The following table displays the approximate usable storage container capacity available based on the different types of cluster fault tolerance and the number of nodes.

> **Note:** The usable capacity shown in the table is calculated assuming that the cluster is an all-flash configuration with uniform nodes, each containing 12 disks.

Table 6: Usable Capacity Comparison Based On Cluster Fault Tolerance and Replication Factor

Number of Nodes	Usable Capacity		
	1N/1D	1N&1D	2N/2D
3	30%	29%	NA
4	34%	NA	NA
5	36%	NA	18%
6	38%	NA	20%
7	39%	NA	21%
8	39%	NA	23%
9	40%	NA	23%
10	41%	NA	24%

Fault Domains in a Nutanix Cluster

Also known as fault tolerance level and defined as the entity such as a node, block or rack, the failure of which the cluster can tolerate while still running guest VMs and responding to commands through the management console.

You can configure failure domain as a node in the cluster, a block, or a rack.

- Configuring Node Fault Tolerance on page 30
- Block Fault Tolerance on page 30
- Rack Fault Tolerance on page 35

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1879

Configuring Node Fault Tolerance

About this task

To configure node fault tolerance, do the following.

Procedure

1. Log in to the Prism Element web console.
2. Go to **Settings** > **Setup** > **Rack Configuration.**.
3. Select **Node** as the fault tolerance domain, and click **Next**.
4. Optionally, click **Add New Rack** to specify rack and block mapping.
   Nutanix recommends configuring rack and block mapping if you want to enable rack awareness at a later stage.

Block Fault Tolerance

Block fault tolerance lets a Nutanix cluster make redundant copies of data and metadata and place the copies on nodes in different blocks.

A *block* is a rack-mountable enclosure that contains one to four Nutanix nodes. All nodes in a block share power supplies, front control panels (ears), backplane, and fans.

Nutanix offers block fault tolerance as an opt-in procedure or a best-effort procedure. The opt-in block fault tolerance feature offers guaranteed data resiliency when required conditions are met. For more information, see Configuring Block Fault Tolerance on page 30. For best-effort fault tolerance mode, data copies remain on the same block when there is insufficient space across all blocks. For more information, see Block Fault Tolerance in Best Effort mode on page 30.

With block fault tolerance enabled, guest VMs can continue to run after a block failure because redundant copies of guest VM data and metadata exist on other blocks.

Configuring Block Fault Tolerance

About this task

To configure block fault tolerance, do the following.

Procedure

1. Log in to the Prism Element web console.
2. Go to **Settings** > **Setup** > **Rack Configuration.**.
3. Select **Block** as the fault tolerance domain, and click **Next**.
4. Optionally, click **Add New Rack** to specify rack and block mapping.

Block Fault Tolerance in Best Effort mode

When certain conditions are met, Nutanix clusters become block fault tolerant. Block fault tolerance is applied automatically when:

- Every storage tier in the cluster contains at least one drive on each block.
- Every storage container in the cluster has replication factor of at least two.
- For replication factor 2, there are a minimum of three blocks in the cluster.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1880

- There is enough free space in all the tiers, in at least replication factor number of blocks in the cluster. For example, if the replication factor of storage containers in the cluster is two, then at least two blocks require free space.
- A minimum of four blocks for replication factor 2 or six blocks for replication factor 3 is required to maintain block awareness if erasure coding is enabled on any storage container. (If the cluster has fewer blocks, block awareness is lost when erasure coding is enabled.)

> **Note:** This is not applicable for single-node replication target clusters. For more information about how single-node replication target clusters handle failures, see Single-Node Replication Target Clusters in the *Data Protection and Recovery with Prism Element* guide.
>
> Once block fault tolerance conditions are met, the cluster can tolerate a specific number of block failures:
>
> - A replication factor two or replication factor three cluster with three or more blocks can tolerate a maximum failure of one block.
> - A replication factor three cluster with five or more blocks can tolerate a maximum failure of two blocks.

Block fault tolerance is one part of a resiliency strategy. It does not remove other constraints such as the availability of disk space and CPU/memory resources in situations where a significant proportion of the infrastructure is unavailable.

Metadata Block Awareness Requirements for Block Fault Tolerance

Metadata block awareness is required for block fault tolerance. Metadata block awareness can be enabled for replication factor 2 and replication factor 3. To enable metadata block fault tolerance, your metadata must meet the following requirements.

Table 7: Minimum Cluster Requirements

Replication Factor	Minimum Number of Blocks and Nodes Per Block Required
Replication factor 2	• 3 blocks • 1 node per block
Replication factor 3	• 5 blocks • 1 node per block

Table 8: Additional Requirements when Adding Nodes to an Existing Block Aware Cluster

Replication Factor	Requirement	Example
Note: Be sure your cluster has met the previous minimum cluster requirements.		

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1881

Replication Factor	Requirement	Example
Replication factor 2	There must be at least 3 blocks populated with a specific number of nodes to maintain block fault tolerance. To calculate the number of nodes required to maintain block fault tolerance when the cluster replication factor is 2, you need twice the number of nodes in the remaining blocks as there are in the block with the most or maximum number of nodes.	If a block contains 4 nodes, you need 8 nodes distributed across the remaining (non-failing) blocks to maintain block fault tolerance for that cluster. X = number of nodes in the block with the most nodes. In this case, 4 nodes in a block. 2X = 8 nodes in the remaining blocks.
Replication factor 3	There must be at least 5 blocks populated with a specific number of nodes to maintain block fault tolerance. To calculate the number of nodes required to maintain block fault tolerance when the cluster replication factor 3 you need four times the number of nodes in the remaining blocks as there are in the block with the most or maximum number of nodes.	If a block contains 4 nodes, you need 16 nodes distributed across the remaining (non-failing) blocks to maintain block fault tolerance for that cluster. X = number of nodes in the block with the most nodes. In this case, 4 nodes in a block. 4X = 16 nodes in the remaining blocks

Block Fault Tolerant Data Placement

Stargate is responsible for placing data across blocks, and Curator makes data placement requests to Stargate to maintain block fault tolerance.

New and existing clusters can reach a block fault tolerant state. New clusters can be block fault tolerant immediately after being created if the configuration supports it. Existing clusters that were not previously block fault tolerant can be made tolerant by reconfiguring the cluster in a manner that supports block fault tolerance.

New data in a block fault tolerant cluster is placed to maintain block fault tolerance. Existing data that was not in a block fault tolerant state is moved and scanned by Curator to a block fault tolerant state.

Depending on the volume of data that needs to be relocated, it might take Curator several scans over a period of hours to distribute data across the blocks.

Block fault tolerant data placement is on a commercially reasonable effort but is not guaranteed. Conditions such as high disk usage between blocks may prevent the cluster from placing guest VM redundant copy data on other blocks.

Guest VM Data

Redundant copies of guest VM data are written to nodes in blocks other than the block that contains the node where the VM is running. The cluster keeps two copies of each write stored in the oplog.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1882

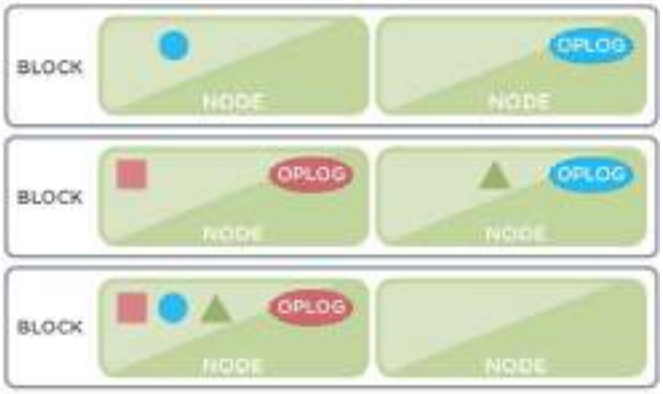
Redundant copies of the guest VM data (designated by) are placed on different blocks. 

Figure 6: Block-aware placement of guest VM data

In the case of a block failure, the under-replicated guest VM data is copied to other blocks in the cluster, and one copy of the oplog contents is available.

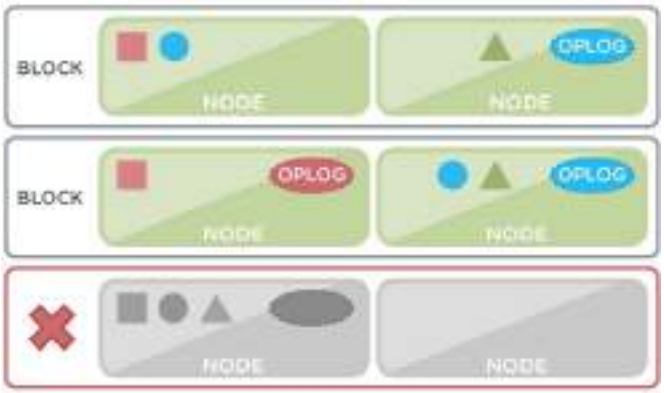


Figure 7: Block-aware placement of guest VM data with block failure

Metadata

The Nutanix Medusa component uses Cassandra to store metadata. Cassandra uses a ring-like structure where data is copied to peers within the ring to ensure data consistency and availability. The cluster keeps at least three redundant copies of the metadata, at least half of which must be available to ensure consistency.

With block fault tolerance, the Cassandra peers are distributed among the blocks to ensure that no two peers are on the same block. In the event of a block failure, at least two copies of the metadata is present in the cluster.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1883

Figure 8: Block-aware placement of metadata

Configuration Data

The Nutanix Zeus component uses Zookeeper to store essential configuration data for the cluster. The Zookeeper role is distributed across blocks to ensure availability in the case of a block failure.

Figure 9: Block-aware placement of configuration data

Data Resiliency Levels for Block Fault Tolerance

The following table shows the level of data resiliency (simultaneous failure) provided for the following combinations of replication factor, minimum number of nodes, and minimum number of blocks.

Table 9: Data Resiliency Levels

Replication Factor	Minimum Number of Nodes	Minimum Number of Blocks	Data Resiliency
2	3	1	1 node or 1 disk failure
2	3	3 (minimum 1 node each)	1 block or 1 node or 1 disk failure
3	5	2	2 nodes or 2 disk failures
3	5	5 (minimum 1 node each)	2 blocks or 2 nodes or 2 disks

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1884

Replication Factor	Minimum Number of Nodes	Minimum Number of Blocks	Data Resiliency
3	6	3 (minimum 2 nodes each)	1 block or 2 nodes or 2 disks
Metro Cluster (For more information, see Metro Availability (ESXi and Hyper-V 2016) in the *Data Protection and Recovery with Prism Element* guide.)	3 nodes at each site	2	1 cluster failure

The state of block fault tolerance is available for viewing through the Prism Element web console and Nutanix CLI. Although administrators must set up the storage tiers or storage containers, they cannot determine where data is migrated. AOS determines where data is migrated.

Prism Element web console	**Cluster Resiliency / Fault Tolerance Status** widget on the **Home** screen
nCLI	`ncli> cluster get-domain-fault-tolerance-status type="rackable_unit"`

Rack Fault Tolerance

Rack fault tolerance is the ability to provide rack level availability domain. With rack fault tolerance, redundant copies of data are made and placed on the nodes that are not in the same rack.

Rack failure can occur in the following situations:

- All power supplies fail within a rack
- Top-of-rack (TOR) switch fails
- Network partition; where one of the racks becomes inaccessible from other racks

When rack fault tolerance is enabled, the cluster has rack awareness and the guest VMs can continue to run with failure of one rack (replication factor 2) or two racks (replication factor 3). The redundant copies of guest VM data and metadata exist on other racks when one rack fails.

Note:

- If sufficient number of working racks are not present after failure, the data is rebuilt in a non-rack-aware manner to get node fault-tolerance level to one. The rack-fault-tolerance stays 0.
- Rack Fault Tolerance is supported for AHV, ESXi, and HyperV.

  Note: – Prism Central workflows are not applicable for rack fault tolerance using HyperV since HyperV support is not available for Prism Central

Configuring Rack Fault Tolerance

About this task

To enable rack fault tolerance, you must specify the mapping of the blocks to the racks based on the actual placement of the blocks in the datacenter.

To configure rack fault tolerance, do the following.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1885

Before you begin

- You must have information on the actual physical mapping of racks and blocks in the datacenter.
- Minimum cluster requirements:
  - Replication factor 2 - 3 racks (4 with Erasure Coding)
  - Replication factor 3 - 5 racks (6, with Erasure Coding), 1 node in each rack
- Network Latency Limit - The round trip latency for communication between Controller VMs in a Nutanix cluster should be less than or equal to 1 ms (millisecond).

Procedure

1. Log in to the Prism Element web console.
2. Go to **Settings** > **Setup** > **Rack Configuration.**.

   Note: Directory List (AD and OpenLDAP) users can view and configure Rack Awareness only if a service account is configured for the directory service. For more information about how to configure a service account for the directory service, see Configuring Authentication in the *Security Guide*.
3. Select **Rack** as the fault tolerance domain, and click **Next**.
4. Click **+ Add New Rack**, and enter the name of the rack in the **Rack Name** field.
5. Click **Add Blocks** to assign the discovered blocks to the rack.
6. Click **+** to add the block to the rack based on the actual placement of the block in the datacenter, and click **Done**.

   Repeat steps 4 through 6 for adding more rack configurations. Verify the configuration and click **Save**.

   Note:

   - Once rack fault tolerance is enabled; create, edit, delete operations are not allowed. To make any new modifications, you must re-configure the fault tolerance level as **Node**. For more information, see Configuring Node Fault Tolerance on page 30.
   - Enabling rack fault tolerance may trigger Cassandra ring change operations and trigger curator scans to redistribute replicas for rack fault tolerance. The time taken for these depend on existing data on cluster, workload on the cluster, and configurations.

   The **Cluster Resiliency / Fault Tolerance Status** widget on the Prism dashboard shows the current state of the fault tolerance.

   Note:

   The fault tolerance has Four states.

   - **OK**: This state indicates that the fault tolerance domain is highly resilient to safely handle a node or a disk (in single or two node clusters) failure.
   - **Warning**: This state indicates that the fault tolerance level is almost reaching to 0. Warning state is displayed if the cluster is not fault tolerant at the configured domain, but is fault tolerant at a lower domain. For example, if you have configured rack as the configured domain and the cluster can no

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1886

longer handle any rack failures due to some reason but can still handle node (lower domain) failures, then fault tolerance state is displayed as Warning.

- **Critical**: This state indicates that the fault tolerance level is 0, and the fault tolerance domain cannot handle a node or a disk (in single or two node clusters) failure.
- **Computing**: This state indicates that the new fault tolerance level is being calculated. This state is displayed soon after a node or disk failure, before rebuild is initiated.

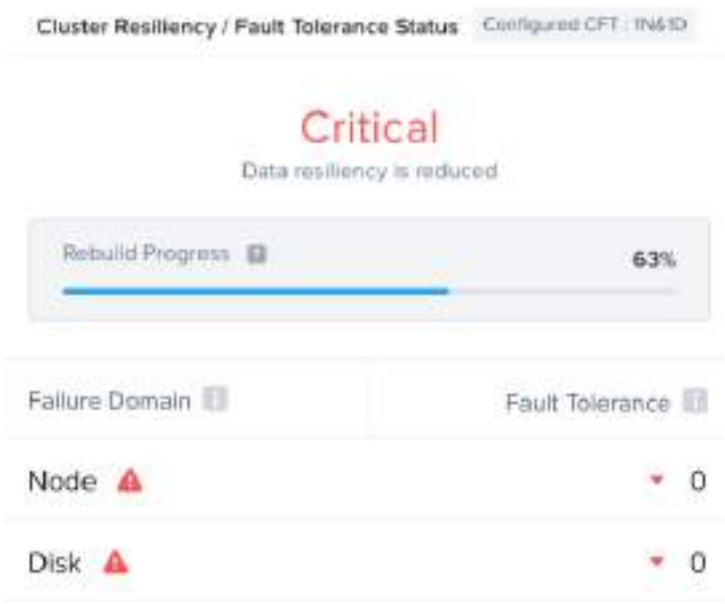


Figure 10: Cluster Resiliency/Fault Tolerance Status widget

Rack Awareness Metadata Requirements for Rack Fault Tolerance

Nutanix stores essential metadata in a ring-like structure to provide data resiliency. Replication of metadata to all the nodes of a rack-aware configuration occurs in the form of a ring to ensure data consistency and availability. With this metadata placement, in the event of a rack failure, a minimum two copies of data are available as a backup.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1887

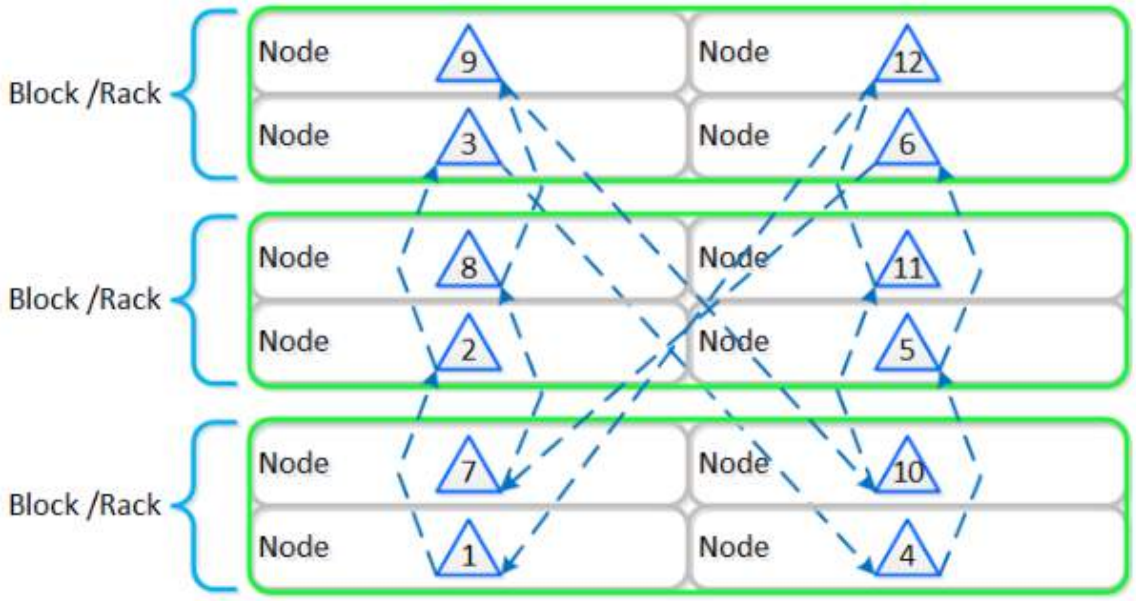


Figure 11: Node replication topology to form a ring-like structure in a rack-aware cluster

Nutanix uses a data resiliency factor also known as replication factor to ensure data redundancy and availability, which is based upon the cluster fault tolerance (1N/1D, 1N&1D, and 2N/2D). The following table provides the metadata and data replication factor values for the corresponding FT level:

Cluster Fault Tolerance Level	Metadata Replication Factor	Data Replication Factor
1N/1D	3	2
1N&1D	3	3
2N/2D	5	3

Rack Awareness Metadata Placement Requirements

Before you add nodes to or remove or move nodes from a rack-aware cluster, you must achieve rack-awareness resiliency by following the metadata placement requirements.

Use the following criteria to calculate the rack-aware metadata placement:

- Minimum number of metadata RF rack domains required:

  Metadata RF = (FT x 2) + 1

  where RF is replication factor and FT is fault tolerance
- Total number of nodes required in a cluster:

  Nodes # N x Metadata RF

  where N is the maximum number of nodes in a rack domain

Example:

If a cluster has 1N/1D and 4 maximum nodes in a rack domain:

Minimum number of metadata RF rack domains required:

Metadata RF = (1 x 2) + 1 = 3

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1888

Total number of nodes required in a cluster:

Nodes = 4 x 3 = 12

Rack-aware resiliency is achieved from 3 racks and 12 nodes.

Data Resiliency Levels for Rack Fault Tolerance

This topic provides information about the level of data resiliency (simultaneous failure) provided for various combinations of replication factor, minimum number of disks, minimum number of nodes, minimum number of blocks, and minimum number of racks when Erasure Coding (EC) is disabled/enabled in the containers.

Table 10: Data Resiliency Levels with EC disabled

Fault Domain	Replication Factor	Minimum number of Disks	Minimum Number of Nodes	Minimum Number of Blocks	Minimum Number of Racks	Data Resiliency
Disk	1*	1	1	1	1	None
	2	2	1	1	1	1 disk failure
Node	2	Not applicable	3	1	1	1 node or 1 disk failure
	3	Not applicable	5	2	1	2 nodes or 2 disk failures
Block	2	Not applicable	3	3	1	1 node or 1 block or 1 disk failure
	3	Not applicable	5	5	1	2 nodes or 2 blocks or 2 disk failures
Rack	2	Not applicable	3	3	3	1 node or 1 block or 1 rack or 1 disk failure
	3	Not applicable	5	5	5	2 nodes or 2 blocks or 2 racks or 2 disk failures

* Before using replication factor 1, see KB-11291 for replication factor 1 guidelines and limitations.

Table 11: Data Resiliency Levels with EC enabled

Fault Domain	Replication Factor	Minimum Number of Nodes	Minimum Number of Blocks	Minimum Number of Racks	Data Resiliency
Node	2	4*	1	1	1 node or 1 disk failure

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1889

Fault Domain	Replication Factor	Minimum Number of Nodes	Minimum Number of Blocks	Minimum Number of Racks	Data Resiliency
	3	6*	2	1	2 nodes or 2 disk failures
Block	2	4	4*	1	1 node or 1 block or 1 disk failure
	3	6	6*	1	2 nodes or 2 blocks or 2 disk failures
Rack	2	4	4	4*	1 node or 1 block or 1 rack or 1 disk
	3	6	6	6*	2 nodes or 2 blocks or 2 racks or 2 disks

* Minimums that are required to enable erasure coding on new containers in rack aware clusters.

Caution: If rack awareness is enabled on a cluster with erasure coding (EC) functionality enabled, the cluster might need to reduce the EC strip size to comply with the new fault tolerance configuration. This leads to an increased usage of space in the cluster temporarily, due to the unpacking of EC strips. After the re-packing of EC strips is complete, some amount of savings will be lost (depending on initial and final EC strip sizes).

For example, an EC enabled 12-node cluster will have the EC strip size as 4/2 (4 data blocks and 2 parity blocks). If rack awareness is enabled on this cluster with 6 racks and 2 nodes in each rack, the EC strip size changes to 2/2 (2 data blocks and 2 parity blocks), leading to lesser savings to accommodate the new fault tolerance configuration.

For more information about EC strip sizes based on cluster size, see the Nutanix Erasure Coding solutions documentation.

Cluster Rebuild Preference

Nutanix AOS provides cluster resilience capability to protect your clusters from failures. You can choose to reserve storage capacity within clusters for use in rebuilding failed disks, nodes, blocks, or racks. For more information, see Rebuild Capacity Reservation on page 114.

The rebuild operation requires additional storage on the cluster and might lead to space bloats during planned maintenance. These space bloats consume the free capacity on a cluster and might impact the cluster operations. For such planned maintenance operations (like software or firmware upgrades), you can set the rebuild preference to *Smart* using Prism Element or Prism Central. When the cluster rebuild preference is set as *Smart*, the system differentiates between the failure and a planned outage during an upgrade. During failure scenarios, the system initiates an immediate rebuild and during planned maintenance, the system optimizes the rebuild behavior to minimize the amount of data moved, rebuilt, and garbage collected.

Note: The *Delayed* cluster rebuild preference setting is deprecated from AOS 6.7 release. If you have the *Delayed* cluster rebuild preference configured in your setup, the system changes it to *Smart*.

Starting with AOS 6.8 release, the cluster rebuild preference is set as *Smart* by default. You can modify the cluster rebuild preference from Prism Element and Prism Central. For information on how to modify the cluster rebuild preference from Prism Element, see Modifying Cluster Rebuild Preference on page 78. For information on

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1890

how to modify the cluster rebuild preference from Prism Central, see Cluster Management in the *Prism Central Infrastructure Guide*.

The following table describes the difference in cluster rebuild operation between *Smart* and *Immediate* preference:

Table 12: Rebuild Preference for Upgrade

Immediate	Smart
During an upgrade or failure, the rebuild process starts almost immediately (approximately 60 seconds) when Stargate of the node being upgraded is down.	During an upgrade, the system identifies the planned outage occurrence as a maintenance activity, and restricts unnecessary component rebuilds that might lead to space bloats on the cluster. However, if the upgrade extends beyond expected time or if any failure occurs in the cluster, the system triggers an immediate rebuild to restore cluster resiliency.

Replication Factor

Replication factor refers to the number of copies of data maintained on a storage container in a cluster.

Nutanix clusters rely on replication factor for data protection and availability. This method provides the highest degree of availability because it does not require reading from multiple storage locations or data recomputation after a failure. However, this advantage comes at the cost of storage resources, as it requires full copies.

Following are the types of replication factor supported in a Nutanix cluster:

- Replication Factor 1 on page 42
- Replication Factor 2 on page 41
- Replication Factor 3 on page 42

For information on how to configure replication factor on a storage container, see Replication Factor Configuration on page 143.

Requirements

The following table lists the replication factor you can configure corresponding to the cluster fault tolerance configured in the cluster and the minimum number of nodes listed for the cluster fault tolerance.

Table 13: Replication Factor Requirements

Replication Factor	Cluster Fault Tolerance	Minimum Number of Nodes
2	1N/1D	3
3	1N&1D	3 (minimum number and maximum number of nodes are the same)
3	2N/2D	5

Replication Factor 2

A replication factor of 2 means that the cluster maintains two copies of the data (the original data and a copy of the original data) for each replication factor 2 enabled storage container.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1891

To configure replication factor 2 in a cluster, the cluster must have a minimum of 3 nodes. For more information, see Requirements on page 41.

For information on how to configure replication factor on a storage container, see Replication Factor Configuration on page 143.

Replication Factor 3

A replication factor of 3 means that the cluster maintains three copies of the data (the original data and two copies of the original data) for each replication factor 3 enabled storage container.

Replication Factor 3 adds an extra layer of data protection at the cost of storing an additional copy of the data. To configure replication factor 3 in a cluster, the cluster must have a minimum of 5 nodes. For more information see Requirements on page 41. Nutanix recommends configuring replication factor 3 at sites with high protection requirements, but this requires more nodes and storage capacity.

For information on how to configure replication factor on a storage container, see Replication Factor Configuration on page 143.

Replication Factor 1

A replication factor of 1 means that the cluster maintains only the original data without any copies.

Nutanix recommends that you only enable replication factor 1 when your cluster is running applications that provide their own data protection or high availability because replication factor 1 does not guarantee data availability if a node or disk failure occurs. When you enable replication factor 1, the cluster maintains a single copy of data for each replication factor 1 enabled storage container. The storage container can contain multiple vDisks you can directly attach to a VM or implement as part of a volume group. Each replication factor 1 enabled storage container is associated with a specific node that you choose. All the data in the replication factor 1 enabled storage container is associated with that node only. For clusters running the ESXi hypervisor, you must associated the storage container with a single host only. Mounting the replication factor 1 enabled storage container on all or multiple hosts is not supported.

Clusters with replication factor 1 enabled storage containers can improve I/O performance for write-intensive applications that do not need storage level data protection. Applications that provide their own data protection and applications that perform at high I/O rates on ephemeral data can benefit from this type of storage. Workloads that can benefit from storing data in an replication factor 1 enabled storage container include artificial intelligence (AI), machine learning (ML), and big data.

For information on how to enable replication factor 1, see Enabling Replication Factor 1 on page 145.

Recommendations

Nutanix recommends the following.

- For each cluster where you want to use replication factor 1, create one replication factor 1 enabled storage container per node. The replication factor 1 enabled storage container can contain multiple replication factor 1 enabled vDisks.
- For clusters running the ESXi hypervisor, make sure you mount the replication factor 1 enabled storage container on a single host only. Mounting the replication factor 1 enabled storage container on all or multiple hosts is not supported.
- Do not enable replication factor 1 storage containers on clusters where SSD tier capacity is less than 6 percent of total cluster capacity.

Limitations

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1892

Table 14: Unsupported Software, Features, and Operations

Nutanix Software	Description
Nutanix Database Service (NDB)	Using a replication factor 1 enabled storage container as part of configuration and deployment is not supported.
Nutanix Files	Using a replication factor 1 enabled storage container as part of configuration and deployment is not supported.
Nutanix Karbon	Using a replication factor 1 enabled storage container as part of configuration and deployment is not supported.
Nutanix Objects	Using a replication factor 1 enabled storage container as part of configuration and deployment is not supported.
Prism Central	Do not deploy Prism Central on replication factor 1 enabled storage containers. This configuration is not supported.
Cluster Hypervisor	**Support or Limitation**
Microsoft Hyper-V	Enabling replication factor 1 on clusters running Microsoft Hyper-V is not supported.
Mixed hypervisor cluster	For VMware ESXi and AHV mixed hypervisor clusters, replication factor 1 enabled storage containers and VMs with attached replication factor 1 enabled vDisks are not supported on the AHV storage-only nodes. You can enable replication factor 1 on the nodes running the VMware ESXi hypervisor.
VMware ESXi	Using vSphere HA with Distributed Resource Scheduler (DRS) is not supported for any VM with at least one replication factor 1 enabled vDisk.
Feature or Operation	**Support or Limitation**
Snapshots and data protection/recovery	For vDisks in replication factor 1 enabled storage containers, disaster recovery operations like snapshots and replication are not supported.
In-place hypervisor conversion	Not supported when converting a cluster from AHV to ESXi.
Deduplication	Not supported for replication factor 1 enabled storage containers.
Erasure coding	Not supported for replication factor 1 enabled storage containers.
Metro availability	Not supported for replication factor 1 enabled storage containers and VMs with attached replication factor 1 enabled vDisks.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1893

Feature or Operation	Support or Limitation
Recycle bin	Not supported. When you delete an replication factor 1 enabled vDisk, the vDisk is marked for deletion as soon as possible and bypasses the recycle bin.
Storage container settings or modification with replication factor 1 enabled	These settings or modifications are not supported. • Increasing the replication factor • Enabling capacity reservation (Reserve Capacity setting) or Reserve Rebuild Capacity • Storage containers with Reserve Capacity or Reserve Rebuild Capacity already enabled
Maintenance mode operations (planned)	The following operations automatically shut down and restart replication factor 1 enabled VMs. • Controller VM shutdown • Memory update • Host boot disk replacement • Nutanix Flow microsegmentation work flows • Request Reboot (rolling reboot operation)
ESXi hypervisor 1-click upgrade	Automatic VM shutdown is not supported. You must manually shut down replication factor 1 enabled VMs before upgrading and restart them after the upgrade is completed.
LCM upgrade operations	The following LCM upgrade operations automatically shut down and restart replication factor 1 enabled VMs. • AOS upgrade • Firmware upgrades for ESXi and AHV clusters • AHV hypervisor upgrade
Upgrade operations, VM with volume group access	• For any VM with a volume group directly attached to the VM (AHV clusters only), the cluster will automatically shut down and power on the VM as part of the upgrade operation. • For any VM with volume group access provided by Nutanix Volumes (that is, connection to the volume group from the VM guest OS through an iSCSI target IP address), you must manually shut down the VM. You can power on the VM when the upgrade operation is completed.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1894

Feature or Operation	Support or Limitation
Unplanned event	These unplanned events might affect I/O operations for VMs with vDisks in replication factor 1 enabled storage containers, as you cannot shut down these VMs in advance of these events. • Disk or node failure • Controller VM Stargate service failure • Controller VM failure or restart • Degraded node
Node removal	When you remove a node that contains an replication factor 1 enabled storage container, the storage container and its vDisks are marked for removal. The storage container is not automatically marked for deletion. As part of node removal (which first fails in this case), you are prompted to delete the storage container, including all data on the storage container. This is effectively the same as deleting the container.
Disk removal or replacement	When you remove or replace a node's disk in an RF1-enabled storage container, data in the RF1-enabled storage container is automatically migrated to other disks associated with the RF1 node. If the node has insufficient disk space, the disk removal fails with a message similar to Warning: no disk space for RF1 data. For a failed disk with RF1 data that has no extra replicas, the data cannot be rebuilt. Therefore, when logically removing a failed disk with RF1 data, the disk removal might get stuck. In order to unblock the disk removal, delete the RF1 data in the degraded disk for a thorough cleanup. For more information, see KB 11662.

Degraded Node

A degraded node contains a CVM that is in a partially unresponsive state and cannot reliably perform cluster operations at the same performance level as normal clusters.

Nutanix clusters are designed to provide fault tolerance using container settings such as replication factor. Fault tolerance setting like replication factor itself does not guarantee protection from partial failures or degraded nodes. For example, a single node containing a disk exhibiting high latency (but that is partially responsive) can equally produce downtime for workloads running in clusters with replication factor 2 and replication factor 3 settings.

Degraded node events can occur because physical hardware can fail in innumerable ways. Diagnostics can capture only some of these events in software-defined failure cases. Degradation can lead to downtime of some or all production workloads running on the cluster.

The following events could contribute to node degradation:

- Network bandwidth reduction
- Network packet drops

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1895

- Soft lockups
- Partly malfunctioning disks
- Hardware issues (such as unreliable DIMM with ECC errors)

Degradation Effects

Nutanix clusters are designed to distribute the cluster services across the Controller VMs on all the constituent nodes to offer the best possible performance and resource allocation for the workloads. This distribution of services can cause a *degraded* (or partially available) node to adversely affect the performance of a cluster until you resolve the degradation.

Degradation versus Complete Failure

The difference between complete and partial failures (leading to degradation) explains the possibility of downtime during a degradation event.

Degradation

When a component such as a NIC or an SSD drive starts generating errors or drastically slows its throughput, the *Local Handler* service provides the first line of resolution.

For example, in an SSD drive, the *Local Handler* refers to either:

- The disk firmware deployed by the disk vendor.
- A Nutanix service on the Controller VM residing on the degraded node, such as the *Stargate* service, or the *Hades* disk manager.

When the *Local Handler* service recognizes that the SSD is producing a failure pattern that matches a harmful pattern, it marks the SSD as offline and Prism displays the SSD as a routine drive failure.

When the *Local Handler* encounters failure patterns that it does not recognize, the SSD continues to remain online. However, as a result of the failure pattern, the faulty device slows or halts the functioning of (or degrades) the distributed services throughout the cluster that depends on the device. This degradation of cluster services can lead to performance impact or storage unavailability for workload residing on nodes beyond the one (node) which has the SSD. This type of failure is termed as a *partial failure* of a component, where manual intervention is required to disable the degraded device and help the cluster services to recover. The *Local Handler* is unable to detect and mark the faulty device as faulty, resulting in the device remaining online and degrading the performance of the cluster.

Complete Failure

A complete failure of a component can be understood as a case where a fault occurring on a single node in the cluster is responded to effectively. Some examples of a complete failure are when a single node in a cluster goes offline due to AC power loss or because it is isolated on the network. In these events, a Controller VM is not reachable from the perspective of the rest of the cluster. In such a case of *complete failure*, the cluster works to restore resiliency based on the fault tolerance configuration of the cluster.

Table 15: Fault-Response Matrix

Type of fault	Local Handler*	Examples of response**
Disk error	Disk firmware	Update S.M.A.R.T. data to reflect that a disk has failed or could soon fail. For more information, see KB 8094.
	HBA firmware	Multiple disks could be marked as offline.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1896

Type of fault	Local Handler*	Examples of response**
	CentOS operating system	Mount disk as read-only.
		Register *udev* event for disk hot-plug
		Remove Controller VM boot disk partitions from RAID.
	Stargate Service	Mark disk as offline if read or write operation is not responding, send to Hades service to test.
	Cassandra Service	Controller VM is detached from the cluster metadata store, or a metadata repair is triggered, when Cassandra becomes unstable due to a failing disk.
	Curator Service	Stops using a particular disk during Curator scans if it produces I/O errors.
	Hades Service	Tests any drive that is marked offline by Stargate to check its S.M.A.R.T. health status and whether it is mountable.
	NCC	Monitors HBA error counters on disk interfaces. Raises alert if thresholds are exceeded.
CPU error	BIOS firmware	Correcting and logging recoverable errors
		Throttle CPU if necessary
		Halting and logging unrecoverable errors
	Hypervisor OS	Throttle performance
		Panic or halt
		Core dump
		Restart or hang.
Memory error	BIOS	Correcting and logging recoverable errors
		Online disabling of bad memory segments
		Decreasing the usable memory of a failing DIMM
		Masking a failing DIMM and potentially others in that channel
	Hypervisor OS	Throttle performance
		Logging errors
		Panic or halt
		Restart or hang.
Network error	NIC firmware	CVM/ host lost connection.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1897

Type of fault	Local Handler*	Examples of response**
	Software virtual switch	Error disable of bonded interface (Link Aggregation Control Protocol (LACP) timer set to *fast*)
		Failover to standby NIC (in active-standby bond modes)

Note:

* Local handlers could have other dependencies on the cluster. Their failure-handling abilities may not be available during events where more than one node is impacted by a particular failure.

**Response logic depends on the features available in the specific software or firmware versions deployed. It may be subject to change. Nutanix recommends that if you consider upgrading to the latest AOS maintenance release for the latest fault-tolerance capabilities.

Degraded Node Detection

Degraded Node Detection (DND) feature helps you limit the duration of impact or effects of a degraded node. In a Nutanix cluster, Degraded Node Detection constitutes the second line of resolution against partial hardware and software failures that escape the current logic of *Local Handler* services.

Degraded node detection consists of a global peer health database which monitors the services that run on each node of the cluster. Each node publishes health scores or votes for the services running on other peer nodes. The peer nodes health scores evaluate metrics such as:

- Remote Procedure Call (RPC) latency
- RPC failures or timeouts
- Network latency

If one node consistently receives poor health scores for approximately three (3) minutes then the peer nodes mark that node as a degraded node. The cluster may experience unavailability of storage containers or data stores during this 3 minute period.

The DND feature acts only when all of the following conditions are met:

- The cluster was **Resilient** prior to the event and could tolerate a node failure.
- The partial failure occurs only on one node in the cluster.
- The adverse effects of the partial failure sustain for at least 5 minutes.

Detection

Degraded Node Detection works as follows:

1. When a degraded node is detected, alerts are generated.

   See the alerts in the **Alerts** page. For more information on these alerts, see KB 3827 and KB 9132.

   The alerts trigger log collection to aid root cause analysis. See the **Log Collection for Alert XXXX** on the **Tasks** page. Click the **Succeeded** link to download the logs.
2. If the degraded node had leadership of critical services including Prism, the leadership is revoked.
3. Insights Data Fabric (IDF) services do not run on the degraded node.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1898

4. Cassandra services operate in Forwarding mode which means that the read and write requests of the Stargate service of the degraded node are serviced by Cassandra services of other nodes.

   Until the degradation is resolved, the cluster cannot guarantee storage availability in the event of subsequent partial or complete failures on other nodes.
5. Stargate of the degraded node stops placing Extent Group replicas on the degraded node.
6. If the degraded node hosts a Zookeeper server, that server is migrated to the Controller VM of another node.
7. The cluster is blocked from starting new upgrades or break-fix activities. If a node becomes degraded in the middle of an ongoing upgrade, an alert is generated.
8. Degraded Node Detection introduces an automatic resolution (auto-resolve) function that acts one day after the node is marked degraded (or after seven days in AOS 5.20.3 and earlier releases). Specifically, if a node remains degraded, the auto-resolve scan runs for about 60 minutes to check if the underlying issue is fixed. If no issues are found during the scan, the degraded node is marked as normal automatically. This ensures that the metadata store on the node is not marked offline permanently in the event that the cluster is currently healthy.

   Note: Note: Do not manually change the degraded status of the node (using the **Mark as Fixed** button in Prism) if you have not confirmed that the issue causing the node or CVM degradation has been fixed. Manually marking a degraded node as fixed can lead to production impacting issues including downtime of the cluster. Contact Nutanix Support for assistance.

Enabling Degraded Node Detection

About this task

To enable the degraded node detection settings in the Prism Element web console, perform the following steps.

Procedure

1. Log into the Prism Element web console.
2. Click the gear icon in the main menu and then select **Degraded Node Settings** in the **Settings** page.
   The **Degraded Node Settings** dialog box appears.
3. Set the degraded node detection status, **Enable Degraded Node Detection**.
   a. Ensure to select the checkbox to enable degraded node detection.
   b. Ensure to clear the checkbox to disable degraded node detection.
4. Click **Save** to confirm the settings.
   The **Degraded Node Settings** window closes and the Prism Element web console displays a pop-up confirmation.

Managing a Degraded Node

Manage a node if it is marked as degraded.

About this task

Once a node is detected as degraded, the leadership and critical services will not be hosted on that node.

Until a degraded node is unmarked from the degraded state, Cassandra services remain in the forwarding state. For more information, see Cluster Components on page 12. Once the degraded node is marked as fixed in Prism, Cassandra restarts its services on the node.

The alert for a degraded node appears in the **Alerts** page of the Prism Element web console.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1899

Procedure

1. Open the degraded node window.
   a. Click the **Alerts** icon at the top of the page.
   b. Click the alert for the degraded node.

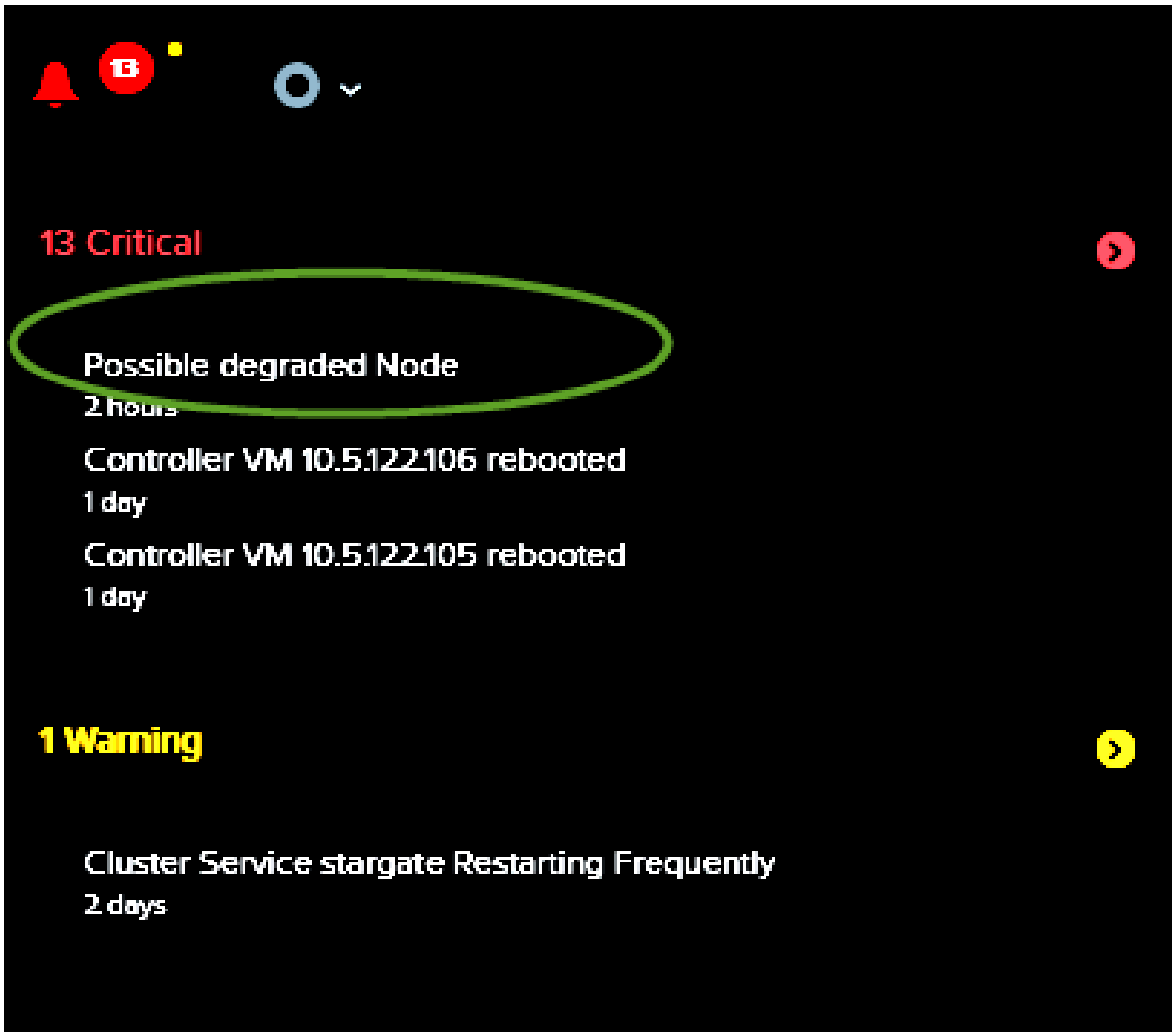


Figure 12: Possible Degraded Node in Alerts

   The degraded node window is displayed.

2. Set the status for the degraded node.
   a. **Resolve**: Select this option after you have fixed the underlying issue.

      Note: Selecting **Resolve** does not resolve the degraded node issue. It merely marks the alert status as **Resolved**, indicating you or Nutanix Support have resolved the underlying issue that triggered the alert.

   b. **Acknowledge**: Select this option to leave the degraded node in its current state, keep the alert unresolved, and mark the alert as acknowledged.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1900

3. You can also view the degraded node in the **Hosts** table.

   a. Go to **Home** > **Hardware** > **Host**.

   b. Select the degraded node which displays a critical alert.

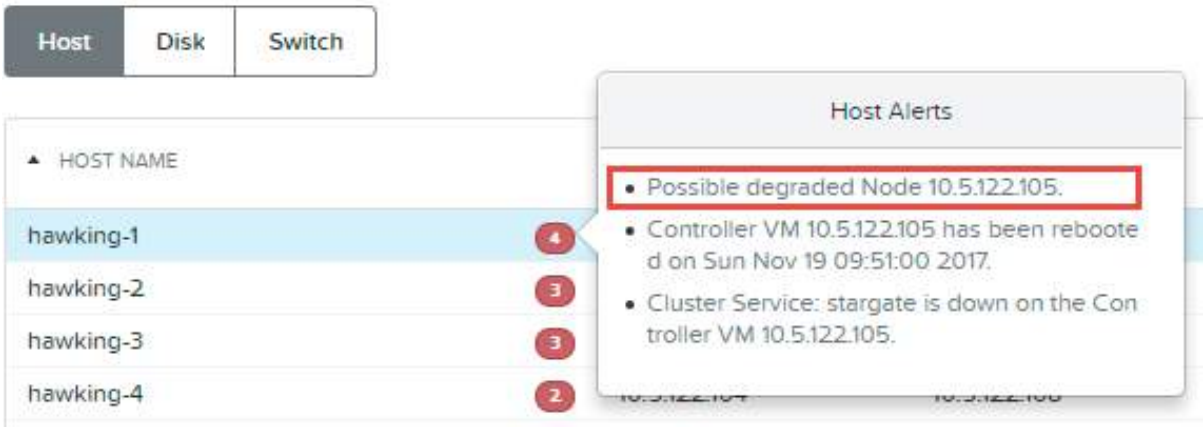


Figure 13: Degraded Node Pop-up Alert

4. To run an NCC check for the degraded node, go to the command line interface and enter

   ```
   nutanix@cvm$ ncc health_checks system_checks degraded_node_check
   ```

   The Prism Element web console does not remove the warning sign for the degraded node.

5. **Caution:** Do not unmark the degraded node if you have not confirmed that the issue causing the node or CVM degradation has been fixed. Unmarking a node can lead to production impacting issues in the cluster. Contact Nutanix Support for assistance.

   To unmark the degraded node, in the **Summary** view, select the fixed node and click **Mark as Fixed**.

Maximum System Values

Following are the considerations regarding the maximum number of hosts in a cluster:

- If you have a pure hypervisor cluster (cluster with only one type of hypervisor), you must adhere to the maximum number of hosts allowed by Nutanix Configuration Maximums for AHV or Nutanix Configuration Maximums for ESXi or Nutanix Configuration Maximums for Hyper-V.
- If your cluster consist of multiple hypervisors (mixed hypervisor cluster), you must adhere to the minimum number of hosts specified for any of the hypervisors in your cluster. For example, if your cluster consists of AHV and ESXi, then you are allowed to have the number of hosts specified for either AHV or ESXi, whichever is less. For more information, see Nutanix Configuration Maximums for AHV, Nutanix Configuration Maximums for ESXi, and Nutanix Configuration Maximums for Hyper-V.
- In a break-fix or generational upgrade (for example moving from NX G5 to G8 platform model) scenario, if you must exceed the number of hosts beyond the configuration maximum, contact Nutanix Support to temporarily allow the cluster extension beyond the limit. Clusters must always adhere to the size limits to ensure optimal performance and stability and you are allowed to exceed the limits only temporarily for these scenarios as an exception. You are expected to follow the size limits once the node is healthy or upgrades are complete. For more information, see KB 12681.

Nutanix clusters are also subject to the vSphere maximum values documented by VMware. For more information about the list of the vSphere maximums, see Configuration Maximums for the version of vSphere you are running.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1901

In case of contention of values between Nutanix and VMware, the Nutanix configuration maximum supersedes the VMware configuration maximum on Nutanix platforms.

Nutanix supports up to 50 VMs for each storage container if you are using Microsoft VSS-based backups in Hyper-V. If the number of VMs in each storage container exceeds 50, you might observe NFS timeouts when running backup jobs.

Three Node Cluster Considerations

A Nutanix cluster must have at least three nodes. Minimum configuration (three node) clusters provide the same protections as larger clusters, and a three node cluster can continue normally after a node failure. However, one condition applies to three node clusters only.

When a node failure occurs in a cluster containing four or more nodes, you can dynamically remove that node to bring the cluster back into full health. The newly configured cluster still has at least three nodes, so the cluster is fully protected. You can then replace the failed hardware for that node as needed and add the node back into the cluster as a new node. However, when the cluster has just three nodes, the failed node cannot be dynamically removed from the cluster. The cluster continues running without interruption on two healthy nodes and one failed node, but the failed node cannot be removed when there are only two healthy nodes. Therefore, the cluster is not fully protected until you fix the problem (such as replacing a bad boot disk) for the existing node.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1902

CLUSTER MANAGEMENT

Managing a Nutanix cluster involves configuring and monitoring the entities within the cluster, including virtual machines, storage containers, and hardware components. You can manage a Nutanix cluster through a web-based management console or a command line interface (nCLI).

- The Prism Element web console is a graphical user interface (GUI) that allows you to monitor cluster operations and perform a variety of configuration tasks. For more information, see Prism Element Web Console Overview on page 53.
- Nutanix employs a license-based system to enable your entitled Nutanix features, and you can install or regenerate a license through the Prism Element web console. For more information, see Prism Licensing on page 74.
- You can upgrade a cluster when a new AOS release is available through the Prism Element web console. For more information, see the Life Cycle Manager Guide.
- If you have multiple clusters, you can manage them all through a single web interface. For more information, see Multi-Cluster Management on page 93.

> **Note:** You can perform most administrative actions using either the Prism Element web console or nCLI. However, some tasks are only supported in the nCLI either because a new feature has not yet been incorporated into the Prism Element web console or the task is part of an advanced feature that most administrators do not need to use. For more information about how to use the nCLI, see Command Reference. For information about platform configuration and hypervisor-specific tasks that are not performed through the Prism Element web console, see AHV Administration Guide and hypervisor-specific guides.

Prism Element Web Console Overview

The web console, also known as Prism Element, provides a graphical user interface to manage most activities in a Nutanix cluster.

Display Features

The Prism Element web console screens are divided into the following sections:

- Main menu bar. The main menu bar appears at the top of every screen in the Prism Element web console. The cluster name appears on the far left of the main menu bar. To the right of the cluster name, you can select an entity from the pull-down list (Home, Health, VM, Storage, Network, Hardware, File Server, Data Protection, Analysis, Alerts, tasks, LCM, Settings) to display information about that entity. You can also search for specific topics or select various tasks from the pull-down lists on the right side of the main menu bar. In addition, the main menu bar includes status icons for quick access to heath, alert, and event information. For more information, see Main Menu on page 58.
- Entity views. There is a dashboard view for each entity. Some entities (VM, Storage, Hardware, and Data Protection) include additional views such as a diagram or table view that you can select from the dashboard of that entity.
- Screen menu bar. Some entity dashboards include another menu bar below the main menu that provides options specific to that screen. In the following example from the **Storage** dashboard, three view tabs (**Overview**, **Diagram**, and **Table**) and three task buttons (**+ Storage Container**, **+ Volume Group**, and **+ Storage Pool**) appear on this menu bar.
- Usage and performance/health statistics. Most views include fields that provide usage and either performance or health (or both) statistics. The usage and performance/health statistics vary based on the entity that you are viewing. For example, virtual machine usage statistics are displayed in terms of CPU and memory, while disk usage statistics show disk capacity in TB. In most cases, performance statistics are displayed in IOPS, latency, and bandwidth.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1903

- Alert and event messages. Several views include fields that list current event and alert messages. The listed messages are context specific, so for example only storage-related alerts and events appear on the Storage screen. Clicking on a message opens the alert or event view at that message. For more information, see Alerts Dashboard in *Prism Element Alerts and Events Reference Guide*.

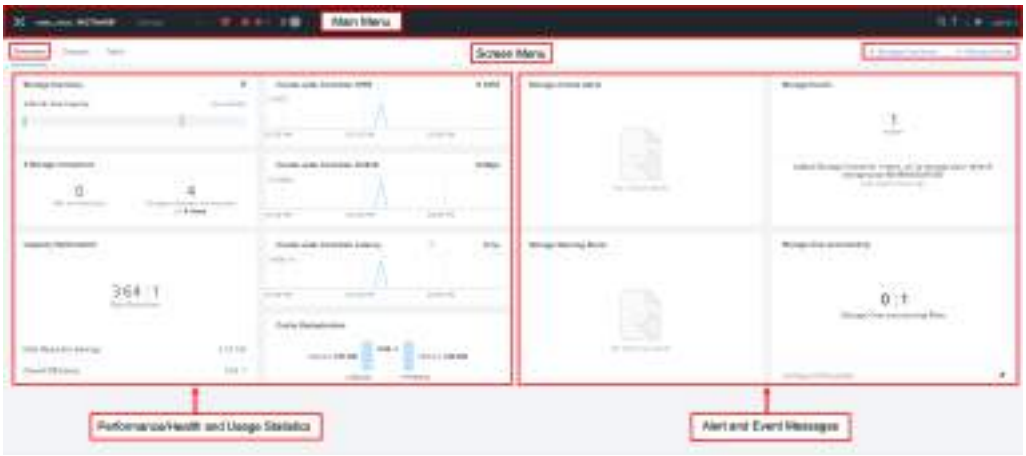


Figure 14: Overview Screen Sections

Logging Into the Prism Element Web Console

About this task

To log into the Prism Element web console, do the following.

For information about default cluster credentials, see KB 1661 lists default cluster credentials.

Procedure

1. Open a web browser.

   > **Note:**
   >
   > Prism Element web console supports the latest version, and the two preceding major versions of Firefox, Chrome, Safari, and Microsoft Edge browsers.

2. Enter http://`management_ip_addr` in the address field and press **Enter**. Replace `management_ip_addr` with the cluster virtual IP address (if configured) or the IP address of any Nutanix Controller VM in the cluster.

   > **Note:** If you are logging into Prism Central, enter the Prism Central VM IP address.

   The browser redirects to the encrypted port (9440) and may display an SSL certificate warning. Acknowledge the warning and proceed to the site. If user authentication is enabled and the browser does not have the correct certificate, a denied access message may appear. For more information, see Configuring Authentication.

3. If a welcome screen appears, read the message, and then click the *Accept terms and conditions* bar at the bottom.

   For more information on the welcome screen, see Configuring a Banner Page on page 365.

4. In the login screen, enter your Nutanix login credentials and press **Enter** or click the right arrow icon.

   > **Note:** If you are using LDAP authentication, enter the user name in the `samAccountName@domain` format; the `domain\user` format is not supported. (Authentication does not use the user principle name

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1904

[UPN]; *user@domain* is simply a concatenation of the user and domain names specified in Configuring Authentication.)

Note: The login page includes background animation that is enabled by default. Click the **Freeze space time continuum!** link at the bottom right of the login screen to disable the animation (or the **Engage the warp drive!** link to enable the animation). For information on how to permanently disable (or enable) the animation, see Modifying UI Settings on page 71.

5. If you are logging in as an administrator (admin user name and password) for the first time, which requires that the default password (Nutanix/4u) be changed, enter a new password in the **password** and **re-type password** fields and then press **Enter** or click the right arrow icon.

   The password must meet the following complexity requirements:

   - At least 8 characters long
   - At least 1 lowercase letter
   - At least 1 uppercase letter
   - At least 1 number
   - At least 1 special character (allowed special characters are: "#$%&'()*+,-./:;<=>@[]^_`{|}~!)
   - At least 4 characters different from the old password
   - Must not be among the last 5 passwords
   - Must not have more than 2 consecutive occurrences of a character
   - Must not be longer than 199 characters

   After you have successfully changed the password, the new password is synchronized across all Controller VMs and interfaces (Prism Element web console, nCLI, and SSH).

   Note:

   - You are prompted to change the password when logging in as the **admin** user for the first time after upgrading AOS. If the first login after upgrade is to the Controller VM through SSH (instead of Prism), you must log in using the default **admin** user password (Nutanix/4u) and then change the password when prompted.
   - The default password expiration age for the `admin` user is 60 days. You can configure the minimum and maximum password expiration days based on your security requirement.
     - `nutanix@cvm$ sudo chage -M <MAX-DAYS> admin`
     - `nutanix@cvm$ sudo chage -m <MIN-DAYS> admin`
   - When you change the **admin** user password, update any applications and scripts using the **admin** user credentials for authentication. Nutanix recommends that you create a user assigned with the admin role instead of using the **admin** user for authentication.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1905

6. If a license agreement screen appears (typically on the first login or if the EULA changed since the last login), which indicates the current EULA has not been acknowledged yet, do the following:

   a. Read the license agreement (on the left).

   b. Enter appropriate information in the **Name**, **Company**, and **Job Title** fields (on the right).

   c. Select the *I have read and agree to the terms and conditions* checkbox.

   d. Click the **Accept** button.

7. If a *Pulse will be Enabled* screen appears (typically on the first login or after an upgrade), read the statement and then do one of the following. This screen refers to the Pulse feature that alerts Nutanix customer support regarding the health of the cluster. For more information, see Pulse Health Monitoring on page 384.

   » Click **Continue** to enable the Pulse feature (recommended).

   » Click **Disable Pulse (not recommended)** to disable the Pulse feature.

   > **Caution:** If Pulse is not enabled, alerting Nutanix customer support when problems occur is disabled.

   Pulse provides Nutanix customer support with analytic information that allows them to dynamically monitor your cluster and identify potential issues before they become problems. For more information, see Remote Diagnostics on page 385. Enabling Pulse is recommended unless providing cluster information to Nutanix customer support violates your security policy.

8. If a screen about enhanced cluster health monitoring appears (typically either after enabling Pulse in the previous step or after upgrading a cluster), read the statement and then do one of the following:

   » Click the **Yes (recommended)** button to enable enhanced cluster health monitoring.

   » Click the **Not Now** button to disable this feature.

   The enhanced (on top of standard Pulse) cluster health monitoring provides Nutanix customer support with more detailed (but more transparent) information that allows them to better monitor the health of your cluster.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1906

Enhanced cluster health monitoring is recommended unless providing information such as entity names violates your security policy.

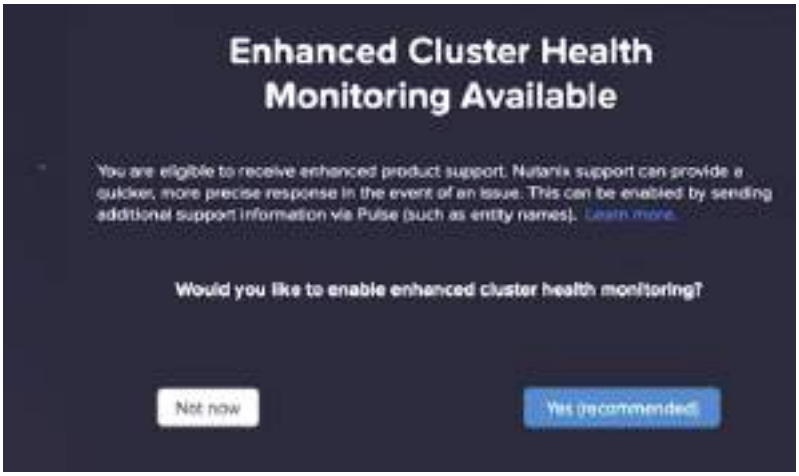


Figure 15: Enhanced Monitoring Screen (upgrade example)

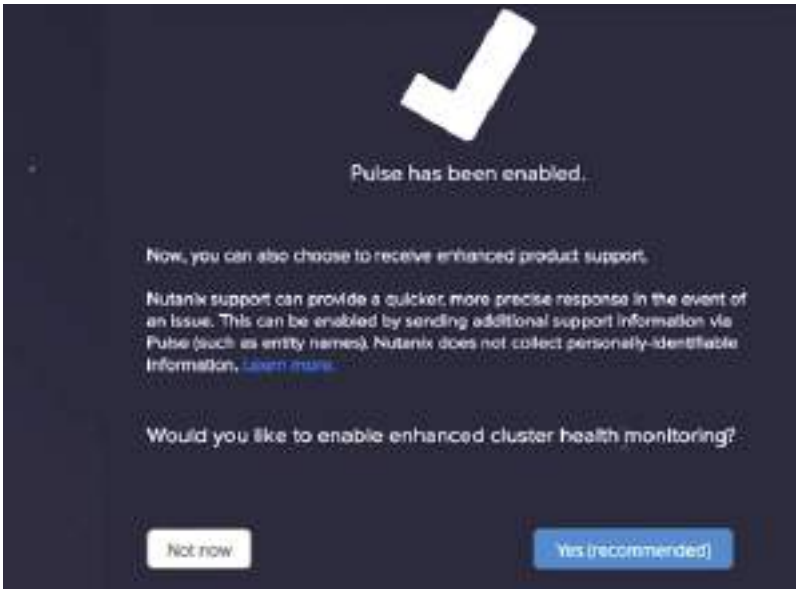


Figure 16: Enhanced Monitoring Screen Example (initial example)

9. [2-node clusters only] If a screen about registering with a Witness appears, see Witness Option in the *Data Protection and Recovery with Prism Element* guide.

Logging Out of the Prism Element Web Console

Procedure

To log out from the Prism Element web console, click the user icon in the main menu and then select the **Sign Out** option from the dropdown list. You are logged out immediately after selecting the option (no prompt or message).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1907

Main Menu

The main menu at the top of every screen provides access to all the features of the Prism Element web console. This section describes each of the main menu options.

Cluster Information

The cluster name appears on the far left of the main menu bar. Clicking the cluster name opens the **Cluster Details** window. This window displays the cluster ID number, cluster name, and cluster virtual IP address (if set). You can modify the name or virtual IP address at any time. For more information, see Modifying Cluster Details on page 74.

View Options

Selecting a view (entity name) from the pull-down list on the left displays information about that entity. Select from the following options:

- **Home**: Displays the main dashboard (see Home Dashboard).
- **Health**: Displays the health dashboard (see Health Dashboard on page 256).
- **VM**: Displays a virtual machine information dashboard (see VM Dashboard).
- **Storage**: Displays a storage information dashboard (see Storage Dashboard on page 124).
- **Network** (AHV only): Displays the network visualiser.
- **Hardware**: Displays a hardware information dashboard (see Hardware Dashboard on page 187).
- **File Server**: Displays a file server dashboard (see Nutanix Files Guide).
- **Data Protection**: Displays a data protection information dashboard (see Data Protection Dashboard).
- **Analysis**: Displays a screen to create and run performance monitors (see Analysis Dashboard on page 334).
- **Alerts**: Displays a screen of alert and events messages (see Alerts Dashboard in *Prism Element Alerts and Events Reference Guide*).
- **Tasks**: Displays a screen of task messages (see View Task Status on page 89).
- **LCM**: Displays the life cycle manager (LCM) dashboard (see Life Cycle Management (LCM) on page 79).
- **Settings**: Displays the Settings menu, as does clicking the gear icon on the right of the main menu (see Settings Menu on page 60).

> **Note:** These views reflect that Prism Element retains alerts and events, and raw metric values for 90 days.

Informational and Search Features

There are multiple ways to access information from the main menu:

- A health (heart) icon appears on the left of the main menu. It can be green (healthy), yellow (warning), or red (unhealthy) indicating the current heath status. Clicking the icon displays the heath details view. For more information, see Health Dashboard on page 256.
- An alerts (bell) icon appears on the left of the main menu when critical (red), warning (yellow), or informational (gray) alert messages have been generated and have not been marked as resolved. The number of unresolved alerts is displayed in the icon. Click the icon to display a drop-down list of the most recent unresolved alerts. Click an alert or the right arrow link to open the alerts view. For more information, see Alerts Dashboard in *Prism Element Alerts and Events Reference Guide*.
- A tasks (circle) icon appears to the right of the alerts icon. The number of active tasks (running or completed within the last 48 hours) is displayed in the icon. Click the icon to display a drop-down list of the active tasks, and

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1908

then click the **View All Tasks** button to open the tasks view. For more information, see View Task Status on page 89.

- A search (magnifying glass) icon appears on the right side of the main menu. Click this icon to display a search field. You can search for information about entities or actions by entering a string in this field. For example, you can enter an action name such as add that returns a list of add actions or an entity name such as MyVM that returns a list of links related to that entity.

Help Menu

A question mark icon appears on the right side of the main menu. Clicking the question mark displays a list of help resource options that you can select. The following table describes each option in the pull-down list.

Table 16: Help Menu Options

Name	Description
Help with this page	Opens the online help at the page that describes this screen. For more information, see Accessing Online Help on page 399.
Health Tutorial	Opens the Health dashboard tutorial that takes you through a guided tour of the health analysis features. For more information, see Health Dashboard on page 256.
General Help	Opens the online help at the introduction page.
Support Portal	Opens a new browser tab (or window) at the Nutanix support portal login page. For more information, see Accessing the Nutanix Support Portal on page 395.
Nutanix Next Community	Opens a new browser tab (or window) at the Nutanix Next Community entry page. This is an online community site for customers and partners to exchange ideas, tips, and information about Nutanix technologies and related datacenter topics. For more information, see Accessing the Nutanix Next Community on page 400.

User Menu

A user icon appears on the far right side of the main menu with the current user login name. Clicking the user icon displays a list of options to update your user account, log out from the Prism Element web console, and other miscellaneous tasks. The following table describes each option in the dropdown list.

Table 17: User Menu Options

Name	Description
Update Profile	Opens the **Update Profile** window to update your user name and email address. For more information, see Updating My Account.
Change Password	Opens the **Change Password** window to update your password. For more information, see Updating My Account.
REST API Explorer	Opens a new browser tab (or window) at the Nutanix REST API Explorer web page. For more information, see Accessing the REST API Explorer on page 397.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1909

Name	Description
Download nCLI	Downloads the Nutanix command line interface (nCLI) as a zip file to your local system. The download occurs immediately after clicking this option (no additional prompts). For more information about installing the nCLI locally and for nCLI command descriptions, see Nutanix Command Reference.
Download Cmdlets Installer	Downloads the PowerShell installer for the Nutanix cmdlets. For more information about the cmdlets, see PowerShell Cmdlets Reference.
Download Prism Central	Opens a new browser tab (or window) at the **Support Tools** page of the Nutanix support portal from which you can download the files to install Prism Central. If a login page appears, enter your Nutanix support portal credentials to access the portal. For more information, see Prism Central Infrastructure Guide.
About Nutanix	Opens a window that displays Nutanix operating system (AOS) and other version information. For more information, see Finding the AOS Version Using Prism Element on page 74.
Nothing To Do?	Opens a game that is strictly for entertainment. To quit the game, click the *X* at the upper right of the screen.
Sign Out	Logs out the user from the Prism Element web console. For more information, see Logging Out of the Prism Element Web Console on page 57.

Settings Menu

The Prism Element web console includes a Settings page from which you can configure a variety of system services.

You can access the **Settings** page by doing either of the following:

- Click the gear icon on the right of the main menu.

  For more information, see Main Menu on page 58.

- Select **Settings** from the dropdown list on the left of the main menu.

The **Settings** page displays a menu of tasks (on the left) you can perform. Click the task to open the window or page for that option in the pane to the right. The following table describes each menu option.

Table 18: Settings Menu List

Name	Description
General	
Cluster Details	Opens the **Cluster Details** window to view or modify certain cluster parameters. For more information, see Modifying Cluster Details on page 74.
Configure CVM	Opens the **Configure CVM** window to increase the Controller VM memory size. For more information, see Increasing the Controller VM Memory Size on page 106.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1910

Name	Description
Convert Cluster	Opens the **Convert Cluster** window to convert the cluster from ESXi to AHV and then from AHV to ESXi. For more information, see In-Place Hypervisor Conversion on page 368.
Expand Cluster	Opens the **Expand Cluster** window to add new nodes to the cluster . For more information, see Expanding a Cluster on page 201.
Image Configuration [AHV only]	Opens the **Image Configuration** window to import and mange image files that can be used to create VMs. For more information, see Configuring Images on page 295.
Licensing	Opens the **Licensing** window to install or update the cluster license that enables entitled Nutanix features. For more information, see Prism Licensing on page 74.
Reboot [AHV]	Opens the **Request Reboot** window to gracefully restart the nodes in the cluster one after the other. You can select the nodes you want to restart. For more information, see Rebooting an AHV or ESXI Node in a Nutanix Cluster on page 107.
Remote Support	Opens the **Remote Support Services** window, which enables (or disables) Nutanix remote support access. For more information, see Controlling Remote Connections on page 393.
Upgrade Software	Opens the **Upgrade Software** window to upgrade the cluster to a newer AOS version, or update other upgradeable components. For more information, see Software and Firmware Upgrades on page 78.
vCenter Registration [ESXi only]	Opens the **vCenter Registration** window to register (or unregister) the cluster with the vCenter instance. For more information, see Registering a Cluster to vCenter Server on page 366.
Setup	
Connect to Citrix Cloud [AHV and XenServer only]	Opens the **Connect to Citrix Cloud** window to connect to the Citrix Workspace Cloud. For more information, see Connect to Citrix Cloud on page 330.
Prism Central Registration	Opens the **Prism Central Registration** window to add the cluster into a central registration for multicluster connection and support. For more information, see Registering or Unregistering a Cluster with Prism Central in *Prism Central Infrastructure Guide*.
Pulse	Opens the **Pulse** window to enable the sending of cluster information to Nutanix customer support for analysis. For more information, see Pulse Configuration on page 386.
Rack Configuration	Opens the **Rack Configuration** page to configure the fault tolerant domain for node, block, and rack awareness. For more information, see Rack Fault Tolerance on page 35.
Network	
HTTP Proxy	Opens the **HTTP Proxy** window to configure an HTTP proxy to which the Nutanix software can connect. For more information, see Configuring HTTP Proxy on page 394.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1911

Name	Description
Name Servers	Opens the **Name Servers** window to configure name servers for the cluster. For more information, see Configuring Name Servers on page 353.
Network Configuration [AHV only]	Opens the **Network Configuration** window to configure network connections for the cluster. For more information, see Network Configuration for VM Interfaces on page 167.
Network Switch	Opens the **Network Switch Configuration** window to configure network switch information needed for collecting network traffic statistics. For more information, see Configuring Network Switch Information on page 172. This option does not appear when running a hypervisor that does not support this feature.
NTP Servers	Opens the **NTP Servers** window to specify which NTP servers to access. For more information, see Configuring NTP Servers on page 354.
SNMP	Opens the **SNMP Configuration** window to enable and configure SNMP for the cluster. For more information, see Configuring SNMP on page 355.
Security	
Cluster Lockdown	Opens the **Cluster Lockdown** window, which allows you to delete (or add) public authentication keys used for SSH access into the cluster. Removing all public keys locks down the cluster from external access. For more information, see Controlling Cluster Access.
Data at Rest Encryption [SEDs only]	Opens the **Data-at-Rest Encryption** screen to configure key management for self encrypting drives (SEDs) and enable data encryption across the cluster. This menu option appears only when the data drives in the cluster are SEDs. For more information, see Data-at-Rest Encryption.
Filesystem Whitelists	Opens the **Filesystem Whitelist** window to specify whitelist addresses. For more information, see Configuring a Filesystem Whitelist on page 352.
SSL Certificate	Opens the **SSL Certificates** window to create a self-signed certificate. For more information, see Certificate Management.
Users and Roles	
Authentication	Opens the **Authentication Configuration** window to configure authentication for the cluster. For more information, see Configuring Authentication.
Local User Management	Opens the **Local User Management** window. This window lists current users and allows you to add, update, and delete user accounts. For more information, see User Management.
Role Mapping	Opens the **Role Mapping** window to configure role mappings that apply in the user authentication process. For more information, see Configuring Authentication.
Email and Alerts	
Alert Email Configuration	Opens the **Alert Email Configuration** window, which enables (or disables) the e-mailing of alerts. For more information, see Configuring Alert Emails in *Prism Element Alerts and Events Reference Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1912

Name	Description
Alert Policies	Opens the **Alert Policies** window, which allows you to specify what events should generate an alert and how frequently the system should check for each event type. For more information, see Configuring Alert Policies in *Prism Element Alerts and Events Reference Guide*.
SMTP Server	Opens the **SMTP Server Settings** window to configure an SMTP server. For more information, see Configuring an SMTP Server on page 355.
Data Resiliency	
Configure Witness [ESXi and AHV only]	Opens the **Configure Witness** window to add a witness VM for metro availability and two-node clusters. For more information, see Witness Option in *Data Protection and Recovery with Prism Element Guide*.
Degraded Node Settings	Opens the **Degraded Node Settings** window to enable or disable Degraded Node Detection. For more information, see Degraded Node on page 45.
Manage VM High Availability [AHV only]	Opens the **Manage VM High Availability** window to enable high availability for guest VMs in the cluster. For more information, see Enabling High Availability for the Cluster on page 305.
Cluster Fault Tolerance	Opens the **Cluster Fault Tolerance** window to increase the fault tolerance of the cluster. For more information, see Increasing the Cluster Fault Tolerance Level on page 76.
Appearance	
Language Settings	Opens the **Languages** window, which allows you to select the language of the Prism Element web console. For more information, see Localization (L10n) on page 375.
UI Settings	Opens the **UI Settings** window to configure Prism UI background themes, disable (or re-enable) the login screen. For more information, see Modifying UI Settings on page 71.
Welcome Banner	Opens the **Edit Welcome Banner** window to create a welcome banner message that appears before users login to the Prism Element web console. For more information, see Configuring a Banner Page on page 365.

Home Dashboard

The Home dashboard is the opening screen that appears after logging into the Prism Element web console. It provides a dynamic summary view of the cluster status. To view the Home dashboard at any time, select **Home** from the pull-down list on the far left of the main menu.

Menu Options

The Home dashboard does not include menu options other than the options available from the main menu. For more information, see Main Menu on page 58.

Home Screen Details

The Home dashboard displays cluster-level performance and usage statistics on the left, health status information in the middle, and the most recent alert and event messages on the right. The following table describes each field in this screen. Several fields include a slide bar on the right to view additional information in that field. The displayed information is dynamically updated to remain current.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1913

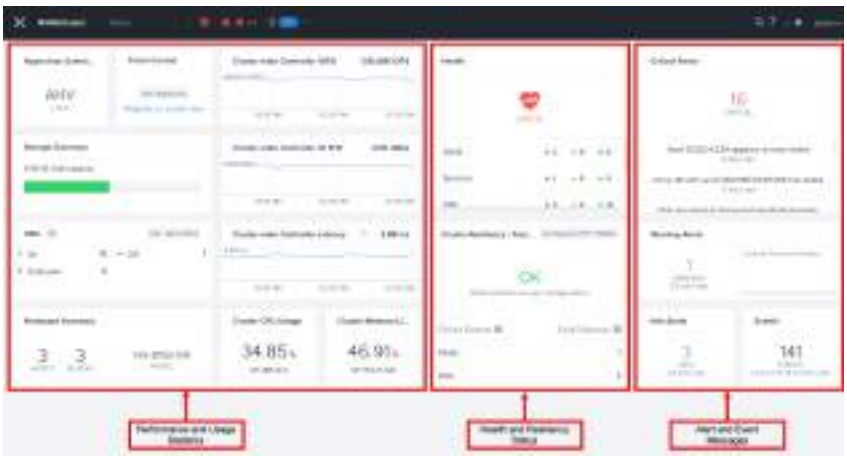


Figure 17: Home Dashboard

Note: These fields reflect that Prism Element retains alerts and events, and raw metric values for 90 days.

For information about how the statistics are derived, see Understanding Displayed Statistics on page 70.

Table 19: Home Screen Fields

Name	Description
Hypervisor Summary	Displays the name and version number of the hypervisor.
Prism Central	Displays whether you have registered the cluster to a Prism Central instance or not. Click **Register** to register the cluster to a Prism Central instance. If you have already registered, you can click **Launch** to launch the Prism Central instance in a new tab of your browser.
Storage Summary	Displays information about the physical storage space utilization (in GiB or TiB) and resilient capacity of the cluster. Placing the cursor anywhere on the horizontal axis displays a breakdown view of the storage capacity usage. The **View Details** link displays the resiliency status and storage information of all the individual nodes in the cluster. For more information, see Storage Details Page on page 126. You can also configure a threshold warning for the resilient capacity utilization in the cluster by clicking the gear icon. For more information, see Configuring a Warning Threshold for Resilient Capacity on page 113.
VM Summary	Displays the total number of VMs in the cluster broken down by on, off, and suspended states.
Hardware Summary	Displays the number of hosts and blocks in the cluster, plus one or more Nutanix block model numbers.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1914

Name	Description
Cluster-wide Controller IOPS	Displays I/O operations per second (IOPS) in the cluster. The displayed time period is a rolling interval that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. (These display features also apply to the I/O bandwidth and I/O latency monitors.) For more in-depth analysis, you can add this chart (and any other charts on the page) to the analysis page by clicking the blue link in the upper right of the chart. For more information, see Analysis Dashboard on page 334.
Cluster-wide Controller IO Bandwidth	Displays I/O bandwidth used per second in the cluster. The value is displayed in an appropriate metric (MBps, KBps, and so on) depending on traffic volume.
Cluster-wide Controller Latency	Displays the average I/O latency (in milliseconds) in the cluster.
Cluster CPU Usage	Displays the current CPU utilization percentage along with the total available capacity (in GHz).
Cluster Memory Usage	Displays the current memory utilization percentage along with the total available capacity (in GB).
Health	Displays health status for the cluster as a whole (good, warning, critical) and summary health status for the VMs, hosts, and disks in the cluster. Clicking the VMs, hosts, or disks line displays detailed information about that object in the Health page. For more information, see Health Dashboard on page 256.
Cluster Resiliency/Fault Tolerance Status	Displays the following: • type of cluster fault tolerance, the current failure domain (rack, block, or node), and the level of fault tolerance (1 or 2). • indicates if there is a change in the current fault domain from their configured state. • displays a **Rebuild Progress** indicator that allows you to track the estimated time until full resiliency has been restored to the cluster if a data rebuild is triggered after a component failure. For more information on the **Cluster Resiliency / Fault Tolerance Status** widget, see the following Cluster Resiliency/Fault Tolerance Status section.
Critical Alerts	Displays the most recent unresolved critical alert messages. Click a message to open the Alert screen at that message. For more information, see Alerts Dashboard in *Prism Element Alerts and Events Reference Guide*.
Warning Alerts	Displays the most recent unresolved warning alert messages. Click a message to open the Alert screen at that message.
Info Alerts	Displays a summary of informational alerts.
Events	Displays a summary of events.

Cluster Resiliency/Fault Tolerance Status

The **Cluster Resiliency / Fault Tolerance Status** widget indicates whether the cluster can safely handle a node failure, that is, whether a copy of all data in any node exists somewhere in the cluster. The fault tolerance status of a cluster can have any one of the following states:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1915

- **OK**: This state indicates that the fault tolerance domain is highly resilient and can safely handle a node or disk (in single or two-node clusters) failure.
- **Warning**: This state indicates that the fault tolerance level is almost reaching 0. A warning state is displayed if the cluster is not fault tolerant at the configured domain but is fault tolerant at a lower domain. For example, if you have configured rack as the configured domain and the cluster can no longer handle any rack failures due to some reason but can still handle node (lower domain) failures, then the fault tolerance state is displayed as **Warning**.
- **Critical**: This state indicates that the fault tolerance level is 0, and the fault tolerance domain cannot handle a node or disk (in single or two-node clusters) failure.
- **Computing**: This state indicates that the new fault tolerance level is being calculated.

Clicking anywhere in the widget displays the **Cluster Resiliency / Fault Tolerance Status** dialog box. This dialog box displays more detailed cluster resiliency status information. This window provides information about the number and type of failures the cluster can withstand safely. The **Failures Tolerable** column indicates the number of simultaneous failures of that component type that can be tolerated (0, 1, or 2). When no failure can be tolerated, a message is displayed to highlight the limitation, where there are not enough blocks in the cluster to support a block failure.

Note:

- The resiliency status for single-node backup cluster is at the disk level and not at the node level. For more information, see Single-Node Replication Target Clusters in the *Data Protection and Recovery with Prism Element Guide*.
- When a node goes down, the extent group (egroup) fault tolerance status remains unchanged as the node is assumed (initially) to be unavailable just temporarily. However, Stargate fault tolerance goes down by one until all data has been migrated off that node. The egroup fault tolerance status goes down only when a physical copy of the egroup replica is permanently bad. For more information on Stargate, see Cluster Components on page 12.

Rebuild Progress (Cluster Resiliency/Fault Tolerance Status Widget)

You can monitor the data rebuild status of cluster entities like disks and nodes through the **Rebuild Progress** indicator. This rebuild progress bar reflects in the **Cluster Resiliency / Fault Tolerance Status** widget on the Prism Element **Home** page within a maximum duration of 90 seconds when a data rebuild event occurs due to a disk removal (or a node removal which triggers disk removals of the individual disks).

For example, if you mark a disk for removal, it takes a maximum of 90 seconds for its rebuild progress to appear in the **Cluster Resiliency / Fault Tolerance Status** widget.

The main objective of this feature is to provide the admin with information about the ongoing data rebuilds for disks and nodes. Along with the overall ETA and rebuild progress percentage for participating entities, you can also monitor the individual progress of the entities.

Data Rebuild Scenarios

You can monitor the data rebuild for the following scenarios.

- You mark a disk for removal.

  A disk is removed in any of the following cases.

  - You manually perform the **Remove Disk** operation.
  - A Stargate process internally encounters that a disk has gone down and marks it for removal.
- You mark a node offline.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1916

The **Cluster Resiliency / Fault Tolerance Status** widget displays the data rebuild progress and ETA as an aggregate of all overlapping rebuilds. If a data rebuild operation intersects other rebuild operations, they are considered to belong to a single rebuild generation. In such a scenario, the Prism Element web console displays the weighted average of the progress percentage of all the entities and maximum time of the ETA for all rebuilds in that generation.

For information on how to monitor the overall data rebuild ETA, overall progress percentage, and detailed progress information for nodes and disks respectively, see the Monitoring Node Rebuild Progress on page 69 and Monitoring Disk Rebuild Progress on page 68 sections.

> **Note:** **Cluster Resiliency / Fault Tolerance Status** widget displays only a single generation data rebuild at any point in time.

Rebuild Phases

A data rebuild has the following phases.

- **Rebuilding Data**. Indicates that the data rebuilt progress up to 100% . This includes time to rebuild data and also validate that all data has actually been rebuilt.
- **Data Rebuild Complete**. Indicates the success of the data rebuild operation.
- **Aborted**. Indicates an aborted rebuild operation. The rebuild operation aborts when a node that went offline comes back online.

Data Rebuilt

The following data rebuilds when a rebuild scenario triggers.

> **Note:** The data rebuild percentage does not account for metadata rebuild. For example, if the metadata rebuild is at 10% and the data rebuild is 100%, the **Cluster Resiliency / Fault Tolerance Status** widget displays the rebuild percentage as 100%. The metadata rebuild progress currently appears on the **Tasks** page of the Prism Element web console.

- Extent store data
  - Extent groups on victim disk.
- Oplog episodes
  - Unflushed oplog episodes on the victim disk.
- Near Sync LWS episodes.

> **Note:** The progress percentage of the extent store data rebuild restricts to 95% until the rebuild completes for oplog and NearSync LWS episodes

Keyboard Shortcuts in Prism Element Web Console

You can use the following keyboard shortcuts to invoke important menu options or views in Prism Element web console:

Table 20: Keyboard Shortcuts for Prism Element web console

Shortcut Key	Menu Option/View
m	Main Menu
s	Settings Menu

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1917

Shortcut Key	Menu Option/View
f or /	Spotlight (search bar)
u	User Menu
a	Alerts menu
h	Help menu (? menu)
p	Recent tasks

You can use the arrow keys to select a particular menu option.

If you are on a page with sub pages (such as Storage Dashboard), yo can use the following keyboard shortcuts to navigate through the various view:

Table 21: Keyboard Shortcuts for a dashboard

Shortcut Key	Menu Option/View
o	Overview View
d	Diagram View
t	Table View

Monitoring Disk Rebuild Progress

About this task

Perform the following procedure to monitor the data rebuild progress and overall rebuild completion ETA for a disk. Curator periodically sends the data rebuild information to Insights. Prism Element queries this data rebuild information from the Insights DB. The rebuild progress bar for the disk reflects in the **Cluster Resiliency / Fault Tolerance Status** widget within a maximum duration of 90 seconds.

Procedure

1. Log in to Prism Element web console.
2. Go to **Home** > **Cluster Resiliency / Fault Tolerance Status** widget.
3. Monitor the **Rebuild Progress** progress bar to view the rebuild completion percentage.
4. Hover over the (?) symbol to view the rebuild completion ETA for the current generation.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1918

5. To view the following rebuild metrics for the individual entities, click anywhere on the **Rebuild Progress** field.
   The system opens the **Rebuild Progress Details** dialog box displaying the following rebuild metrics.

   - **Disk ID**: Displays the disk identification number (ID number).
   - **Serial No**: Displays the disk serial number (serial number).
   - **Slot No**: Displays the slot number associated with the disk (slot number).
   - **Node**: Displays the node name.
   - **Type**: Displays the disk type (tier name). The Nutanix platform can contain disk tiers for PCIe solid state disks (SSD-PCIe), SATA solid-state disks (SSD-SATA), and direct attach SATA hard disk drives (DAS-SATA) depending on the platform type [SSD-PCIe | SSDSATA | DAS-SATA].
   - **Rebuild Phase**: Displays the current data rebuild status. For information about the data rebuild phases, see Home Dashboard on page 63.
   - **Rebuild Progress**: Displays the rebuild progress percentage.
   - **Elapsed Time**: Displays the time elapsed since the data rebuild operation started.
   - **Estimated Time**: Displays the estimated time for the data rebuild operation to complete.

   You can verify the rebuild event status through the **Tasks** option.

Monitoring Node Rebuild Progress

About this task

Perform the following procedure to monitor the data rebuild progress and overall rebuild completion ETA for a node. Curator periodically sends the data rebuild information to Insights. Prism Element queries this data rebuild trigger from the Insights DB. The rebuild progress bar for the node reflects in the **Cluster Resiliency / Fault Tolerance Status** widget within a maximum duration of 90 seconds.

> **Note:** The offline node progress appears only if the Stargate health is down.

Procedure

1. Log in to Prism Element web console.
2. Go to **Home** > **Cluster Resiliency / Fault Tolerance Status** widget.
3. Monitor the **Rebuild Progress** progress bar to view the rebuild completion percentage.
4. Hover on the (?) symbol to view the rebuild completion ETA for the current generation.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1919

5. Click anywhere on the **Rebuild Progress** field to view the following rebuild metrics for the individual entities.
   The system opens the **Rebuild Progress Details** dialog box displaying the following rebuild metrics.

   - **Node**. Displays the node name.
   - **Rebuild Phase**. Displays the current data rebuild status. For information about the data rebuild phases, see Home Dashboard on page 63.
   - **Rebuild Progress**. Displays the rebuild progress percentage.
   - **Elapsed Time**. Displays the time elapsed since the data rebuild operation started.
   - **Estimated Time**. Displays the estimated time for the data rebuild operation to complete.

   You can verify the rebuild event status through the **Tasks** option.

Understanding Displayed Statistics

The Prism Element web console and Prism Central web console display various statistics that are derived from the following sources:

> **Note:** Most displayed statistics appear in 30 second intervals. The values in the tables represent the most recent data point within the last 30 seconds. Prism Central collects the statistical data from each registered cluster, so the process of collecting that data could result in a longer lag time for some statistics displayed in Prism Central.

1. *Hypervisor*: Hypervisor provides usage statistics only. The support to provide usage statistics is available only in ESXi, and not in Hyper-V and AHV hypervisors. If the cluster consists of Hyper-V or AHV hypervisor, the controller provides the usage statistics.

   > **Note:** Ensure that you consider the usage statistics reported from ESXi hypervisor in both Prism Central and Prism Element, only when it matches with the usage statistics in vCenter.

2. *Controller (Stargate)*: When hypervisor statistics are unavailable or inappropriate, the Controller VM (CVM) provides the statistics from Stargate. For more information about Stargate, see Nutanix Bible. The Controller-reported statistics might differ from those reported by the hypervisor for the following reasons:

   - An NFS client might break up large I/O requests into smaller I/O units before issuing them to the NFS server, thus increasing the number of operations reported by the controller.
   - The hypervisor might read I/O operations from the cache in the hypervisor which are not counted by the controller.

3. *Disk (Stargate)*: Stargate can provide statistics from both controller and disk perspective. The controller perspective includes reading both I/O operations from memory and disk I/O operations, but the disk perspective includes only disk I/O operations.

   > **Note:** The difference in statistics derived from the sources: Hypervisor, Controller, and Disk, only applies to storage-related statistics such as IOPS, latency, and bandwidth.

The following field naming conventions are used in Prism Central to identify the information source:

- A field name with **Controller** word indicates the statistic is derived from the controller (for example *Controller IOPS*).
- A field name with **Disk** word indicates the statistic is derived from the disk (for example *Disk IOPS*).
- A field name without **Controller** or **Disk** word indicates the statistic is derived from the hypervisor. For example **IOPS**.

For VM statistics in a mixed ESXi/AHV cluster, the statistics source depends on the type of hypervisor that hosts the VM. If the Hypervisor is:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1920

- ESXi - The hypervisor is the source for statistics.
- AHV - The controller is the source for statistics.

> **Note:**
>
> - The overview, VM, and storage statistics are derived from either the hypervisor or controller.
> - Hardware statistics are derived from disk.
> - Metrics in the analysis page are derived from any of the sources: hypervisor, controller, or disk, based on the type of metric.

The following table provides the information about the source for various statistics based on hypervisor type:

Table 22: Source for Displayed Statistics

Hypervisor Type	Statistics	Source	Analysis
ESXi	Overview, VM, and Storage	Both Hypervisor and controller *Controller for some storage statistics only*	Metric dependent
	Hardware	Disk	
Hyper-V	Overview, VM, and Storage	Controller	
	Hardware	Disk	
AHV	Overview, VM, and Storage	Controller	
	Hardware	Disk	
Citrix Hypervisor	Overview, VM, and Storage	Controller	
	Hardware	Disk	
Mixed (ESXi + AHV)	Overview, VM, and Storage	Hypervisor	
	Hardware	Disk	

Modifying UI Settings

About this task

By default, the logon page includes background animation, and Prism logs out the users automatically after the users have been idle for 15 minutes. You can disable the background animation, change the session timeout for users, and configure an override to the session timeout.

Procedure

1. Log in to Prism Element web console.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1921

2. Click the gear icon in the main menu and then select **UI Settings** under **Appearance** in the **Settings** page. The **UI Settings** dialog box appears.

3. To set different variations of the Prism UI background themes, select any of the following options from the **Prism Themes** drop-down menu. The UI changes cosmetically to reflect the selection.

   Important:

   - The Prism themes feature is currently in technical preview. You may encounter visual anomalies in few settings/views where the prism themes are not applied. For example, Licensing Settings. Nutanix recommends that you register a case on the support portal to report any anomalies
   - You are required to save your selection and refresh any open Prism tabs after changing a background theme.
   - The Prism themes setting is not a universal feature between Prism Central and Prism Element web console. The background themes need to be configured in Prism Central and Prism Element web console respectively.

   - Select **Light Theme** for light background with high contrast view. This is the default Prism background theme.
   - Select **Dark Theme** for dark background with high contrast view. A pop-up appears prompting you to click **Continue** to proceed.
   - Select **Auto (OS defined)** to apply background themes defined in the OS. A pop-up appears prompting you to click **Continue** to proceed. For example, if you have defined **Dark** mode in the OS setting, the Prism UI honors the setting and sets a dark background theme.

4. To disable the logon page background animation, clear the **Enable animated background particles** checkbox (or select it to enable).

   Clearing the **Enable animated background particles** checkbox in the Prism **UI Settings** dialog box disables the creation or drawing of particles entirely. This action stops the drawing of the particles on the Prism Element logon page.

   Note: This setting is not persistent. In other words, if the Prism service restarts, this setting is lost and must be disabled again.

   Disabling the particles allows you to conserve critical CPU resources that are used in creating and maintaining the particles.

   Note: Disabling or enabling this setting in Prism Element web console does not propagate to Prism Central or vice versa. The setting must be disabled in Prism Element web console and Prism Central UI separately.

   You can disable the particle animation from the logon page by clicking **Freeze space-time continuum!** at the right bottom of the logon page. This action stores a setting in the local browser to stop the animation. However, this action does not stop creation or drawing of the particles itself.

   Note: You can enable the particle animation by clicking **Engage the warp drive!** .

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1922

5. To customize the theme, background color, title text, or blurb text on the logon page, do the following:

   - Click **UI Settings** dialog box and simultaneously press the option key on the MAC system or Alt key on the Windows system. Options for customizing the theme, title text, and blurb text are displayed.
   - Select the theme from the options displayed for **Theme**. You can change the HEX codes to create your own custom gradient background color for the logon page.
   - In the **Title Text** field, enter the text to create your custom title.
   - In the **Blurb Text** field, enter the text to create your custom blurb text. This text is displayed below the password field.

Figure 18: UI Settings Window for customizing the theme, title text, and blurb text

6. To configure session timeout, do the following under **Security Settings**:

   - Select the session timeout for the current user from the **Session Timeout For Current User** drop-down list.
   - Select the default session timeout for all users (except an administrator) from the **DEFAULT SESSION TIMEOUT FOR NON-ADMIN USERS** drop-down list.
   - Select the appropriate option from the **SESSION TIMEOUT OVERRIDE FOR NON-ADMIN USERS** drop-down list to override the session timeout.

   Note: The timeout interval for an administrator cannot be set for longer than 1 hour.

7. Clear the **Disable 2048 game** checkbox to disable the 2048 game.
8. Click **Save** to save your changes.

Finding the AHV Version on Prism Element

You can see the installed AHV version in the Prism Element web console.

About this task

To view the AHV version installed on the host, do the following.

Procedure

1. Log in to Prism Element web console.
2. The **Hypervisor Summary widget** widget on the top left side of the **Home** page displays the AHV version.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1923

Finding the AOS Version Using Prism Element

To view the Nutanix AOS version running in the cluster, do the following:

Procedure

1. Log in to the Prism Element web console.
2. Click the dropdown next to the username in the top right corner.
3. Select the **About Nutanix** option.

   The **About Nutanix** window displays the AOS version along with the Nutanix cluster check (NCC) and Life Cycle Manager (LCM) version numbers.
4. Click the **Close** button to close the window.

Prism Licensing

Nutanix provides licenses you can apply to enable a variety of features.

The Prism Element web console and Nutanix Support Portal provide the most current information on your licenses. For more information on licenses, see the License Manager Guide.

Modifying Cluster Details

About this task

You can add or modify cluster parameters (cluster name, virtual IP address, and data services IP address) through the **Settings** menu.

Procedure

1. Log in to Prism Element web console.
2. In the main menu, either click the cluster name at the far left or click the gear icon in the main menu and then select **Cluster Details** in the **Settings** page.
   The **Cluster Details** window appears. It displays read-only fields for the cluster UUID (universally unique identifier), ID, incarnation ID, subnet, and encryption status values. It also contains editable fields for cluster name, FQDN, virtual IP configuration, and iSCSI data services IP address. The cluster ID remains the same for the life of the cluster, but the incarnation ID is reset (typically to the wall time) each time the cluster is re-initialized.
3. In the **Cluster Name** field, enter (or update) a name for the cluster.

   The default name is simply Unnamed. Providing a custom name is optional but recommended.
4. In the **FQDN** field, enter the fully qualified domain name (FQDN) for the cluster.

   This requires an administrator to configure the domain name in the DNS server to resolve to all the external IPs of the Nutanix Controller VMs.
5. In the **Virtual IP** field, enter an IP address that will be used as a virtual IP for the cluster.

   A Controller VM runs on each node and has its own IP address, but this field sets a logical IP address that always connects to one of the active Controller VM in the cluster (assuming at least one is active), which removes the need to enter the address of a specific Controller VM. The virtual IP address is normally set

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1924

during the initial cluster configuration, but you can update the address at any time through this field. For more information, see Field Installation Guide.

> **Caution:** All the features that use the cluster virtual IP address will be impacted if you change that address. For more information, see Virtual IP Address Impact on page 75.

> **Note:** You are not required to configure either a virtual IP or a domain name, but configuring both provides better addressing flexibility.

6. In the **Virtual IPv6** field, enter an IPv6 address that will be used as a virtual IPv6 address for the cluster.

   A Controller VM runs on each node and has its own IPv6 address, but this field sets a logical IPv6 address that always connects to one of the active Controller VM in the cluster (assuming at least one is active), which removes the need to enter the address of a specific Controller VM. The virtual IPv6 address is normally set during the initial cluster configuration, but you can update the address at any time through this field. For more information, see Field Installation Guide.

7. In the **ISCSI Data Services IP Address** field, enter (or update) an IP address for use with Nutanix Volumes and other data services applications.

   > **Caution:** For certain features, changing the external data services IP address can result in unavailable storage or other issues. The features in question include Volumes, Calm, Leap, Karbon, Objects, and Files. For more information, see KB 8216 and iSCSI Data Services IP Address Impact on page 76.

8. To disable the Recycle Bin, clear (unselect) **Retain Deleted VMs for 24h**.

   When you disable the Recycle Bin, AOS automatically deletes any entities in the Recycle Bin after 24 hours. Any entities you delete after disabling the Recycle Bin are marked for deletion as soon as possible and are not stored in the storage container Recycle Bin folder. For more information, see Recycle Bin on page 152.

9. To enable the Recycle Bin, select **Retain Deleted VMs for 24h**.

   If you enable the Recycle Bin and then delete a guest VM or volume group vDisk, it retains its contents (deleted vDisks and configuration information) for up to 24 hours, unless the cluster free storage space reaches critical thresholds.

10. When the field entries are correct, click the **Save** button to save the values and close the window.

Virtual IP Address Impact

Any Nutanix feature that uses the virtual IP address might be adversely affected if you change the cluster virtual IP address.

- You can no longer manage a Nutanix cluster (Hyper-V) through the System Center Virtual Machine Manager (SCVMM).
- Nutanix data protection service might lose connection if you configured the remote site using the virtual IP address of that cluster.
- All the VMs running the NGT (Nutanix guest tools) instance will be affected. For information about NGT reconfiguration, see Reconfiguring NGT on page 321.
- External machines mounting shares from Nutanix might fail if the virtual IP address is used for HA functionality (as recommended).
- Some products such as Nutanix Objects use the virtual IP address for access. Check your product-specific documentation before changing the virtual IP address.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1925

iSCSI Data Services IP Address Impact

To provide access to cluster storage, Nutanix Volumes utilizes an iSCSI data services IP address to clients for target discovery which simplifies external iSCSI configuration on clients. This iSCSI data services IP address acts as an iSCSI target discovery portal and initial connection point.

Nutanix does not recommend configuring iSCSI client sessions to connect directly to Controller VM IP addresses. The data services address is owned by one Controller VM at a time. If the owner Controller VM becomes unavailable, the address moves to another Controller VM, ensuring that it is always available.

This IP address is also used as a cluster-wide address by clients configured as part of Nutanix Files and other products. This IP address:

- Should be in the same subnet as the cluster Controller VM IP `eth0` network interface addresses
- Helps load balance storage requests
- Enables path optimization in the cluster, preventing bottlenecks
- Eliminates the need for configuring a multipathing service such as Microsoft multipath I/O (MPIO)

Nutanix recommends setting the iSCSI data services IP address once for each cluster, but you can change it if needed through the **Cluster Details** window in the Prism Element web console. For more information, see Modifying Cluster Details on page 74.

If you change the iSCSI data services IP address, you will need to reconfigure any clients to use the new IP address.

- Log out of or disconnect from existing iSCSI or Nutanix Files sessions.
- Delete the old IP address if necessary.
- Re-discover the new target or reestablish Nutanix Files sessions.

> **Caution:** For certain features, changing the external data services IP address can result in unavailable storage or other issues. The features in question include Volumes, Calm, Leap, Karbon, Objects, and Files. For more information, see KB 8216.

Cluster Fault Tolerance Configuration

This section provides information on how to configure cluster fault tolerance.

You can configure cluster fault tolerance in the following ways:

- When you create a new cluster using Prism Central. For more information, see Creating a Cluster in the *Prism Central Infrastructure Guide*.
- When you configure a cluster using Foundation. For more information see Configuring the Foundation GUI Automatically and Configuring Foundation VM by Using the Foundation GUI in the *Field Installation Guide* or Run Foundation Central in the *Foundation Central Guide*.
- When you create a new cluster using nCLI. For more information, see Command Reference Guide.

For information on the types of cluster fault tolerance, see Cluster Fault Tolerance on page 25.

Increasing the Cluster Fault Tolerance Level

You can increase the fault tolerance of a cluster from 1N/1D to 2N/2D. This topic describes how to increase cluster fault tolerance.

Before you begin

- Ensure that the cluster has a minimum of five nodes.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1926

- You cannot increase the fault tolerance of a cluster from 1N/1D to 1N&1D. The 1N&1D cluster fault tolerance must be configured when you create the cluster.
- You cannot increase the fault tolerance of a cluster with 1N&1D fault tolerance.
- If you enable block fault tolerance in addition to increasing the cluster fault tolerance you need a minimum of 5 blocks.
- Increasing the cluster fault tolerance might require at least 30 percent of your disk space.
- You cannot revert the changes made to cluster fault tolerance or reduce the cluster fault tolerance. For example, you cannot reduce the cluster fault tolerance from 2N/2D to 1N/1D. If you attempt to reduce cluster fault tolerance, the Prism Element web console displays an error.
- For information on the types of cluster fault tolerance, see Cluster Fault Tolerance on page 25.

About this task

To increase the cluster fault tolerance, follow these steps:

> **Note:** A cluster with 2N/2D fault tolerance supports replication factor 3.

Procedure

1. Log in to the Prism Element web console.
2. From the dropdown menu on the left of the main menu, select **Settings**.
   The system displays the **Global Settings** page.
3. From the **Data Resiliency** section in the left navigation pane, click **Cluster Fault Tolerance**.
   The system displays the **Cluster Fault Tolerance** page.

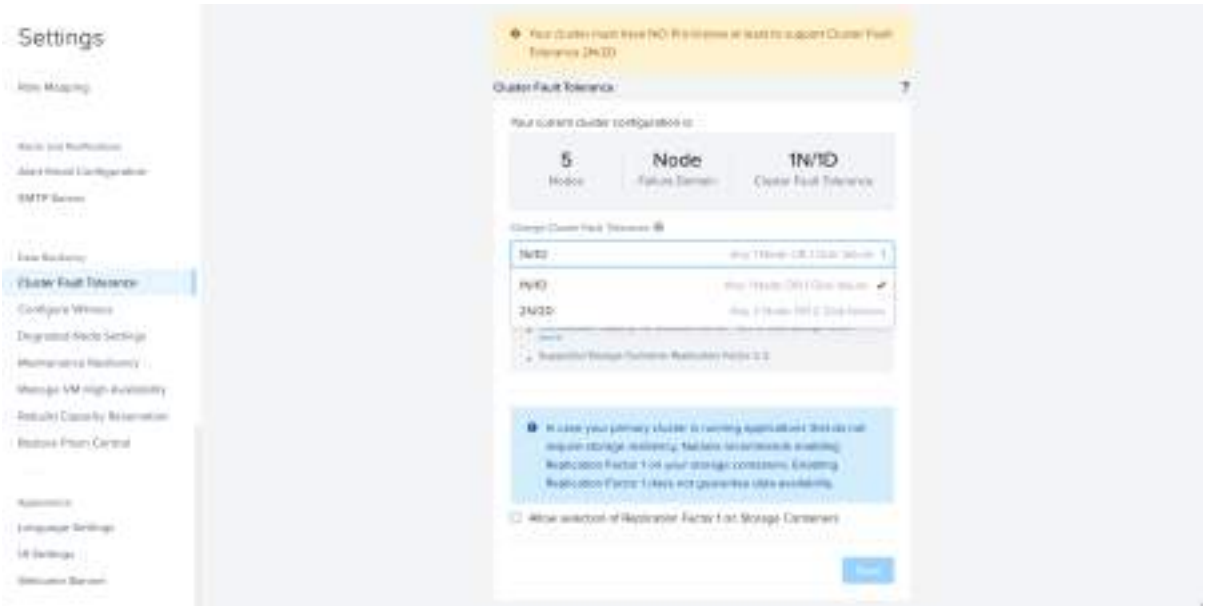


Figure 19: Increasing Cluster Fault Tolerance

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1927

4. From the **Change Cluster Fault Tolerance** dropdown menu, select **2N/2D**.
   The system increases the fault tolerance to 2N/2D and displays **Configured CFT : 2N/2D** in the **Cluster Resiliency / Fault Tolerance Status** widget in the dashboard of the Prism Element web console.

   > **Note:** The system might take a few hours to increase the cluster fault tolerance because it must replicate the metadata across the Cassandra ring.

What to do next

Set the replication factor to 3, manually, for every storage container you want to have three copies of the data.

Increasing the cluster fault tolerance without any increase in the replication factor provides granular control for a container without incurring the overhead of a third copy. However, this also means no container has a third copy of the data until you explicitly increase the replication factor for that container to 3.

For more information, see Increasing the Replication Factor using CLI on page 143.

Modifying Cluster Rebuild Preference

You can modify the cluster rebuild preference setting from the Prism Element web console.

Before you begin

For information on the types of cluster rebuild preferences, see Cluster Rebuild Preference on page 40.

About this task

To modify the cluster rebuild preference, follow these steps:

> **Note:** By default, the cluster rebuild preference is set as *Smart*.

Procedure

1. Log in to the Prism Element web console.
2. From the dropdown menu on the left of the main menu, select **Settings**.
   The system displays the **Global Settings** page.
3. From the **Data Resiliency** section in the left navigation pane, click **Maintenance Resiliency**.
   The system displays the **Maintenance Resiliency** page.
4. Perform one of the following:
   - » Clear the **Smart Rebuild** checkbox to modify the cluster rebuild preference to Immediate.
   - » If cleared, select the **Smart Rebuild** checkbox to modify the cluster rebuild preference to Smart.
5. Click **Save**.
   The system updates the cluster rebuild preference based on your choice.

Software and Firmware Upgrades

You can only upgrade ESXi and Hyper-V hypervisor, File, and File Server through the Prism Element web console **Upgrade Software** feature (also known as 1-click upgrade).

For other firmware and software component upgrades, see Life Cycle Manager Guide.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1928

Note: Starting with LCM 2.7, Foundation upgrades are exclusively performed through LCM. The one-click upgrade for Foundation has been disabled; the Foundation tab under **Settings** > **Upgrade Software** is not present anymore.

Life Cycle Management (LCM)

The life cycle manager (LCM) tracks software and firmware versions of the various components in a cluster. It allows you to view information about the current inventory and update the versions as needed. To view the LCM dashboard, select **LCM** from the drop-down list on the left of the main menu. For more information, see the Life Cycle Manager Guide.

Nutanix Cluster Check (NCC)

Before doing any upgrade procedure, run Nutanix Cluster Check from Prism Element and Prism Central.

Run NCC on Prism Element Clusters

- For Prism Element clusters, run the NCC checks from the **Health** dashboard of the Prism Element web console. You can select to run all the checks at once, the checks that have failed or displayed some warning, or even specific checks of your choice. You can also log on to a Controller VM and run NCC from the command line.
- if you are running checks by using Prism Element web console, you are unable to collect the logs at the same time.
- You can also log on to a Controller VM and run NCC from the ncc command line.

Run NCC on Prism Central

For Prism Central clusters, log on to the Prism Central VM through a secure shell session (SSH) and run the NCC checks using the ncc command line. You cannot run NCC from the Prism Central web console. For more information, see *Prism Central Infrastructure Guide*.

Running NCC (Prism Element)

About this task

Before doing any upgrade procedure, run Nutanix Cluster Check from the Prism Element web console or ncc command line.

Procedure

Do these steps to run NCC from the Prism Element web console.

a. In the Health dashboard, from the **Actions** drop-down menu, select **Run Checks**.

b. Select the checks that you want to run for the cluster.

- **All checks**. Select this option to run all the checks at once.
- **Only Failed and Warning Checks**. Select this option to run only the checks that failed or triggered a warning during the health check runs.
- **Specific Checks**. Select this option and type the check or checks name in the text box that appears that you want to run.

This field gets auto-populated once you start typing the name of the check. The **Added Checks** box lists all the checks that you have selected for this run.

c. Select the **Send the cluster check report in the email** option to receive the report after the cluster check.

To receive the email, ensure that you have configured email configuration for alerts. For more information, see the Prism Element web console Guide.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1929

The status of the run (succeeded or aborted) is available in the **Tasks** dashboard. By default, all the event triggered checks are passed. Also, the **Summary** page of the **Health** dashboard updates with the status according to health check runs.

Run NCC from the Controller VM Command Line

Procedure

Do these steps to run NCC by using the ncc command.

a. Log on to a Controller VM.

b. Run NCC. See Displaying NCC Help on page 80 to display NCC help.

```
nutanix@cvm$ ncc health_checks run_all
```

If the check reports a status other than INFO or PASS, resolve the reported issues before proceeding. If you are unable to resolve the issues, contact Nutanix Support for assistance.

Displaying NCC Help

Get help about NCC from the command line. You can also run the NCC checks from the **Health** dashboard of the Prism Element web console. Click **Actions** > **Manage Checks**, then select an NCC check. Click the link to the Knowledge Base article for more information about that check.

Procedure

- Show top-level help about available health check categories.

```
nutanix@cvm$ $ ncc health_checks
```

- Show top-level help about a specific available health check category. For example, hypervisor_checks.

```
nutanix@cvm$ ncc health_checks hypervisor_checks
```

- Show all NCC flags to set your NCC configuration. Use these flags under the direction of Nutanix Support.

```
nutanix@cvm$ ncc -help
```

Use Upgrade Software in the Prism Element Web Console (Legacy 1-Click Upgrade)

Prism Element support specific software upgrades that you can apply through the Prism Element web console **Upgrade Software** feature (also known as 1-click upgrade).

You can view the available upgrade options, start an upgrade, and monitor upgrade progress through the web console. In the main menu, click the gear icon, and then select **Upgrade Software**.

This page enables you to upgrade the following software when you cannot or choose not to use LCM.

- File
- File Server
- VMware ESXi or Microsoft Hyper-V hypervisors (use LCM to upgrade AHV)

- **CURRENT VERSION** displays the version running currently in the cluster.
- **AVAILABLE COMPATIBLE VERSIONS** displays any versions to which the cluster can be updated.
- The **upload the AOS base software binary** link enables you to install from binary and metadata files, which might be helpful for updating isolated (dark-site) clusters not connected to the Internet.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1930

- **Enable Automatic Download**. When you select **Enable Automatic Download**, the Prism Element web console regularly checks for new versions and downloads the software package for you. You can then choose to install it.

Options for Downloading Updates

> **Note:** You must allow access to the upgrade URLs in your firewall, listed in Firewall Best Practices in the *Security Guide*.

Nutanix recommends performing most upgrades through Life Cycle Manager (LCM) in the Prism Element web console. If you choose to upgrade individual cluster software components through **Settings** > **Upgrade Software** in the Prism Element web console, follow the recommended upgrade order as described in Recommended Upgrade Order for Dark Site Method section in *Life Cycle Manager Guide*.

You can choose how to obtain the latest versions of the AOS or other software that Nutanix makes available on the Nutanix Support portals. You might need to download software from hypervisor vendor release web pages.,

Table 23: Software Download Options

Downloadable Component	Automatic/On-Demand 1-Click Upgrade	File Upload 1-Click Upgrade
• File Server • File	• On demand: The Prism Element web console regularly checks for new versions and notifies you through **Upgrade Software** that a new version is available. Click **Download** to retrieve and install the software package.	• Nutanix Support Portal lists binaries, metadata, and checksums when available. You can upload the binary file and metadata to upgrade clusters.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1931

Downloadable Component	Automatic/On-Demand 1-Click Upgrade	File Upload 1-Click Upgrade
• Hypervisor	• On demand AHV: For most AOS versions, upgrade AHV by using the LCM, linked from **Upgrade Software** in the Prism Element web console. • On-demand is not available for ESXi. You can check the Nutanix Support portal for metadata JSONs for Nutanix-qualified ESXi versions. • On-demand is not available for Microsoft Hyper-V.	• Older AOS versions support AHV upgrades that you apply through **Settings** > **Upgrade Software** in the Prism Element web console • Nutanix Support Portal lists binaries, metadata, and checksums when available. You can upload the binary and metadata files to upgrade clusters. • Other hypervisor metadata files and checksums required to install hypervisor software are listed when available. • Hypervisor vendor web site. Hypervisor vendors such as VMware provide upgrade packages. For example, you can download the metadata file from Nutanix and hypervisor binary package from VMware and then upload the files through **Upgrade Software** to upgrade cluster hosts. See Upgrading ESXi Hosts by Uploading Binary and Metadata Files on page 84 or Upgrading Hyper-V Hosts by Uploading Binary and Metadata Files on page 88 for more information.

AOS Upgrade

To upgrade your cluster to AOS 6.8 or later versions, you must use LCM. However, you must upgrade LCM at your site to the latest version before you upgrade AOS. For more information, see LCM Updates in the *Life Cycle Manager Guide*.

> **Note:** Starting with LCM 3.0, 1-click upgrade for AOS is deprecated.

ESXi Upgrade

These topics describe how to upgrade your ESXi hypervisor host through the Prism Element web console **Upgrade Software** feature (also known as 1-click upgrade). For information on how to install or upgrade VMware vCenter server or other third-party software, see your vendor documentation.

AOS supports ESXi hypervisor upgrades that you can apply through the web console **Upgrade Software** feature (also known as 1-click upgrade).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1932

You can view the available upgrade options, start an upgrade, and monitor upgrade progress through the web console. Click **Settings** from the drop-down menu of the Prism Element web console, and select **Upgrade Software**. You can see the current status of your software versions and start an upgrade.

VMware ESXi Hypervisor Upgrade Recommendations and Limitations

- To install or upgrade VMware vCenter Server or other third-party software, see your vendor documentation.
- Always consult the VMware web site for any vCenter and hypervisor installation dependencies. For example, a hypervisor version might require that you upgrade vCenter first.
- If you have not enabled fully automated DRS in your environment and want to upgrade the ESXi host, you need to upgrade the ESXi host manually. For LCM upgrades on the ESXi cluster, it is recommended to have a fully automated DRS, so that VM migrations can be done automatically. For information on fully automated DRS, see *Set a Custom Automation Level for a Virtual Machine* in the *VMware vSphere Documentation*. For information on how to upgrade ESXi hosts manually, see ESXi Host Manual Upgrade in the *vSphere Administration Guide*.
- Disable Admission Control to upgrade ESXi on AOS; if enabled, the upgrade process will fail. You can enable it for normal cluster operation otherwise.

  Nutanix Support for ESXi Upgrades

  Nutanix qualifies specific VMware ESXi hypervisor updates and provides a related JSON metadata upgrade file on the Nutanix Support Portal for one-click upgrade through the Prism Element web console **Software Upgrade** feature.

  Nutanix does not provide ESXi binary files, only related JSON metadata upgrade files. Obtain ESXi offline bundles (not ISOs) from the VMware web site.

  Nutanix supports the ability to patch upgrade ESXi hosts with versions that are greater than or released after the Nutanix qualified version, but Nutanix might not have qualified those releases. For more information, see the Nutanix hypervisor support statement in our Support FAQ. For updates that are made available by VMware that do not have a Nutanix-provided JSON metadata upgrade file, obtain the offline bundle and md5sum checksum available from VMware, then use the web console **Software Upgrade** feature to upgrade ESXi.

  Trusted Platform Module (TPM) 2.0 enabled hosts

  Before upgrading a host with Trusted Platform Module (TPM) 2.0 enabled, in a cluster running ESXi 7.0U2 and later versions, Nutanix recommends that you backup the recovery key created when encrypting the host with TPM. For information on how to generate and backup the recovery key, see *KB 81661* in the *VMware documentation*. Ensure you use this recovery key to restore the host configuration encrypted by TPM 2.0 if it fails to start after upgrading the host in the cluster. For information on how to restore an encrypted host, see *KB 81446* in the *VMware documentation*. If you don't have the recovery key, and if the host fails to start after an upgrade, contact Nutanix Support.

  Mixing nodes with different processor (CPU) types in the same cluster

  If you are mixing nodes with different processor (CPU) types in the same cluster, you must enable enhanced vMotion compatibility (EVC) to allow vMotion/live migration of VMs during the hypervisor upgrade. For example, if your cluster includes a node with a Haswell CPU and other nodes with Broadwell CPUs, open vCenter and enable VMware enhanced vMotion compatibility (EVC) setting and specifically enable EVC for Intel hosts.

  CPU Level for Enhanced vMotion Compatibility (EVC)

  AOS Controller VMs and Prism Central VMs require a minimum CPU micro-architecture version of Intel Sandy Bridge. For AOS clusters with ESXi hosts, or when deploying Prism Central VMs on any ESXi cluster: if you have set the vSphere cluster enhanced vMotion compatibility (EVC) level, the minimum level must be **L4 - Sandy Bridge**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1933

vCenter Requirements and Limitations

> **Note:** You might be unable to log in to vCenter Server as the /storage/seat partition for vCenter Server version 7.0 and later might become full due to a large number of SSH-related events. For information on the symptoms and solutions to this issue, see KB 10830.

- If your cluster is running the ESXi hypervisor and is also managed by VMware vCenter, you must provide vCenter administrator credentials and vCenter IP address as an extra step before upgrading. Ensure that ports 80 / 443 are open between your cluster and your vCenter instance to successfully upgrade.
- If you have just registered your cluster in vCenter. Do not perform any cluster upgrades (AOS, Controller VM memory, hypervisor, and so on) if you have just registered your cluster in vCenter. Wait at least 1 hour before performing upgrades to allow cluster settings to become updated. Also do not register the cluster in vCenter and perform any upgrades at the same time.
- Cluster mapped to two vCenters. Upgrading software through the web console (1-click upgrade) does not support configurations where a cluster is mapped to two vCenters or where it includes host-affinity must rules for VMs.

  Ensure that enough cluster resources are available for live migration to occur and to allow hosts to enter maintenance mode.

Mixing Different Hypervisor Versions

For ESXi hosts, mixing different hypervisor versions in the same cluster is temporarily allowed for deferring a hypervisor upgrade as part of an add-node/expand cluster operation, reimaging a node as part of a break-fix procedure, planned migrations, and similar temporary operations.

Upgrading ESXi Hosts by Uploading Binary and Metadata Files

Before you begin

Ensure that the following prerequisites are met before you upgrade the ESXi host through **Upgrade Software** in the Prism Element web console:

- For more information, see VMware ESXi Hypervisor Upgrade Recommendations and Limitations.
- For more information, see General Hypervisor Upgrade Recommendations section in *Life Cycle Manager Guide*.
- Follow the recommended upgrade order. For more information, see Recommended Upgrade Order for Dark Site Method section in *Life Cycle Manager Guide*.
- For more information on how to install or upgrade VMware vCenter server or other third-party software, see your vendor documentation.

About this task

To download Nutanix-qualified ESXi metadata .JSON files and upgrade the ESXi hosts through **Upgrade Software** in the Prism Element web console, perform the following steps. Nutanix does not provide ESXi binary files, only related JSON metadata upgrade files.

Procedure

1. Before performing any upgrade procedure, make sure you are running the latest version of the Nutanix Cluster Check (NCC) health checks and upgrade NCC if necessary.
2. Run NCC. For more information, see Running NCC (Prism Element) in *Prism Element Web Console Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1934

3. Log on to the Nutanix support portal and navigate to the Hypervisors Support page from the **Downloads** menu, then download the Nutanix-qualified ESXi metadata .JSON files to your local machine or media.

   a. The default view is **All**. From the drop-down menu, select **Nutanix - VMware ESXi**, which shows all available JSON versions.

   b. From the release drop-down menu, select the available ESXi version. For example, **7.0.0 u2a**.

   c. Click **Download** to download the Nutanix-qualified ESXi metadata .JSON file.

4. Log in to the Prism Element web console for any node in the cluster.

5. Click **Settings** from the drop-down menu of the Prism Element web console, and select **Upgrade Software** > **Hypervisor**.

6. Click the **upload the Hypervisor binary** link.

7. Click **Choose File** for the metadata JSON (obtained from Nutanix) and binary files (offline bundle zip file for upgrades obtained from VMware), respectively, browse to the file locations, select the file, and click **Upload Now**.

8. When the file upload is completed, click **Upgrade** > **Upgrade Now**, then click **Yes** to confirm.

   [Optional] To run the pre-upgrade installation checks only on the Controller VM where you are logged on without upgrading, click **Upgrade** > **Pre-upgrade**. These checks also run as part of the upgrade procedure.

9. Type your vCenter IP address and credentials, then click **Upgrade**.

   Ensure that you are using your Active Directory or LDAP credentials in the form of domain\username or username@domain.

   > **Note:** AOS can detect if you have uploaded software that is already installed or upgraded. In this case, the **Upgrade** option is not displayed, because the software is already installed.

   The **Upgrade Software** dialog box shows the progress of your selection, including status of pre-installation checks and uploads, through the **Progress Monitor**.

10. On the **LCM** page, click **Inventory** > **Perform Inventory** to enable LCM to check, update and display the inventory information.

    For more information, see Performing Inventory with Life Cycle Manager section in the *Life Cycle Manager Guide*.

Upgrading ESXi by Uploading An Offline Bundle File and Checksum

About this task

- Do the following steps to download a non-Nutanix-qualified (patch) ESXi upgrade offline bundle from VMware, then upgrade ESXi through **Upgrade Software** in the Prism Element web console.
- Typically you perform this procedure to patch your version of ESXi and Nutanix has not yet officially qualified that new patch version. Nutanix supports the ability to patch upgrade ESXi hosts with versions that are greater than or released after the Nutanix qualified version, but Nutanix might not have qualified those releases.

Procedure

1. From the VMware web site, download the offline bundle (for example, update-from-esxi6.0-6.0_update02.zip) and copy the associated MD5 checksum. Ensure that this checksum is obtained from the VMware web site, not manually generated from the bundle by you.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1935

2. Save the files to your local machine or media, such as a USB drive or other portable media.
3. Log on to the Prism Element web console for any node in the cluster.
4. Click **Settings** from the drop-down menu of the Prism Element web console, and select **Upgrade Software** > **Hypervisor**.
5. Click the **upload the Hypervisor binary** link.
6. Click **enter md5 checksum** and copy the MD5 checksum into the **Hypervisor MD5 Checksum** field.
7. Scroll down and click **Choose File** for the binary file, browse to the offline bundle file location, select the file, and click **Upload Now**.
8. When the file upload is completed, click **Upgrade** > **Upgrade Now**, then click **Yes** to confirm.

   [Optional] To run the pre-upgrade installation checks only on the Controller VM where you are logged on without upgrading, click **Upgrade** > **Pre-upgrade**. These checks also run as part of the upgrade procedure.
9. Type your vCenter IP address and credentials, then click **Upgrade**.

   Ensure that you are using your Active Directory or LDAP credentials in the form of domain\username or username@domain.

   > **Note:** AOS can detect if you have uploaded software that is already installed or upgraded. In this case, the **Upgrade** option is not displayed, because the software is already installed.

   The **Upgrade Software** dialog box shows the progress of your selection, including status of pre-installation checks and uploads, through the **Progress Monitor**.

Hyper-V Upgrade

AOS supports hypervisor upgrades that you can apply through the Prism Element web console **Upgrade Software** feature (also known as 1-click upgrade).

You can view the available upgrade options, start an upgrade, and monitor upgrade progress through the web console. In the main menu, click the gear icon, and then select **Upgrade Software** in the **Settings** panel that appears, to see the current status of your software versions (and start an upgrade if warranted).

Hyper-V Hypervisor Upgrade Recommendations, Requirements, and Limitations

This section provides the requirements, recommendations, and limitations to upgrade Hyper-V.

Recommendations

Nutanix recommends that you schedule a sufficiently long maintenance window to upgrade your Hyper-V clusters.

Budget sufficient time to upgrade: Depending on the number of VMs running on a node before the upgrade, a node could take more than 1.5 hours to upgrade. For example, the total time to upgrade a Hyper-V cluster from Hyper-V 2016 to Hyper-V 2019 is approximately the time per node multiplied by the number of nodes. Upgrading can take longer if you also need to upgrade your AOS version.

Requirements

> **Note:**
>
> - You can upgrade to Windows Server 2022 Hyper-V only from a Hyper-V 2019 cluster.
> - Upgrade to Windows Server 2022 Hyper-V from an LACP-enabled Hyper-V 2019 cluster is not supported unless the Hyper-V vSwitch bound/team is set to Switch Embedded Teaming (SET). For more information, see KB 11220.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1936

- Direct upgrade to Windows Server 2022 Hyper-V from Hyper-V 2016 or Windows Server 2012 R2 is not supported.
- Foundation version 5.2.2 is the minimum supported version for upgrade to Windows Server 2022.
- For Windows Server 2022 Hyper-V, only NX Series G6 and later models are supported.
- For Windows Server 2022 Hyper-V, SET is the default teaming mode. LBFO teaming is not supported on Windows Server 2022 Hyper-V.
- For Hyper-V 2019, if you do not choose LACP/LAG, SET is the default teaming mode. NX Series G5 and later models support Hyper-V 2019.
- For Hyper-V 2016, if you do not choose LACP/LAG, the teaming mode is Switch Independent LBFO teaming.
- For Hyper-V (2016 and 2019), if you choose LACP/LAG, the teaming mode is Switch Dependant LBFO teaming.

- Before upgrading, ensure that the Active Directory user account has the necessary permissions to add and remove Active Directory objects.
- The platform must not be a light-compute platform.
- Before upgrading, disable or uninstall third-party antivirus or security filter drivers that modify Windows firewall rules. Windows firewalls must accept inbound and outbound SSH traffic outside of the domain rules.
- Enable Kerberos when upgrading from Windows Server 2012 R2 to Windows Server 2016. For more information, see Enabling Kerberos for Hyper-V.

  Note: Kerberos is enabled by default when upgrading from Windows Server 2016 to Windows Server 2019.

- Enable virtual machine migration on the host. Upgrading reimages the hypervisor. Any custom or non-standard hypervisor configurations could be lost after the upgrade is completed.
- If you are using System Center for Virtual Machine Management (SCVMM) 2012, upgrade to SCVMM 2016 first before upgrading to Hyper-V 2016. Similarly, upgrade to SCVMM 2019 before upgrading to Hyper-V 2019 and upgrade to SCVMM 2022 before upgrading to Windows Server 2022 Hyper-V.
- Upgrade using ISOs and Nutanix JSON File
  - Upgrade using ISOs. The Prism Element web console supports 1-click upgrade (**Upgrade Software** dialog box) of Hyper-V 2016, 2019, or 2022 by using metadata upgrade JSON file. This file is available in the Nutanix Support portal Hypervisor Details page and the Microsoft Hyper-V ISO file.
  - The Hyper-V upgrade JSON file, when used on clusters where Foundation 4.0 or later is installed, is available for Nutanix NX series G4 and later, Dell EMC XC series, or Lenovo Converged HX series platforms. You can upgrade hosts to Hyper-V 2016, 2019 (except for NX series G4) on these platforms by using this JSON file.

Limitations

- When upgrading hosts to Hyper-V 2016, 2019, and later versions, the local administrator user name and password is reset to the default administrator name Administrator and password of nutanix/4u. Any previous changes to the administrator name and/or password are overwritten.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1937

- VMs with any associated files on local storage are lost.
  - Logical networks are not restored immediately after upgrade. If you configure logical switches, the configuration is not retained and VMs could become unavailable.
  - Any VMs created during hypervisor upgrade (including as part of disaster recovery operations) and not marked as HA (High Availability) experiences unavailability.
  - Disaster recovery: VMs with the Automatic Stop Action property set to *Save* is marked as *CBR Not Capable* if they are upgraded to version 8.0 after upgrading the hypervisor. Change the value of Automatic Stop Action to *ShutDown* or *TurnOff* when the VM is upgraded so that it is not marked as *CBR Not Capable*
- Enabling Link Aggregation Control Protocol (LACP) for your cluster deployment is supported when upgrading hypervisor hosts from Windows Server 2016 to 2019.

Upgrading Hyper-V Hosts by Uploading Binary and Metadata Files

This procedure enables you to update Hyper-V through the Prism Element web console **Upgrade Software** dialog box.

Before you begin

Ensure that the following prerequisites are met before you upgrade the Hyper-V hosts:

- Check the Hyper-V Hypervisor Upgrade Recommendations, Requirements, and Limitations on page 86.
- Check the General Hypervisor Upgrade Recommendations section in *Life Cycle Manager Guide*.
- Follow the recommended upgrade order. For more information, see Recommended Upgrade Order for Dark Site Method section in *Life Cycle Manager Guide*.
- Ensure that the latest version of the Nutanix Cluster Check (NCC) health checks is installed and upgrade NCC if necessary.

Procedure

1. Run NCC as described in Running NCC (Prism Element) on page 79.
2. Download the Microsoft Hyper-V Windows Server .ISO file from the Microsoft web site.
3. Log on to the Nutanix support portal and select the hypervisor metadata .JSON file from the **Downloads** menu.
4. Save the files to your local machine or media, such as a USB drive or other portable media.
5. Log in to Prism Element web console.
6. Click the gear icon in the main menu of the web console, select **Upgrade Software** in the **Settings** page, and then click the **Hypervisor** tab.
7. Click the **upload a Hypervisor binary** link.
8. Click **Choose File** for the metadata and binary files, respectively, browse to the file locations, select the file, and click **Upload Now**.
9. [Optional] When the file upload is completed, to run the pre-upgrade installation checks only on the Controller VM where you are logged on without upgrading, click **Upgrade** > **Pre-upgrade**. These checks also run as part of the upgrade procedure.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1938

10. When the file upload is completed, click **Upgrade** > **Upgrade Now**, then click **Yes** to confirm.

    > **Note:** AOS can detect if you have uploaded software that is already installed or upgraded. In this case, the **Upgrade** option is not displayed, because the software is already installed.

    The **Upgrade Software** dialog box shows the progress of your selection, including status of pre-installation checks and uploads, through the **Progress Monitor**.

11. On the **LCM** page, click **Inventory** > **Perform Inventory** to enable LCM to check, update and display the inventory information.

    For more information, see Performing Inventory with Life Cycle Manager section in the *Life Cycle Manager Guide*.

View Task Status

The web console displays detailed information about all tasks that have been performed on the cluster.

Task Page Navigation

- To view the Task dashboard, log in to Prism Element web console, and select **Home** > **Tasks**.
- An icon also appears in the main menu when one or more tasks are active (running or completed within the last 48 hours). The icon appears blue when a task runs normally, yellow when it generates a warning, or red when it fails. Clicking the icon displays a drop-down list of active tasks; clicking the **View All Tasks** button at the bottom of that list displays a details screen with information about all tasks for this cluster.

  > **Note:** The drop-down list of active tasks may include a **Clean Up** button (top right). Clicking this button removes from the list any tasks that are no longer running. However, this applies to the current session only. The full active list (including the non-running tasks) appears when you open a new Prism Element web console session.

- When multiple tasks are active, you can filter the list by entering a name in the filter by field.
- You can also filter the list by clicking the **Filters** button and selecting the desired filter options

Each task appears in the list for a minimum of one hour after completion, but how long that task remains in the list depends on several factors. In general, the maximum duration is two weeks. However, tasks are rotated off the list as new tasks arrive, so a task might disappear from the list much sooner when activity is high. In some cases a task appears for longer than two weeks because the last task for each component is retained in the listing.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1939

View Task Status Dashboard

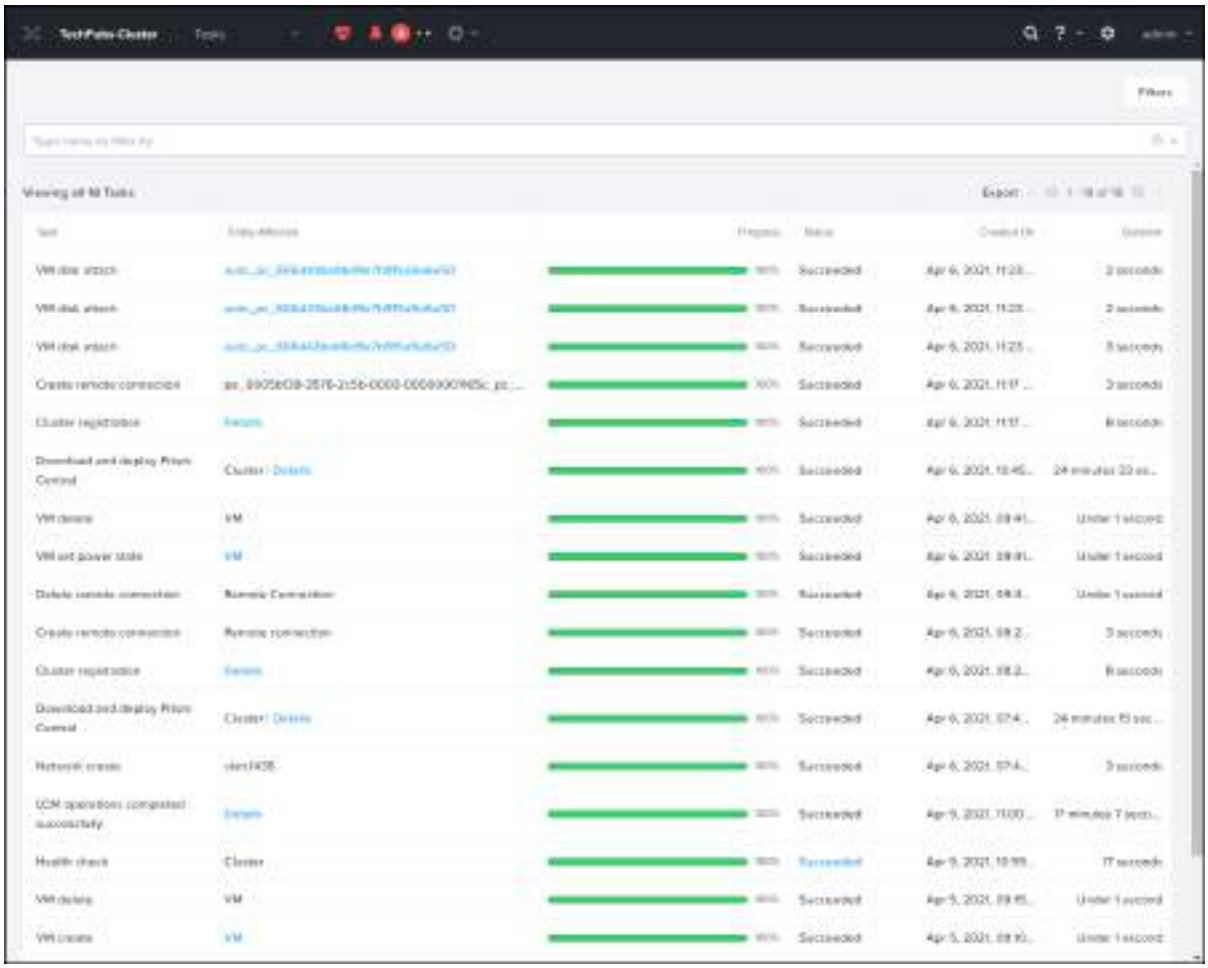


Figure 20: Task Dashboard

Table 24: Tasks List Fields

Parameter	Description	Values
Task	Specifies which type of operation the task is performing.	Any cluster operation you can perform in the Prism Element web console
Entity Affected	Display the entity on which task has been performed. If the link appears on the entity, click it to display the details.	Entity description
Percent	Indicates the current percentage complete for the task.	0%-100%
Status	Indicates the task status, which can be pending, running, completed, or failed.	pending, running,completed,failed
Created On	Displays when the task began.	seconds, minutes, hours

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1940

Parameter	Description	Values
Duration	Displays how long the task took to complete.	seconds, minutes, hours

Viewing the Progress of the Download or Upgrade Process

About this task

> **Note:** As part of the AOS upgrade, the node where you have logged on and initiated the upgrade restarts. The Prism Element web console appears unresponsive and might display the following message: Unable to reach server. Check for internet connectivity. Wait a few minutes and log on to the Prism Element web console again.

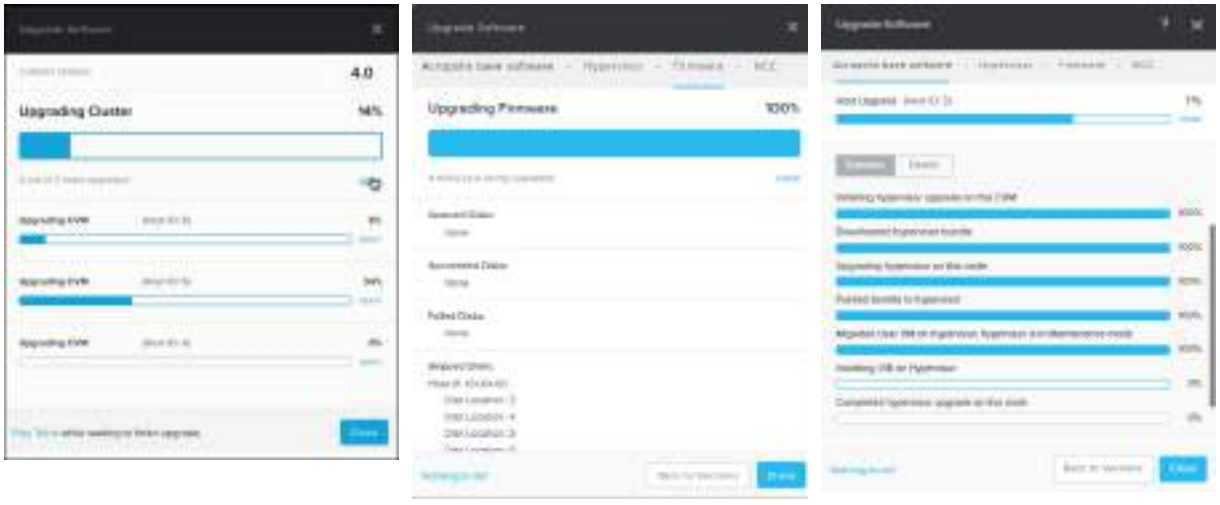
You can see the progress of the download or upgrade process through one of the following.

- LCM **Updates** page. For more information, see Life Cycle Manager Guide.
- **Upgrade Software** dialog box in Prism Element web console.
- **Alerts** summary on the main menu

Procedure

1. Log in to Prism Element web console.
2. Click the gear icon, and select **Upgrade Software**.
3. Under the **Upgrade Software** dialog box progress bar, click **Open**.
   The dialog box displays each Controller VM or disk as it progresses through the upgrade. For example:

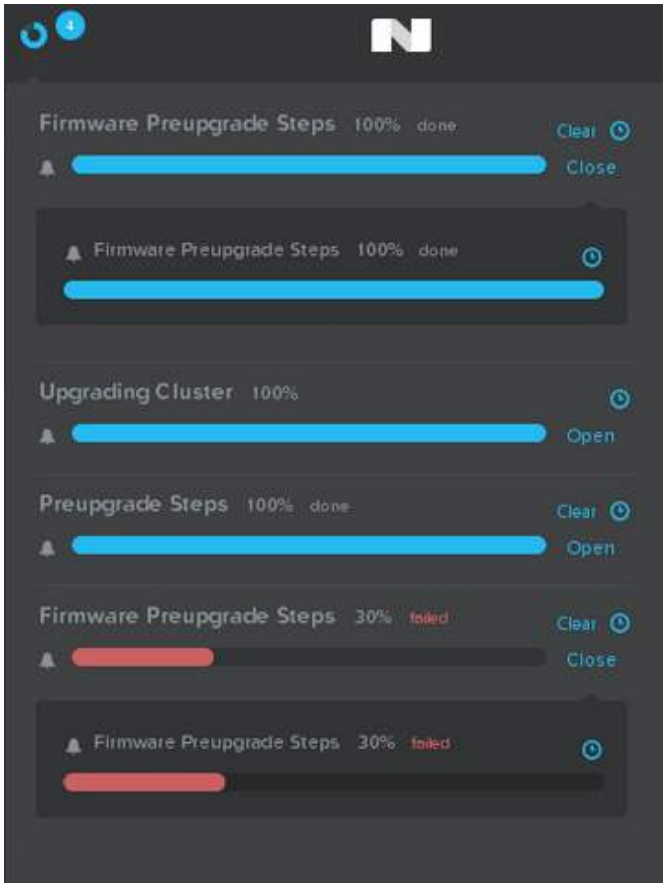
Table 25: Upgrade Progress



4. Click **open** to see progress including download, installation, and upgrade completion progress bars.
5. Click **Close** at any time; you can reopen the **Upgrade Software** dialog box from the main menu.
   If you click **Close**, the **Alerts** summary on the main menu also shows upgrade progress.
6. Click the **Alerts** summary on the main menu.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1941

7. Click **Open** to see progress details, including download, installation, and upgrade completion progress bars.



8. Hover your mouse pointer over the clock icon to see timestamps related to the upgrade task.

Pausing an In-Progress Download

Procedure

1. If a software download is in progress, do one of the following:
   - » Open **Upgrade Software** from the **Settings** page in the Prism Element web console.
   - » Click the **Alerts** summary on the main menu.
2. Click **Open** near the download progress bar.
3. Click the **Pause** icon to temporarily stop the download.
4. Click the **Play** icon to resume.

Deleting a Downloaded Image

About this task

In some cases, you might need to delete a downloaded software image. A pre-upgrade check fails if a corrupted image exists (for example, corrupted as the result of a transient network glitch). You might also delete an image and download it again to clear a pre-upgrade check error message. Another example is

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1942

when you want to download the image again for any reason. The upgrade feature reports that you have already downloaded an image, preventing you from downloading it again.

Procedure

1. Log on to the Controller VM where the image has been downloaded by using a secure shell session (SSH).
2. Change to the /home/nutanix/software_downloads/*download_type* directory, where *download_type* is software, hypervisor, or ncc.
3. Delete the image and retry to download it.

Multi-Cluster Management

Nutanix provides an option to monitor and manage multiple clusters through a single web console. The multi-cluster view, known as Prism Central, is a centralized management tool that runs as a separate VM. From the Prism Element web console, you can either register the cluster with an existing Prism Central instance or deploy a Prism Central instance and register the cluster with it.

Prism Central provides the following features:

- Single sign on for all registered clusters
- Summary dashboard across clusters that can be customized as desired
- Summary views for major entity types with drill-down options to view detailed information about individual entities
- Multi-cluster analytics capabilities
- Multi-cluster alerts summary with drill-down options to view information about possible causes and corrective actions for each alert
- Ability to configure individual clusters through direct Prism Central actions (for selected administrative tasks) or through one-click access to the web console for a cluster
- Prism Central Intelligent Operations
- Ability to configure network and security settings, data protection and recovery settings, and Prism Central management settings
- Performance monitoring, application discovery and monitoring, and reports management

For more information about Prism Central, refer to the Prism Central documentation. For information about how the Prism Central documentation is organized, see Prism Central Documentation Portfolio.

For information on how to install Prism Central using 1-click method, see Installing Prism Central Using 1-Click Method on page 93.

For information on how to register or unregister a cluster with Prism Central, see Registering or Unregistering a Cluster with Prism Central on page 98.

For information on how to backup and migrate Prism Central, see Prism Central Backup, Restore, and Migration in *Prism Central Infrastructure Guide*.

Installing Prism Central Using 1-Click Method

This section describes how to install Prism Central in Nutanix environment with a connected site (with internet connectivity) or dark site (without internet connectivity) setup.

Before you begin

Ensure that you meet the following prerequisites before you install Prism Central:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1943

- Check the Requirements for Prism Central Deployment and Limitations of Prism Central Deployment.
- Check the port requirements between Prism Central and Prism Element. For more information, see Ports and Protocols.
- Check the following requirements for the connected site (with internet connectivity) and dark site (without internet connectivity) environment.

Table 26: Prism Central Installation Requirements - Connected Site and Dark Site

Connected site	Dark Site

• The specified gateway must be reachable.
• Ensure the port TCP port 2100 is open from the Prism Element cluster to the Prism Central VM IP address. For the complete list of required ports, see Ports and Protocols.
• Ensure network connectivity between the VM VLAN and portgroup of the Prism Element cluster Controller VM and the Prism Central VM VLAN and portgroup.
• No duplicate IP addresses are used.
• The storage container used for deployment is mounted on all hypervisor hosts.
• When installing on an ESXi cluster:
  • vCenter and the ESXi cluster must be configured properly. For more information, see vSphere Administration Guide for Acropolis.
  • vCenter must be registered in Prism.
  • DRS must be enabled in vCenter.
  • vCenter is up and reachable during the deployment.
	Download Prism Central binary .TAR and metadata .JSON files from the Nutanix Support portal from a connected machine.
	1. Log in to the Downloads page for Prism Central.
	2. Click **Download** and **Metadata** to save the **Prism Central 1-click deploy from Prism Element** binary .TAR and metadata .JSON files, respectively, to your local media.
	You can also copy these files to a USB stick, CD, or other media.
	Note: Do not use the Prism Central OVA, ZIP, AHV image, or AOS binary .TAR.GZ and upgrade metadata JSON files from the Nutanix support portal to create this new Prism Central instance. Use the .TAR format binary and metadata .JSON files.
	The Prism Central OVA is used only to install or upgrade Prism Central in non-Nutanix ESXi environment. For more information, see Prism Central Installation in a Non-Nutanix ESXi Environment and Prism Central Upgrade in Non-Nutanix ESXi Environment.

About this task

Perform this procedure for both connected site (with internet connectivity) and dark site (without internet connectivity).

Procedure

1. Log in to the Prism Element web console as the user admin for your cluster.
2. Run NCC as described in Run NCC Checks .

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1944

3. Do one of the following:

   » On the **Home** dashboard, click **Register or create new** from the **Prism Central** widget.

   » Click the gear icon in the main menu and then select **Prism Central Registration** from the **Settings** menu.

4. In the first screen of the **Prism Central** dialog box, click the **Deploy** button.

   This screen includes two options, **Deploy** and **Connect**. For information on how to connect to an existing Prism Central instance using **Connect** option, see Registering or Unregistering a Cluster with Prism Central.

   > **Note:** On an ESXi cluster, you must first register a vCenter Server before you deploy a new Prism Central instance.

5. *(Applicable for Dark site only)* In the **PC Version** step of **Prism Central Deployment** screen, click the **Upload Installation Binary** link, select the Prism Central Metadata File (.json) and Prism Central Installation Binary (.tar) files, and click **Upload**.

   If there is already an image uploaded, the system displays the available versions.

6. *(Applicable for Connected site only)* In the **PC version** step of **Prism Central Deployment** screen, select the required Prism Central version you intend to install.

   Select **Show compatible versions** checkbox to view the list of PC versions compatible with the AOS cluster.

   > **Note:** If the Prism Central version you want to install does not appear in the list, typically because the cluster does not have Internet access (such as at a dark site), you can click the **Upload Installation Binary** link to upload an image from your local media as described in Step 5 on page 95.

7. Click **Next**.
   The **Scale type** step appears.

8. In the **Scale type** step, do one of the following:

   » To deploy a 1-VM instance of Prism Central, select **Deploy Single-VM PC** .

   » To deploy a 3-VM instance of Prism Central, select **Deploy Scale-Out PC (on 3-VMs)**.

   A Prism Central instance can consist of either a single VM or a set of three VMs. A 3-VM instance increases both the capacity and resiliency of Prism Central at the cost of maintaining the additional VMs. For information on Prism Central scalability, see the *Prism Central Scalability* topic in the release notes Prism Central version to be installed.

9. Click **Next**.
   The **Configuration** step appears

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1945

10. In the **Configuration** step, do the following in the indicated fields:

    a. Select (click the radio button for) the Prism Central VM size based on the number of guest VMs it must manage across all the registered clusters:

       For Prism Central configuration limits, see KB-8932 and Nutanix Configuration Maximums.

    b. **Network**: Select an existing network for this Prism Central instance from the list.

       If the target network is not listed, click the **Create Network** link to create a new network. For more information, see Network Management.

    c. **Subnet Mask**: Enter the subnet mask value.

    d. **Gateway**: Enter the IP address of the gateway.

    e. **DNS Address(es)**: Enter the IP address for one or more DNS servers. Enter multiple addresses in a comma separated list.

    f. **NTP Address(es)**: Enter the IP address for one or more NTP servers. Enter multiple addresses in a comma separated list.

    g. **Select a Container**: Select a container for the Prism Central VM from the drop-down list.

    h. *(Applicable for Scale-Out PC (on 3-VMs) only)* **Virtual IP**: Enter a virtual IP address for the Prism Central instance

       > **Note:** A virtual IP can be used as a single point of access for Prism Central. When you enter virtual IP, the IP addresses for the three PC VMs are populated automatically. You can keep those addresses or change them as desired.

       > **Important:** The virtual IP and FQDN are mutually exclusive in Prism Central. However, while installing Prism Central, you can only configure the virtual IP. After installing Prism Central, you can use either FQDN or virtual IP. For more information, see Managing Prism Central.
       >
       > To configure FQDN, the administrator must configure the domain name in the DNS server to resolve to all the external IPs of the Prism Central VMs.

    i. **VM Name**: Enter a name for the Prism Central VM.

    j. **IP**: Enter a static IP address for the Prism Central VM.

11. Click **Next**.
    The **Microservices** step appears.

12. In the **Microservices** step, do the following in the indicated fields:

    a. **Prism Central Service Domain Name**: Enter a unique domain name for the Prism Central Microservices. For more information, see *Prism Central Service Domain Name restrictions* in Microservices Infrastructure Prerequisites and Considerations.

    b. **Internal Network**: Select the network to use for Prism Central micro services communication from the dropdown list.

       The default selection **Private Network [default]** is a pre-configured private VxLAN network. Instead, if you want microservices infrastructure to use a different network, you can select the network (managed or

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1946

unmanaged) from the drop-down list. If the network you want microservices infrastructure to use does not appear in the list, you must first configure it. For more information, see Network Configuration.

c. The **Use default settings (recommended)** checkbox is available only when you have retained the default selection (**Private Network [default]**) for **Internal Network** in the preceding step. This checkbox is selected by default. Do one of the following:

- Retain the check mark for the **Use default settings (recommended)** checkbox and click **Validate**. (Go to step 12.d on page 97.)

  Retaining the check mark for the **Use default settings (recommended)** checkbox allows Prism Central to use the **Private Network [default]** with the default values for **Subnet Mask**, **Gateway IP Address** and **IP Address Range**.

- Clear the **Use default settings (recommended)** checkbox, if you want Prism Central to use the **Private Network [default]** setting with specific (non-default or custom) values for **Subnet Mask**, **Gateway IP Address** and **IP Address Range**.

Configure the **Internal Network** for microservices infrastructure if you did one of the following:

- Selected a managed or unmanaged network other than **Private Network [default]** for **Internal Network**.

  If you selected a managed network, the values in the **Subnet Mask**, **Gateway IP Address** and **IP Address Range** fields are already configured. If you selected an unmanaged network, you must enter the necessary values in the respective fields.

- Cleared the **Use default settings (recommended)** checkbox with the **Private Network [default]** selection for **Internal Network**.

Enter the values for the following parameters to configure **Internal Network**:

Parameter	Description
Subnet Mask	Enter the subnet mask.
Gateway IP Address	Enter the IP address for the gateway.
IP Address Range	Enter a range of IP addresses that the network can use. Enter a range of at least 10 available (unreserved) addresses for a 3-VM (scale out) Prism Central instance or at least 5 addresses for a 1-VM Prism Central instance. The addresses must be consecutive or sequential. For a managed network, the range of addresses for microservices infrastructure must be outside the range of reserved IP addresses (for example, DHCP IP Pool) in the selected network.

d. After you check that the values entered for all the fields are correct, click **Next**.

13. Click **Next**.
The **Summary** step appears.

14. In the **Summary** step, check the details entered for Prism Central installation, and click **Deploy**.
This begins the deployment process. On the **Home** page, the Prism Central widget displays **Deploying** until the installation is completed, then it displays **OK**. Click **OK** to launch the Prism Central web console in your browser.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1947

15. Monitor the deployment progress (1-VM or 3-VM Prism Central instances) from the **Tasks** page and view information about the deployed VMs through the **VM** dashboard. For more information, see Tasks View.

What to do next

you can expand your cluster, remove nodes, and enable services such as Self-service, Flow Network Security, and Intelligent Operations without registering the hosting cluster with Prism Central.

Register this cluster with Prism Central, if you want to manage this cluster through Prism Central. For more information about how to connect to an existing Prism Central instance, see Registering or Unregistering a Cluster with Prism Central.

Registering or Unregistering a Cluster with Prism Central

You need to register a cluster with Prism Central only if you want to manage the cluster through Prism Central.

Before you begin

- If you have never logged into Prism Central as the admin user, you must log in and change the password before you attempt to register a cluster with Prism Central. For more information, see Logging Into Prism Central.
- Do not enable client authentication in combination with ECDSA certificates on a registered cluster since it causes interference when communicating with Prism Central.
- Ports 9440 and 80 need to be open in both directions between the Prism Central VM and all the Controller VMs (and the cluster virtual IP address if configured) in each registered cluster. For the complete list of required ports, see Ports and Protocols.
- If you have a proxy server configured and you want the cluster - Prism Central communication to go through the proxy, open the relevant ports on the proxy. If you do not want the communication to go through the proxy, add the Prism Central IP address to the proxy whitelist (allowlist) in the cluster settings. For more information about configuring proxy, see Configuring HTTP Proxy on page 394. For the complete list of required ports, see Ports and Protocols.
- A cluster can register with just one Prism Central instance at a time. To register with a different Prism Central instance, first unregister the cluster.

About this task

To register a cluster with Prism Central, follow these steps:

> **Note:** To perform this task, ensure that you log in to the Prism Element web console as an admin user.

Procedure

1. Log in to the Prism Element web console on the target cluster.
2. To run Nutanix Cluster Checks, go to the **Health** dashboard, and from the **Actions** dropdown menu, click **Run Checks**.
3. Do either of the following:
   - » In the **Home** dashboard, click **Register or create new** from the **Prism Central** widget.
   - » Click the Settings icon, and navigate to **Setup** > **Prism Central Registration** in the **Settings** page.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1948

4. In the **Prism Central Registration** window, click **Connect**.

   The **Prism Central Registration** window provides two options: **Deploy** and **Connect**. This procedure describes how to connect to an existing Prism Central instance. For instructions on how to deploy a new Prism Central instance, see Installing Prism Central.

   A window appears outlining what services are available through Prism Element and Prism Central.

5. Click **Next** after reviewing the message.

6. Enter the following information:

   a. **Prism Central IP**: Indicates the IP address of the Prism Central VM.

   b. **Port**: The default port number is 9440. This is an optional field. For the complete list of required ports, see Ports and Protocols.

   c. **Username**: Indicates the user name for Prism Central. You can enter admin as the Prism Central user name.

   d. **Password**: Indicates the password for the Prism Central user.

7. Click **Connect** to save the values and close the window.
   The cluster is now registered with the specified Prism Central VM. After successful registration, the system allows passing information between the specified cluster and Prism Central.

   Note:

   - The user credentials provided when registering a cluster (Prism Element) with Prism Central are only used once. After registration, modifying the admin password would not impact any communication between Prism Central and the cluster.
   - On small, large, and x-large Prism Central deployments, when you register a new cluster to Prism Central, Prism Central synchronises the past 90 days of data (including multiple metrics) from the cluster. On x-small Prism Central deployments, Prism Central synchronises the past 2 hours of data (including multiple metrics) from the cluster. To view the list of metrics that are synced during registration, see the file */home/nutanix/config/arithmos/data_sender/arithmos_history.json* in the Controller VM. To view the list of metrics that are synced during a regular synchronisation between Prism Central and the cluster, see the file */home/nutanix/config/arithmos/data_sender/arithmos.json* in the Controller VM.

What to do next

Once your cluster is registered with Prism Central, you can configure various settings for network, security, and alerts. For more information, see Admin Center Settings Options.

Unregistering from Prism Central

Before you begin

Caution: Unregistering a cluster from Prism Central is not a supported workflow. The unregistered cluster might be disallowed for re-registration with a Prism Central instance.

You can use the destroy Cluster feature of Prism Central, which implicitly unregisters the cluster. For more information, see Destroying a Cluster.

If you still want to go ahead with unregistration of the cluster, consider the following points:

- Unregistering a cluster through the Prism Element web console is no longer available. This option is removed to reduce the risk of accidentally unregistering a cluster. Several features such as role-based access control,

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1949

application management, micro-segmentation policies, and self-service capability require Prism Central to run your clusters. If a cluster is unregistered from Prism Central, it leads to features unavailability and configuration erasure. You can only use the following procedure from Controller VM (CVM) to unregister a cluster.

- Perform the entire registration process, followed by the cleanup process.
- Do not remove the IPs of the cluster and Prism Central from the whitelists on both sides until the unregistration process completes successfully.

If you have enabled additional applications or features in Prism Central, see the following table for recommendations before you unregister a cluster. For more information, see KB 4944.

Table 27: Unregistering a cluster with additional applications enabled

Nutanix Disaster Recovery (Leap)	Before unregistering the cluster from Prism Central, you must remove any Nutanix Disaster Recovery (Leap) configuration involving virtual machines or volume groups for the cluster being unregistered. Otherwise you will not be able to manage the snapshot creation or replication policies configured on the cluster. For more information, see KB 12749. **Note:** Do not proceed with unregistration, if the stretch config (AHV Synchronous replication) is present.
Flow Networking	You must disable Flow Networking on the cluster before unregistering it from Prism Central, using the steps mentioned in Unregistering a PE from the PC in *Flow Virtual Networking Guide*. If Flow Networking is not disabled on the cluster prior to unregistering from Prism Central, attempts to enable Flow Networking in the same cluster does not work as expected. For more information, see KB 12449.
NuCalm/App Management	You must clean up Calm entities after unregistration. Contact Nutanix Support for assistance in cleaning up the CALM entities.
Prism Self Service configuration	Changes that have been made to the Prism Self Service configuration in Prism Central are lost after unregistration. Ensure that you follow the extra cleanup steps mentioned in KB 4944.
NKE Kubernetes	Do not unregister the cluster hosting an NKE Kubernetes cluster from Prism Central. Unregistration of cluster from Prism Central will prevent the management of the NKE clusters.

About this task

To unregister a cluster from an existing Prism Central instance, perform the following steps:

Procedure

1. Log in to any CVM of the registered cluster through an SSH session.
2. Run the cluster status command and verify that all services are in a healthy state.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1950

3. Run the following command to unregister the cluster from Prism Central.

```
nutanix@cvm$ ncli multicluster remove-from-multicluster external-ip-address-or-svm-ips=pc-name-or-ip username=pc-username password=pc-password
```

Replace *pc-name-or-ip* with the Prism Central name or IP address and *pc-username* and *pc-password* with the login credentials for your Prism Central administrator account. If the password contains any special characters, ensure to enclose the password in single quotes. This step can take some time (though typically just a few seconds).

If the unregistration process is successful at Prism Element cluster, you will see a task UUID in the command output. After you see the task UUID in the command output, wait for about 2 minutes to let the unregistration process complete at Prism Central.

4. Run the following command on Prism Element to verify if the cluster unregistration process is successful on Prism Element:

```
nutanix@cvm$ ncli multicluster get-cluster-state
```

The command output should list 0 as registered cluster count: Registered Cluster Count: 0

5. Run the following command on Prism Central to verify if the cluster unregistration process is successful on Prism Central:

```
nutanix@pcvm$ ncli multicluster get-cluster-state
```

If the command output does not include the name and UUID of the cluster you want to unregister, the unregistration process is successful. If the cluster information is still visible in the command output, refer to KB-4944 to troubleshoot the issue.

6. Run the following command to retrieve the UUID for the cluster:

```
nutanix@cvm$ ncli cluster info
```

The following output shows the **Cluster UUID** value in the cluster information output:

```
Cluster Id           : 586dd889-84dc-422f-b8e8-8ce3cd781dcf::4100682370753502671
    Cluster Uuid             : 586dd889-84dc-422f-b8e8-8ce3cd781dcf
    Cluster Name             : PC_10.51.147.185
    Cluster Version          : pc.2024.1
    Cluster Full Version     : el8.5-release-fraser-2024.1-stable-
ca1136cd25915d9b5635483235e1fd7af3ccddfb
    External IP address      : 10.51.147.185
    Is LTS                   : false
    External Data Services... :
    Support Verbosity Level  : BASIC_COREDUMP
    Lock Down Status         : Disabled
    Password Remote Login ... : Enabled
    Timezone                 : Atlantic/Reykjavik
    NCC Version              : ncc-5.0.0
    Degraded Node Monitoring  : Enabled
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1951

7. Log in to the Prism Central VM through an SSH session (as the *nutanix* user) and perform the following steps:

   a. Run the unregistration clean-up script.

   ```
   [pcvm]$ python /home/nutanix/bin/unregistration_cleanup.py uuid
   ```

   Replace *uuid* with the value you obtained in step 6 on page 101. This script removes all remaining registration information about that cluster and completes the unregistration process with the Prism Central VM.

   > **Note:** If you do not run the clean-up script, some artifacts continue to retain references to entities that are no longer managed by the cluster. Some artifacts that might have lost references due to the unregistration process might not be able to recover their references.

   b. Run the following command to retrieve the UUID for Prism Central:

   ```
   [pcvm]$ ncli cluster info
   ```

   Find the **Cluster UUID** value in the displayed information (see step 6 on page 101), which in this case is the UUID for Prism Central.

8. Go back to the CVM, and run the unregistration_cleanup.py script to complete the unregistration process on the cluster.

   ```
   nutanix@cvm$ python /home/nutanix/bin/unregistration_cleanup.py uuid
   ```

   In this case the *uuid* is the Prism Central UUID obtained in substep 7.b on page 102.

   If you do not encounter any error after running the cleanup script, you can consider that the cleanup is successful.

What to do next

Once the unregistration process is complete, you are not allowed to re-register the cluster with a new or re-created Prism Central instance. If you need to register the cluster again, see KB-15679 or contact Nutanix Support.

If the clean up process is not completed successfully, perform the following actions:

- Check the logs to indicate if there are any input errors when calling the script. The logs for the unregistration cleanup script are available under ~/data/logs/unregistration_cleanup.log.
- If any error occurred during script processing, run the cluster status command and check that the cluster services are up and running. Re-run the script and check if the script processes successfully.

> **Note:** If Prism Self Service is enabled and the unregistered cluster is set as the default cluster, you must update the default project to select a new (registered) cluster. For information about how to modify a project, see Modifying a Project information in *Prism Central Admin Center Guide*.

Restoring Prism Central (1-Click Recovery)

If you protected or backed up your Prism Central instance, you can use an AHV or ESXi cluster to restore the Prism Central instance. For continuous backups (backups stored on on-prem Nutanix clusters), you can recover the Prism Central instance from a registered cluster only. For point-in-time backups (backups stored on Amazon S3), you can recover the instance on a registered cluster, or you can recover it on a cluster that is not registered with any Prism Central instance.

Before you begin

Ensure that the Nutanix cluster you use to restore the Prism Central instance meets the following requirements.

- Registered to the protected Prism Central instance.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1952

- To restore from a continuous backup, the cluster must run AOS 6.5.3.1 or later. For more information on the supported AOS versions, see Compatibility and Interoperability Matrix.
- To restore from a point-in-time backup, the cluster must run AOS 6.8 or later. For more information on the supported AOS versions, see Compatibility and Interoperability Matrix.
- Configured with ISCSI data service IP address for efficient recovery of Nutanix Disaster Recovery or NCM Self-Service configurations.

> **Note:** The Nutanix cluster takes about 10 minutes to stabilize the Prism Central instance after the recovery task on the Prism Element web console is displayed as complete. This is because Microservices Infrastructure causes the system to rotate certificates after the restoration and restart services like IAM and Flow Virtual Networking.

About this task

> **Important:**
>
> After restoring your Prism Central instance, ensure that you manually restore Files to the pre-disaster version. For more information, see Manually Failing Over to a Remote Site in the *Files Manager User Guide*.
>
> Accessing Prism Central (PC) using APIs or any other alternative method is strongly discouraged until the restoration process has been fully completed, as such actions may lead to locking of PC username credentials resulting in subsequent login issues.

To restore a Prism Central instance, perform the following steps.

Procedure

1. Log in to any Prism Element web console registered to the Prism Central instance you want to restore.

   The Prism Element dashboard shows the Prism Central widget, which contains Prism Central information (IP address and connection status). If this is a fresh Prism Element that you created and you have yet to register to a Prism Central instance, it won't appear. Instead, you see the **Register or Deploy Prism Central**.

2. Click the Settings icon and navigate to **Data Resiliency** > **Restore Prism Central** from the **Settings** menu. For more information, see Settings Menu in the `Prism Element Web Console Guide`.
   The **Restore Prism Central** page appears. This page provides you options to restore the Prism Central instance from a Prism Element cluster or S3-compatible object storage.

3. Select from where you want to restore the Prism Central instance and click **Restore Now**.

   > **Note:** If you configured only continuous backup, the **Restore Now** option is available only when Prism Central is in a disconnected state(shown **Disconnected** in the Prism Element web console.

   The **Restore Prism Central** window appears. This window shows the service data that will be recovered and those that will not.

4. Click **Continue** and specify the following information according to the source from where you want to recover.

   » To recover from a continuous backup, see Restore Prism Central-Field Information for Continuous Backup on page 104.

   » To recover from a point-in-time backup, see Restore Prism Central-Field Information for S3-based Object Storage on page 105.

   The Prism Central instance is restored in 60 to 90 minutes, depending on the configuration data of the hosts. The restoration involves the deployment of Prism Central and the restoration of its configuration data from the backup, which can take anywhere between 60 and 120 minutes, depending on the size of the data. The restored

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1953

Prism Central instance takes an additional 30 to 40 minutes to show all the guest VMs, disks, and metrics. Wait to perform any actions on the restored Prism Central instance until all the recovery tasks are complete on the cluster. You can see the restoration status and the related processes in the **Tasks** window.

What to do next

Consider the following after the Prism Central restoration.

- Use the newly restored Prism Central instance only.

  If the old Prism Central instance becomes available, shut down or delete the old instance because running the old Prism Central instance can cause data corruption.

  > **Note:** If the Prism Central restoration fails, contact Nutanix Support. Do not bring up the old Prism Central instance.

- Reset the credentials.

  Prism Central restores with the default credentials. Nutanix recommends changing the default credentials. For information about changing the default credentials, see Logging Into Prism Central in the *Prism Central Infrastructure Guide*.

  > **Note:** If you have both S3-compatible object storage and Nutanix on-prem clusters configured as backup targets and you recovered the Prism Central instance through an on-prem cluster. In that case, you must reconfigure the s3 bucket credentials after the recovery through the **Prism Central Backup and Restore** widget in **Settings** > **Prism Central Management**.

- Reconfigure the proxy server. For information on how to configure the HTTP proxy through the Prism Central web console, see Configuring an HTTP Proxy in the *Prism Central Admin Center Guide*

  If the old Prism Central instance had a proxy server, reconfigure the proxy server so that the recovered Prism Central instance maps to the correct IP address.

- Reconfigure the fully qualified domain name (FQDN).

  If the old Prism Central instance had an FQDN, reconfigure the FQDN so that the recovered Prism Central instance maps to the correct IP address.

- Recovery plan jobs (RPJ) in progress: Perform the steps in KB-10962.

  If the old Prism Central instance had a failover task running (Nutanix Disaster Recovery) or protection policy with guest VMs protected with synchronous replication schedule, perform the steps in KB 10962 to ensure that all the failover tasks stuck in the running state are terminated and a script is executed for efficient recovery of the Prism Central instance.

- Reconfigure Life Cycle Manager (LCM) if you do not use the Nutanix portal or if you use LCM in the dark site. For information on how to configure LCM on a dark site, see LCM Settings for Dark Sites - No Internet Connectivity. For information on reconfiguration of LCM 3.1, see KB 17966.

Restore Prism Central-Field Information for Continuous Backup

Procedure

1. Select the cluster where you want to restore the Prism Central instance.
2. Verify the version of Prism Central instance that would restore on the selected cluster.
3. Select the network where you want to restore and install Prism Central instances.

   The **Subnet Mask**, **Gateway**, and **DNS Address(s)** fields show the relevant information associated with the selected network.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1954

4. Enter details (name, IP address) for the Prism Central instance you want to restore and click **Save**.
5. Review the summary and click **Recover**.

Restore Prism Central-Field Information for S3-based Object Storage

Procedure

1. In **Connect** tab, specify the following details, then click **Next**.
   a. **AWS Region Name**. Enter an AWS region name. For more information, see `AWS documentation`.
   a. **AWS Bucket Name**. Enter a bucket name. For more information, see `AWS documentation`.
   b. (Optional for NC2 environments) **Access Key**. Enter your access key.
   c. (Optional for NC2 environments) **Secret Access Key**. Enter your secret access key.
2. In **Source** tab, select the Prism Central backup you want to restore, and click **Next**.
   An S3 bucket can be used to back up multiple Prism Central instances. The instances are listed as the `PC_<IP_ADDRESS>` or the FQDN if configured.
3. In **Restore Point** tab, specify the date for the point-in-time backup, and then select one of the available restore points to restore the Prism Central instance and click **Next**.
4. In **Installation** tab, verify the cluster IP address where Prism Central instance was hosted originally and the version of your instance, and click **Next**.
5. In **Configuration** tab, specify the networking details and click **Next**.

   > **Note:** If you are restoring the Prism Central instance from the same cluster (Prism Element web console) where the Prism Central instance was hosted, details like **vLAN**, **Subnet Mask**, **Gateway IP**, **DNS Address(es)**, **NTP Address(es)**, **Container**, and **Virtual IP** are populated automatically. You must configure these details if you are trying to restore the Prism Central instance from a different AZ or a cluster.

6. In the **Microservices** tab, specify the Prism Central service domain name, internal network, and the required input to enable Microservices Infrastructure (CMSP). Nutanix recommends using the default settings for **Subnet Mask**, **Gateway IP Address**, and **IP Address Range**.

   > **Note:** Ensure that the IP address range does not conflict with the reserved DHCP IP address pool in your network.

7. In **Summary** tab, review the information you configured in the previous steps, and click **Restore**.

CVM Memory Configuration

Foundation provisions the default memory and vCPUs to each Controller VM (CVM) according to your platform category. After Foundation, you can increase the memory reserved for each Controller VM in your cluster by using the 1-click Controller VM Memory Upgrade feature available in the Prism Element web console. You might need to increase the Controller VM memory based on your cluster configuration.

CVM Field Specifications

For information about the minimum CVM configurations (CVM logical cores, CPU physical cores per socket, and vRAM) based on your platform category, see Controller VM (CVM) Field Specifications topic in *Acropolis Advanced Administration Guide*.

Foundation allocates the maximum resources to Controller VM (CVM) of the SO node as follows:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1955

- CVM vCPU = Number of physical host CPUs minus 2, limited to a maximum of 22 vCPUs.

  Note: This is applicable till Foundation version 5.3.x. From Foundation version 5.4 onwards, the capping of maximum 22 vCPUs is not applicable.

- CVM memory = Available RAM minus 16 GiB, limited to a maximum of 256 GiB.

  Note:

  - This is applicable from Foundation version 5.3 and above. In the earlier Foundation versions, the memory allocation happens without capping to 256 GiB.
  - A capping of maximum 256 GiB is applied, and Foundation allocates the maximum possible vRAM to CVM. For example, if the available RAM is 512 GiB, the system allocates a maximum of 256 GiB and never considers the 512-16 = 496 GiB value. However, if you change the system allocated vRAM, the vRAM gets overridden with the supplied value.

Note: Minimum Foundation version of 5.3 supports these limits with NUMA pinnings or alignments. Earlier Foundation versions with a minimum version of 5.0 support these limits but not NUMA pinnings or alignments.

Increasing the Controller VM Memory Size

Before you begin

Foundation allocates the maximum resources to Controller VM (CVM) of the SO node as follows:

- CVM vCPU = Number of physical host CPUs minus 2, limited to a maximum of 22 vCPUs.

  Note: This is applicable till Foundation version 5.3.x. From Foundation version 5.4 onwards, the capping of maximum 22 vCPUs is not applicable.

- CVM memory = Available RAM minus 16 GiB, limited to a maximum of 256 GiB.

  Note:

  - This is applicable from Foundation version 5.3 and above. In the earlier Foundation versions, the memory allocation happens without capping to 256 GiB.
  - A capping of maximum 256 GiB is applied, and Foundation allocates the maximum possible vRAM to CVM. For example, if the available RAM is 512 GiB, the system allocates a maximum of 256 GiB and never considers the 512-16 = 496 GiB value. However, if you change the system allocated vRAM, the vRAM gets overridden with the supplied value.

Note: Minimum Foundation version of 5.3 supports these limits with NUMA pinnings or alignments. Earlier Foundation versions with a minimum version of 5.0 support these limits but not NUMA pinnings or alignments.

About this task

Note:

- vCenter access details and credentials are required to update the CVM configuration. The details are encrypted on the CVM and removed after the update is complete.
- Nutanix does not support decreasing the CVM memory below the recommended minimum requirements.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1956

Perform the following procedure to increase the CVM memory in the Prism Element web console.

Procedure

1. Log in to the Prism Element web console.
2. Run NCC as described in Running Checks by Using Prism Element Web Console on page 261.
3. Click the gear icon in the main menu and then select **Configure CVM** in the **Settings** page.
   Prism Element web console displays the **Configure CVM** dialog box.
4. If your cluster is running the ESXi hypervisor and you are managing your cluster by using VMware vCenter Server, you must enter the vCenter authentication information to increase the CVM memory by performing the following steps:
   a. In the **Configure CVM** dialog box, click **Add vCenter**.
   b. Enter the vCenter Server IP address and administrator credentials.
   c. Click **Add**.
5. Select the **Target CVM Memory Allocation** memory size and click **Apply**.

   Note:

   - You can allocate a maximum CVM memory of 64 GB through the Prism Element web console. To upgrade the CVM memory beyond 64 GB, contact Nutanix support.
   - If a CVM was already allocated more memory than your choice, it remains at the allocated amount. For example, if a Controller VM is at 20 GB memory and you select 28 GB, the Controller VM memory is upgraded to 28 GB. However, if a Controller VM is at 48 GB memory and you select 28 GB, the Controller VM memory remains unchanged at 48 GB.

   AOS applies memory to each CVM that is below the amount you choose. Resizing memory for a CVM requires a restart. Only one CVM restarts at a time, thus preventing any production impact.

Resource Requirements Supporting Snapshot Frequency (Asynchronous, NearSync, and Metro)

For DR solutions with asynchronous, nearsync, and synchronous (using metro availability) replication schedules to succeed, the nodes must have certain resources.

For information on snapshot frequency requirements, see Resource Requirements Supporting Snapshot Frequency (Asynchronous, NearSync and Metro) information in the *Data Protection and Recovery with Prism Element Guide* or On-Prem Hardware Resource Requirements information in the *Nutanix Disaster Recovery Guide*.

Note: For metro availability, the synchronous replication is supported with snapshots generated every 6 hours. Any node that supports 6-hour snapshot retention can support synchronous replication with 0 seconds RPO. For more information, see Synchronous (0 seconds RPO) in *Nutanix Disaster Recovery Guide*.

Rebooting an AHV or ESXI Node in a Nutanix Cluster

About this task

The **Request Reboot** operation in the Prism Element web console gracefully restarts the selected nodes one after the other.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1957

Note: Reboot host is a graceful restart workflow. Hosts are automatically put into maintenance mode and all the user VMs are migrated to another host when you perform a reboot operation for a host. There is no impact on the user workload due to the reboot operation. Reboot fails if the ESXI node is already in maintenance mode.

Procedure

To reboot the nodes in the cluster, perform the following steps:

1. Log on to the Prism Element web console.
2. Click **Settings** from the drop-down menu of the Prism Element web console and then select **Reboot**.
3. In the **Request Reboot** window, select the checkbox associated with the nodes you want to restart, and click **Reboot**.

   A progress bar is displayed that indicates the progress of the restart of each node.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1958

STORAGE MANAGEMENT

Storage in a Nutanix cluster is organized hierarchically into several components that allow you to manage capacity and performance. Following is a brief outline of the storage features of Nutanix and how to navigate these storage features.

- Nutanix clusters provide storage pool, storage container, volume group, and virtual disk components to organize storage. For more information see Storage Components on page 109.
- Nutanix clusters provide effective storage capacity management to ensure that containers have sufficient storage for optimal performance while maintaining cost-efficiency and avoiding disruptions. For more information, see Capacity Management on page 111.
- Nutanix clusters provide storage efficient capabilities that allows strategic management of storage resources. For more information, see Storage Efficiency on page 117.
- Prism Element web console helps you monitor storage usage across the cluster. For more information see Storage Dashboard on page 124.
- Prism Element web console helps you create storage containers and volume groups. For more information, see Creating a Storage Container on page 138 and Creating a Volume Group on page 147.
- Prism Element web console helps you configure the replication factor of a storage container in a cluster. For more information, see Replication Factor Configuration on page 143.
- Prism Element web console helps you configure a threshold warning for storage capacity available in the cluster after accounting for the storage space needed to rebuild and restore in case of any component failures. For more information, see Configuring a Warning Threshold for Resilient Capacity on page 113.
- Prism Element web console helps you reserve storage capacity for rebuilding failed nodes, blocks or racks. For more information, see Rebuild Capacity Reservation on page 114.

Storage Components

Storage in a Nutanix cluster is organized into the following components.

Storage Tiers

Each type of storage hardware (SSD-PCIe (NVMe), SSD (SATA SSD), and HDD) is placed in a storage tier. You can determine the tier breakdown for disks in a storage pool through the web console . For more information, see Storage Table View on page 131 .

Storage Pools

Storage pools are groups of physical disks from one or more tiers. Storage pools provide physical separation because a storage device can only be assigned to a single storage pool at a time. Nutanix recommends creating a single storage pool for each cluster. This configuration allows the cluster to dynamically optimize capacity and performance. Isolating disks into separate storage pools provides physical separation, but can create an imbalance of these resources if the disks are not actively used. When you expand your cluster by adding new nodes, the new disks can also be added to the existing storage pool. This scale-out architecture allows you to build a cluster that grows with your needs.

When you create a cluster, a default predefined storage pool is available. This pool includes the total capacity of all the disks on all the hosts in the cluster.

Storage Containers

A storage container is a subset of available storage within a storage pool. Storage containers are created within a storage pool to hold virtual disks (vDisks) used by virtual machines. For more information, see Creating a Storage

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1959

Container. By default, storage is thinly provisioned, which means that the physical storage is allocated to the storage container as needed when data is written, rather than allocating the predefined capacity when the storage container is created. Storage efficiency features such as compression, deduplication, and erasure coding are enabled at the container level.

When you create a Nutanix cluster, the following storage containers are created by default:

- NutanixManagementShare: The NutanixManagementShare storage container is a built-in storage container for Nutanix clusters for use with the Nutanix Files and Self-Service Portal (SSP) features. This storage container is used by Nutanix Files and SSP for file storage, feature upgrades, and other feature operations. To ensure proper operation of these features, do not delete this storage container. Nutanix also recommends that you do not delete this storage container even if you are not using these features. The NutanixManagementShare storage container is not intended to be used as storage for vDisks, including Nutanix Volumes.
- SelfServiceContainer: SelfServiceContainer is a built-in storage container within a Nutanix cluster that is used for storage by VMs created using Image service features such as Self-Service and OpenShift. SelfServiceContainer can also be used like any other container for regular VMs, volume groups, and images. General requirements for using container-level configurations such as compression, deduplication, erasure coding, and replication factor in SelfServiceContainer are the same as any other container. Nutanix recommends that you do not delete this storage container.
- Default-Container-XXXX: Default-Container-XXXX container is a built-in storage container used by VMs to store vDisks for user VMs and applications. You can rename the Default-Container or delete it and create a new one according to your naming convention.

Volume Groups

A volume group is a collection of logically related virtual disks (or volumes). A volume group is attached to VM either directly or using iSCSI. You can add vDisks to a volume group, attach them to one or more consumers, include them in disaster recovery policies, and perform other management tasks. You can also detach a volume group from one VM and attach it to another, possibly at a remote location to which the volume group is replicated.

You manage a volume group as a single unit. When a volume group is attached to a VM, the VM can access all of the vDisks in the volume group. You can add, remove, and resize the vDisks in a volume group at any time.

Each volume group is identified by a UUID, a name, and an iSCSI target name. Each disk in the volume group also has a UUID and a SCSI index that specifies ordering within the volume group. A volume group can be configured for either exclusive or shared access.

You can backup, protect, restore, and migrate volume groups. You can include volume groups in protection domains configured for asynchronous data replication (Async DR), either exclusively or with VMs. However, volume groups cannot be included in a protection domain configured for metro availability, in a protected vStore, or in a consistency group for which application consistent snapshots are enabled.

vDisks

A vDisk is created within a storage container or volume group to provide storage to the virtual machines. A vDisk shows up as a SCSI device when it is mapped to a VM.

Containers for VMware and Hyper-V (Datastores/SMB Shares)

In vSphere, a datastore is a logical container for files necessary for VM operations. Nutanix provides the choice by supporting both iSCSI and NFS protocols when mounting a storage volume as a datastore within vSphere. NFS has many performance and scalability advantages over iSCSI, and it is the recommended datastore type.

In Hyper-V environments, storage containers are mounted as an SMB share.

> **Note:** Using a Nutanix storage container as a general-purpose NFS or SMB share is not recommended. For NFS and SMB file service, use Nutanix Files.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1960

NFS Datastores. The Distributed Storage Fabric (DSF) reduces unnecessary network chatter by localizing the data path of guest VM traffic to its host. This boosts performance by eliminating unnecessary hops between remote storage devices that is common with the pairing of iSCSI and VMFS. To enable vMotion and related vSphere features (when using ESX as the hypervisor), each host in the cluster must mount an NFS volume using the same datastore name. The Nutanix web console and nCLI both have a function to create an NFS datastore on multiple hosts in a Nutanix cluster.

To correctly map the local ESX datastore to the Nutanix container:

- Map the NFS share with 192.168.5.2 (internal IP address) and not the Controller VM IP address or cluster virtual IP address.
- The name of the datastore should be same as the name of the container.

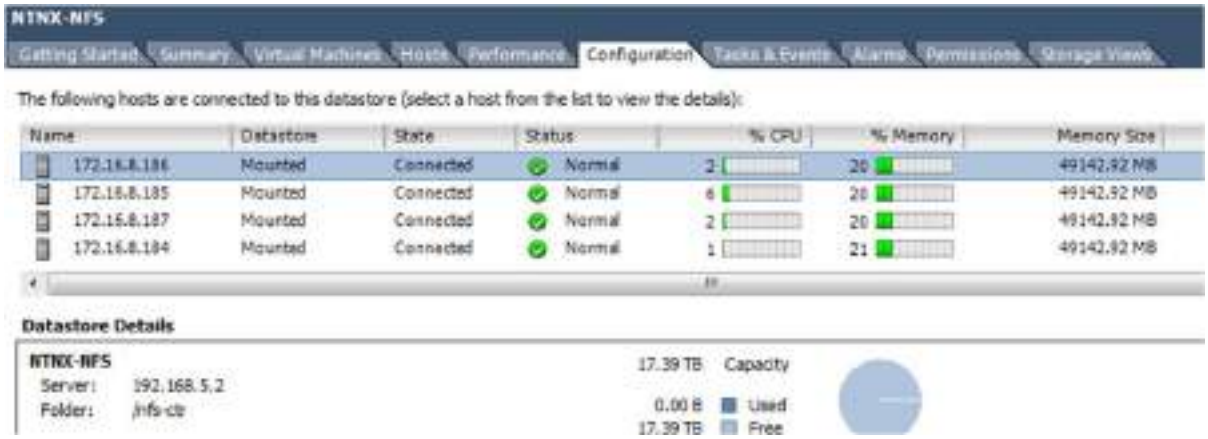


Figure 21: vSphere Configuration of NFS Datastore

SMB Library Share. The Nutanix SMB share implementation is the Hyper-V equivalent of an NFS Datastore with feature and performance parity with a vSphere configuration. The registration of a Nutanix storage container as an SMB Library share can be accomplished through a single powershell script, or through the Virtual Machine Manager GUI.

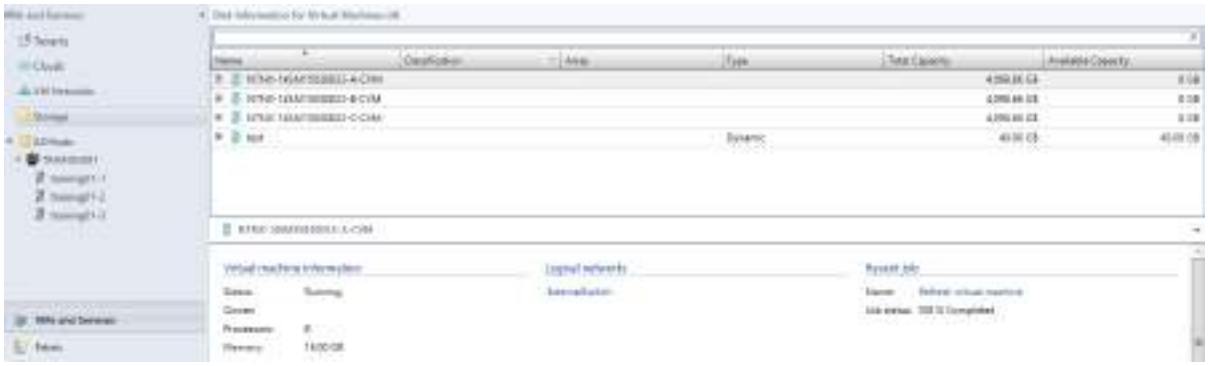


Figure 22: Hyper-V Configuration of an SMB Share

Capacity Management

Storage container capacity management involves monitoring and optimizing the allocation of storage resources within containers to ensure efficient utilization and prevent over-provisioning or resource exhaustion.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1961

Capacity Reservation Best Practices

Capacity reservation allows you to guarantee that a storage container has a minimum amount reserved that is unavailable to other storage containers.

By default, each storage container has access to all of the unused storage in the storage pool. If a storage pool consists of multiple storage containers, one storage container might take all the remaining storage space and leave others with no available space. To make sure that there is space available for a storage container, you can enable capacity reservation.

The following best practices are applicable for capacity reservation:

- Reserve capacity for a storage container only if the storage pool consists of multiple storage containers. Unless there is a specific reason to have multiple storage containers, Nutanix recommends you to configure a single storage pool with a single storage container.
- Do not reserve more than 90% of the total space in the storage pool.
- When you set an advertised capacity for a storage container, be aware that some extra space should be allocated beyond the projected size of any VMs placed in the container. This extra space is to allow room for data that is not yet garbage collected. The extra space is based on the workload and can be substantial, for example, 10% or more of the storage capacity in some cases.

Cluster Resilient Capacity

Cluster resilient capacity is the storage capacity available in the cluster after accounting for the storage space needed to rebuild and restore the cluster in case of any component failures.

Cluster Resilient Capacity Calculation with Homogeneous Capacity Entities in Failure Domains

For homogeneous capacity entities in a failure domain, the cluster resilient capacity is calculated as described in the following table:

Table 28: Cluster Resilient Capacity Calculation - Homogenous Capacity Entities

Cluster Fault Tolerance	Replication Factor	Failure Domain	Amount of space reserved (Re Capacity)
1N/1D	2	Node	1 node worth of capacity
		Block	1 block worth of capacity
		Rack	1 rack worth of capacity
1N&1D	3	Node	1 disk per node worth of capacit
		Block	1 disk per block worth of capacit
		Rack	1 disk per rack worth of capacity
2N/2D	3	Node	2 nodes worth of capacity
		Block	2 blocks worth of capacity
		Rack	2 racks worth of capacity

Cluster Resilient Capacity Calculation with non-homogeneous Capacity Entities in Failure domains

For non-homogeneous capacity entities in a failure domain, the cluster resilient capacity is calculated as the maximum available capacity at the lowest supported failure domain that can meet the required replication factor after cluster fault tolerance failures at the configured failure domain.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1962

The following table provides the examples for resilient capacity calculation when non-homogeneous capacity entities exist in failure domain:

Table 29: Cluster Resilient Capacity Calculation - Non-homogenous Capacity Entities

Cluster Fault Tolerance	Replication Factor	Failure Domain	Total Number of Nodes	Node Capacities	Failures
1N/1D	2	Node	5 nodes	10 TiB 10 TiB 10 TiB 40 TiB 40 TiB	Failure o capacity
1N&1D	3	Node	3 nodes	30TiB (3 disks of 10TiB each) 30TiB (3 disks of 10TiB each) 40TiB (4 disks of 10TiB each)	Failure o capacity any node
2N/2D	3	Node	5 nodes	10 TiB 10 TiB 20 TiB 40 TiB 40 TiB	Failure o capacity

Configuring a Warning Threshold for Resilient Capacity

Resilient capacity is the storage capacity available in the cluster after accounting for the storage space needed to rebuild and restore in case of any component failures. The resilient capacity in a cluster depends on the cluster fault tolerance level and the configured cluster failure domain (node, block, or rack).

About this task

You can configure a warning threshold to track the resilient capacity in the cluster. When the used capacity crosses the set threshold, the storage summary widget changes color as a warning.

To configure a warning threshold for resilient capacity, do the following.

Procedure

1. Log on to the Prism Element web console.
2. From the dropdown menu on the left of the main menu, select **Storage**.
   The system displays the **Storage** dashboard.
3. Click the gear icon in the **Storage Summary** widget.
   The system displays the **Configure Warning Threshold** dialog box.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1963

4. Select one of the following:

   » **Use default**: Select this option to use the default 75% warning threshold limit for resilient capacity.

   » **Set manually**: Select this option and enter your custom warning threshold limit for resilient capacity in the cluster.

5. Click **Save**.
   A resilient capacity marker is set according to the warning threshold limit on the storage capacity chart in the **Storage Summary** widget. Hover over the chart for more information.

Rebuild Capacity Reservation

Rebuild capacity is the storage capacity reserved in the cluster to enable self-healing and rebuilding failed nodes, blocks or racks (depending on what is configured as cluster failure domain).

Nutanix recommends that you reserve rebuild capacity in a cluster. Reserving rebuild capacity in a cluster enhances the self-healing mechanism of the cluster. You can reserve rebuild capacity using the Prism Element web console.

When you enable the **Reserve Rebuild Capacity** option in Prism Element web console, the system reserves the necessary capacity within the total cluster storage capacity based on *Failure Domain* and *Fault Tolerance* by removing the reserved capacity from the storage pool of the cluster. When there is a failure of the *Failure Domain* entity such as failure of a node, then the cluster rebuilds the data of the node by replicating the data on the remaining nodes.

For more information about *Failure Domain* and *Fault Tolerance*, see Cluster Resiliency on page 22.

For information on how to enable **Reserve Rebuild Capacity**, see Reserving Rebuild Capacity on page 116.

> **Note:** The cluster will stop accepting Write requests when the *Resilient Capacity* limit is reached. For information on cluster resilient capacity, see Cluster Resilient Capacity on page 112.

Requirements and Limitations

You can reserve rebuild capacity subject to the following limitations:

- Nutanix supports rebuild capacity reservation on the cluster with three or more nodes. Nutanix does not support rebuild capacity reservation on single-node and two-node clusters.
- It is advisable for the Prism administrator to confirm if a manual container reservation was previously configured on the cluster for this purpose before configuring a rebuild capacity reservation.
- The cluster must have a single storage pool that is the default storage pool. Do not create storage pools in the cluster when you have reserved rebuild capacity.
- For more information about storage pools, see Storage Components on page 109.
- Total capacity used or consumed must be less than the resilient capacity.

  If the used capacity is close to the resilient capacity and it increases due to large write operations and/or internal background jobs and migration tasks, then the used capacity can overshoot the resilient capacity. If rebuild capacity is already reserved on the cluster, the cluster stops accepting write requests.

  Total Capacity in the cluster is the sum of resilient capacity and reserved rebuild capacity. Capacity usage as the percentage of resilient capacity (Used Capacity) changes the color of the bar displaying the used capacity. Capacity usage also generates alerts. For example, if usage is 95 percent or more, then the cluster generates a

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1964

critical alert after a specified number of NCC check iterations. When you have reserved rebuild capacity and the usage is 95 percent or more (of the resilient capacity), the cluster stops accepting Write requests.

> **Caution:** Enabling Rebuild Capacity Reservation on a cluster with current usage (Total Used Space) close to the Resilient Capacity threshold might result in a VM outage. To avoid the issue, before enabling reservation ensure that current usage (Total Used Space) is not more than 90% of the calculated Resilient Capacity threshold.

- When you enable **Reserve Rebuild Capacity**, the usable capacity reduces from the Total Capacity to resilient capacity. Therefore, Recycle Bin usage as a percentage of usable capacity also changes to being a percentage of the resilient capacity after reserving Rebuild Capacity. For more information, see Recycle Bin on page 152.

  For example, if Recycle Bin usage as a percentage of usable capacity is four percent (4%) before enabling Reserve Rebuild Capacity, it could change to, for example, 10% of resilient capacity after enabling **Reserve Rebuild Capacity**. When Reserve Rebuild Capacity is enabled, Recycle Bin usage as a percentage of resilient capacity is used as the threshold to auto-disable Recycle Bin. This threshold percentage is five percent of usable (whether Total or resilient) capacity. In the above example, when Curator identifies that the threshold percentage is exceeded during a full scan, the Recycle Bin is auto-disabled.

  > **Note:** Auto-disabling of Recycle Bin depends on full scans by Curator. Therefore, the excess usage condition of the Recycle Bin could continue for sometime between two full scans before Recycle Bin is disabled.

- Changes in the cluster storage capacity impacts Resilient, Rebuild, Used and Free capacities in the cluster.

  - When rebuild capacity is reserved and you try to remove a host or a disk, the cluster calculates the possible used capacity and resilient capacity after the removal. A confirmation dialog box appears displaying a message that the `Resilient capacity will be reduced to` the possible reduced capacity after the removal. If the used capacity is greater than the possible resilient capacity, then the host or disk removal fails.

    Thus when rebuild capacity is reserved, Prism allows a node or disk removal only if the cluster's data can rebuild after such removal and at the same time preserve the configured domain's fault tolerance.

  - When rebuild capacity reservation is enabled, the data consumption of failed nodes is not accounted in the total usage. When rebuild capacity reservation is not enabled, the data consumption of failed nodes is added to the total usage thereby inflating it.

  - When rebuild capacity reservation is enabled, Oplog usage is accounted in the total usage. The oplog is a fast write back cache to absorb random writes. Its consumption will also be accounted towards total usage when rebuild capacity reservation is enabled.

- You cannot reserve rebuild capacity if you have enabled replication factor 1. You cannot enable replication factor 1 if you have reserved rebuild capacity.

- If you want to change the failure domain, for example, from Node to Block you must disable Rebuild Capacity Reservation. You can enable Rebuild Capacity Reservation after changing the failure domain. You cannot change the failure domain when Rebuild Capacity Reservation is enabled.

  Do not modify the failure domain using APIs when the Rebuild Capacity Reservation is enabled.

- Ensure that features such as Erasure Coding, De-duplication and compression are not disabled after you enable rebuild capacity reservation. Disabling such features can lead to drastic increase in used capacity beyond 95 percent and put the cluster in read-only mode when the usage before turning off these features is close to the threshold.

- The rebuild process is completed only when cluster fault tolerance is not exceeded. For example, if failure domain is Node and fault tolerance is 2N/2D, the rebuild process that starts after one node failure completes successfully. The rebuild process that starts after a second node failure (concurrent) also completes successfully. However, at this stage, if a third node fails, the rebuild process starts but does not complete.

- The rebuild process does not complete if data replicas are unavailable due to reasons such as link failures or disk failures.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1965

Note:

Usage due to internal background jobs and migration tasks can increase the used capacity even when there are no write operations running. Heavy write operations with small containers also drastically increases the used capacity. When the used capacity is close to resilient capacity, increase the capacity of the hosts in the cluster to ensure that the usage does not meet or exceed 95 percent of the total capacity.

Rebuild Capacity Display

When rebuild capacity is not reserved, the **Overview** tab of **Storage** page displays resilient capacity *Warning Threshold* in **Storage Summary**.

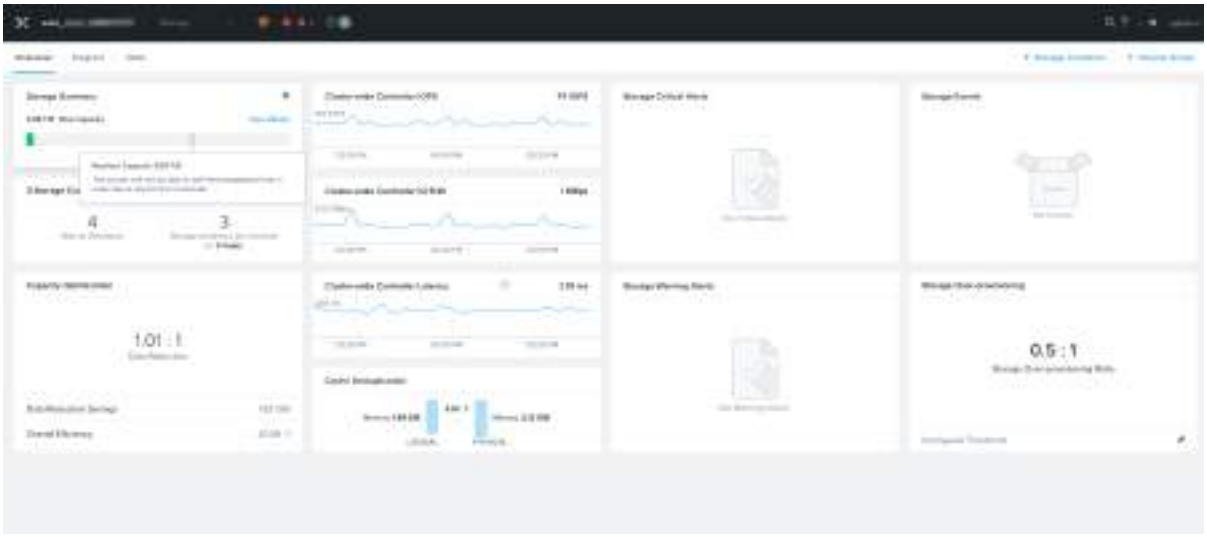


Figure 23: Storage Summary - Rebuild Capacity not reserved

For more information about *Resilient Capacity* and *Warning Threshold* configuration, see Configuring a Warning Threshold for Resilient Capacity on page 113.

Click the **View Details** link to open the **Storage Details** page, after selecting Physical in the drop-down on the right. The **Storage Details** page displays a banner informing you about rebuild capacity reservation. It also provides the **Enable Now** link that opens the **Rebuild Capacity Reservation** where you can reserve rebuild capacity.

To enable rebuild capacity reservation, see Reserving Rebuild Capacity on page 116.

When you enable rebuild capacity reservation, the cluster calculates the required rebuild capacity based on parameters such as fault tolerance, failure domain, and total storage capacity in the cluster. The reserved rebuild capacity is displayed on the **Rebuild Capacity Reservation** page.

After you reserve rebuild capacity, the **Overview** tab of **Storage** page does not display resilient capacity *Warning Threshold* in **Storage Summary**.

After you reserve rebuild capacity, the **Storage Details** page displays a banner informing you that the cluster has reserved rebuild capacity. The details show an additional item - Rebuild Capacity with the capacity reserved in TiB. The capacity numbers change in the **Storage Details** page after the reservation.

Reserving Rebuild Capacity

You can reserve rebuild capacity in a Nutanix cluster.

About this task

To reserve rebuild capacity, follow these steps:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1966

Procedure

1. Log on to the Prism Element web console.
2. From the dropdown menu on the left of the main menu, select **Settings**.
   The system displays the **Global Settings** page.
3. From the **Data Resiliency** section in the left navigation pane, click **Rebuild Capacity Reservation**.
   The system displays the **Rebuild Capacity Reservation** page.
4. Select the **Reserve Rebuild Capacity** checkbox.
5. Click **Save**.
   The system reserves rebuild capacity in the cluster.

Storage Efficiency

Nutanix provides storage efficient capabilities that allows strategic management of storage resources to maximize capacity utilization, enhance performance, and ensure reliability.

In a Nutanix cluster, where data is distributed across multiple nodes, achieving efficiency is critical to reducing costs, optimizing resource usage, and maintaining scalability.

To minimize redundancy, conserve space, and enhance fault tolerance, a Nutanix cluster supports the following storage efficiency capabilities:

- Deduplication on page 117
- Compression on page 118
- Erasure Coding on page 118

Deduplication

Deduplication reduces space usage by consolidating duplicate data blocks on Nutanix storage when you enable capacity deduplication on a storage container.

Important:

- Deduplication is only supported on clusters with a minimum of three nodes.
- If deduplication enabled on storage containers having protected VMs, the system lowers the replication speed.
- Turning deduplication on for VAAI clone or linked clone environments is not recommended.

Capacity Deduplication

Enable capacity deduplication of persistent data to reduce storage usage. Capacity deduplication means deduplication performed on the data in hard disk storage (HDD).

Note:

- Capacity deduplication is not enabled by default.
- Capacity deduplication is available if you have purchased a Nutanix Cloud Infrastructure (NCI) Starter or higher license.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1967

Important: Nutanix recommends that you configure the Controller VMs with at least 32 GiB of RAM and 300 GiB SSDs for the metadata disk for Capacity Deduplication.

How to enable Deduplication

The **Capacity** deduplication property is enabled at the storage container level. These storage container properties can be set in the web console or nCLI.

Deduplication Best Practices

The following table provides the scenarios where deduplication is recommended and where it is not recommended:

Enable deduplication	Do not enable deduplication
• Full clones • Physical-to-virtual (P2V) migration • Persistent desktops	• *Linked clones or Nutanix VAAI clones*: Duplicate data is managed efficiently by DSF so deduplication has no additional benefit • *Server workloads*: Redundant data is minimal so may not see significant benefit from deduplication

Compression

You can enable compression on a storage container. Compression can save physical storage space and improve I/O bandwidth and memory usage—which may have a positive impact on overall system performance.

Note: If the metadata usage is high, compression is automatically disabled. If compression is automatically disabled, an alert is generated.

The following types of compression are available:

Post-process compression

Data is compressed after it is written. The delay time between write and compression is configurable, and Nutanix recommends a delay of 60 minutes.

Inline compression

Data is compressed as it is written. When you create a new storage container, inline compression is enabled by default for all license tiers. It is set to a delay of 0, compressing data immediately as it is written.

Compression Ratios

You can view compression ratios and usage savings in the Prism Element web console.

- *Cluster*

  In the **Storage** dashboard, under **Capacity Optimization**, click the **After** bar, and hover your mouse over **Compression**.

- *Storage container*

  In the **Storage** dashboard **Table** view, on the **Storage Container** tab, click the storage container for which you want to view the compression ratio. You can see the compression ratio for the selected storage container under **Storage Container Details**.

Erasure Coding

Erasure coding increases the usable capacity of a cluster. Instead of replicating data, erasure coding uses parity information to rebuild data in the event of a disk failure. The capacity savings of erasure coding are in addition to deduplication and compression savings.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1968

Important: Erasure coding is supported on clusters with a minimum of 4 nodes when using replication factor 2 and a minimum of 6 nodes when using replication factor 3.

If you have configured 1N/1D cluster fault tolerance, two data copies are maintained. For example, consider a 6-node cluster with 4 data blocks (a b c d). In this example, we start with 4 data blocks (a b c d) configured with 1N/1D cluster fault tolerance.

The white text represents the data blocks and the green text represents the copies.

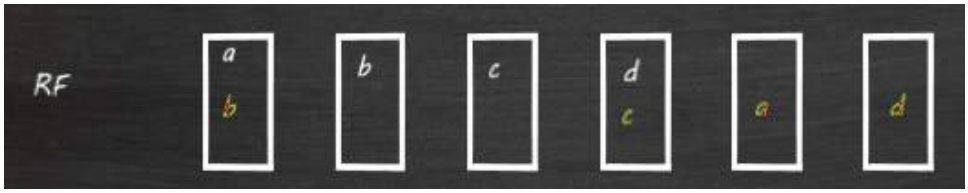


Figure 24: Data copies before Erasure Coding

When the data becomes cold, the erasure code engine performs an exclusive OR operation to compute parity “P” for the data.

Figure 25: During Computing Parity

After parity is computed, the data block copies are removed and replaced with the parity information. Redundancy through parity results in data reduction because the total data on the system is now a+b+c+d+P instead of 2 × (a+b+c +d).

Note: Each block in the stripe is placed on a separate node to protect from a single node failure.

Figure 26: After Computation of Parity

If the node that contains data block c fails, block c is rebuilt using the rest of the erasure coded stripe (a b d and P) as displayed in the following example:

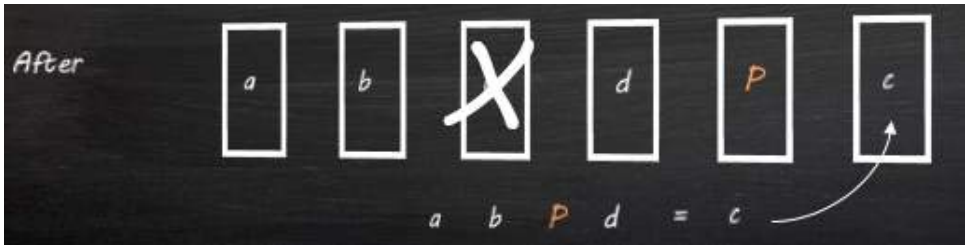


Figure 27: Post Node Failure

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1969

Block c is then placed on a node that does not have any other members of this erasure coded stripe.

> **Note:** When the cluster is configured with 2N/2D cluster fault tolerance, two parity blocks are maintained so that the erasure coded data has the same resiliency as the replicated data. An erasure coded stripe with two parity blocks can handle the failure of two nodes.

Example of Data Reduction Savings from Erasure Coding

The space savings from the erasure coding depends on the cluster size, cluster fault tolerance setting, and percentage of cold data.

You can view the erasure coding usage savings from the storage container summary.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1970

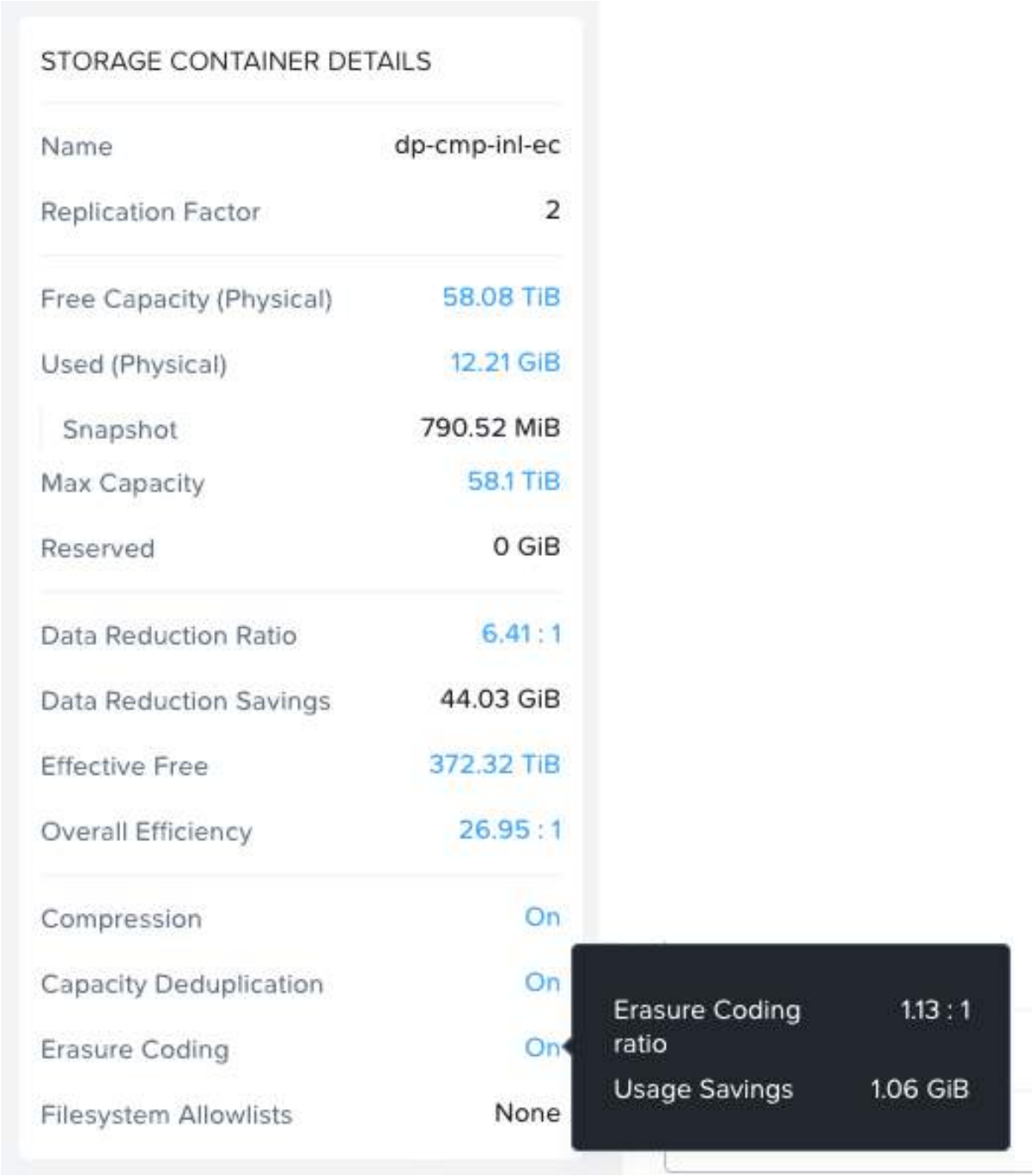


Figure 28: Storage Container Summary: Usage Savings Screen

In a 6-node cluster configured with replication factor 2, erasure coding uses a stripe size of 5 where 4 nodes are for data and 1 node is for parity. The sixth node in the cluster ensures that if a node fails, another node is available for rebuild. You can view the erasure coding usage savings from the storage container summary.

Erasure coding stripe size adapts to the size of the cluster starting with the minimum 4 nodes with a maximum of 5 node stripe width. The following is an example displaying the various configurations of cluster size, possible stripe widths, and approximate savings that might occur when erasure coding is enabled.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1971

Figure 29: Example of Space Saving from Erasure Coding on 20 TiB Nodes

Erasure Coding Best Practices and Requirements

Nutanix recommends the following best practices and requirements to implement Erasure Coding:

- A cluster must have at least four nodes/blocks/racks to enable erasure coding. The cluster can have all four flash nodes or a combination of flash and hybrid nodes, or all hybrid nodes. If erasure coding is enabled on a storage container, a minimum of four blocks for replication factor 2 or six blocks for replication factor 3 is required to maintain block awareness.
- The following table provides the information about the recommended minimum configuration for multiple node removal operations:

Table 30: Minimum Recommended Configuration for Erasure Coding

Desired Awareness Type	Cluster Fault Tolerance	Min. Units	Simultaneous Failure Tolerance
Node	1N/1D	4 nodes	1 node
Node	2N/2D	6 nodes	2 nodes
Block	1N/1D	4 blocks	1 block
Block	2N/2D	6 blocks	2 blocks
Rack	1N/1D	4 racks	1 rack
Rack	2N/2D	6 racks	2 racks

> **Note:** Ensure that you maintain a cluster size that is at least one node greater than the combined strip size (data + parity) to allow space to rebuild the strips if a node fails.

- AOS dynamically calculates the erasure coding strip sizes depending on the number of nodes, blocks, and racks. The maximum supported and recommended strip sizes are (4,1) or (4,2), depending on the nodes, blocks, and racks. Nutanix recommends that you do not change the strip size. Greater strip sizes increase the space savings; however, they also increase the cost of rebuild.
- Erasure coding effectiveness (data reduction savings) might reduce on workloads that have many overwrites outside of the erasure coding window. The default value for erasure coding window is seven days for write cold.
- Read performance is affected during rebuild and the amount depends on cluster strip size and read load on the system.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1972

- Erasure coding is an asynchronous process, and hence the time taken to calculate and display space savings depends on the type and coldness of data. A minimum of two full curator scans are required to calculate the data savings.
- Ensure that you have replication factor+1 storage heavy or storage only nodes for all-flash clusters with storage heavy nodes. For example, if you have a four-node replication factor 2 enabled cluster, then you must add a minimum of three storage heavy nodes for optimum performance.

Inline Erasure Coding

Inline erasure coding creates erasure coding strips by erasure coding data without waiting for the data to become write cold.

There are two types of inline erasure coding:

- *Same vDisk strips*: Strips that are created using the data blocks from the same vDisk. Nutanix recommends that you configure inline erasure coding type as same vDisk strips for workloads that do not require data locality.
- *Cross vDisk strips*: Strips that are created using the data blocks across multiple vDisks. Nutanix recommends that you configure inline erasure coding type as cross vDisk strips for workloads that require data locality.

By default, same vDisk strips are created when you enable inline erasure coding.

> **Note:** Inline erasure coding with same vDisk strips can be enabled for clusters running AOS version 5.18 or higher; and with cross vDisk strips can be enabled for clusters running AOS version 6.6 or higher.

Enabling Inline Erasure Coding

Inline erasure coding can be enabled only using nCLI. Inline erasure coding is added as a storage container parameter in Zeus.

Before you begin

> **Caution:**
>
> - Nutanix recommends that you enable inline erasure coding for Object storage containers only. To enable inline erasure coding for any other type of storage container, contact Nutanix Support.
> - Erasure coding must be enabled on the container to enable inline erasure coding. For information about how to enable erasure coding, see Creating a Storage Container.

Procedure

To enable inline erasure coding, perform the following actions:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1973

- Run the following nCLI command:

  ```
  ncli> container create name=container_name sp-id=storage_pool_id  erasure-code=on
   inline-ec-enabled=true
  ```

  Replace *container_name* and *storage_pool_id* with the storage container name and storage pool ID on which you want to enable erasure coding.

  - To explicitly configure inline erasure coding type, run the following nCLI commands:

    - For inline erasure coding type: *Same vDisk strips*

      ```
      ncli> container create name=container_name sp-id=storage_pool_id  erasure-
      code=on inline-ec-enabled=true inline-ec-type=same-vdisk-strips
      ```

    - For inline erasure coding type: *Cross vDisk strips*

      ```
      ncli> container create name=container_name sp-id=storage_pool_id  erasure-
      code=on inline-ec-enabled=true inline-ec-type=cross-vdisk-strips
      ```

    Replace *container_name* and *storage_pool_id* with the storage container name and storage pool ID on which you want to enable erasure coding.

  - To change an existing inline erasure coding type, run the following ncli commands:

    - To change to *Same vDisk strips*:

      ```
      ncli> container edit inline-ec-enabled=true inline-ec-type=same-vdisk-strips
       id=container_id
      ```

    - To change to *Cross vDisk strips*:

      ```
      ncli> container edit inline-ec-enabled=true inline-ec-type=cross-vdisk-strips
       id=container_id
      ```

    Replace *container_id* with the ID of the storage container.

- To verify if inline erasure coding is enabled, run the following nCLI command:

  ```
  ncli> container ls name=container_name
  ```

  Replace *container_name* with the name of the storage container on which you enabled inline erasure coding.

  The system displays Inline EC Enabled : true if inline erasure coding is enabled.

Storage Dashboard

The Storage dashboard displays dynamically updated information about the storage configuration in a cluster. To view the Storage dashboard, select **Storage** from the pull-down list on the far left of the main menu.

Menu Options

In addition to the main menu, the Storage screen includes a menu bar with the following options. For information on the main menu, Main Menu on page 58.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1974

- *View selector*. The Storage dashboard provides three viewing modes.
  - Click the **Overview** button on the left to display storage information in a summary view. For more information, see Storage Overview View on page 125.
  - Click the **Diagram** button to display a diagram of the storage pools and storage containers in the cluster nodes from which you get detailed information by clicking on a storage pool or storage container of interest. For more information, see Storage Diagram View on page 127.
  - Click the **Table** button to display hardware information in a tabular form. The Table screen is further divided into Volume Group, Storage Pool, and Storage Container views; click the **Volume Group** tab to view volume group information, the **Storage Pool** tab to view storage pool information, and the **Storage Container** tab to view storage container information. For more information, see Storage Table View on page 131.
- *Action buttons*. Click the **Volume Group** button on the right to add a volume group to the cluster in a storage container. For more information, see Creating a Volume Group on page 147.

  Click the **Storage Container** button to add a storage container to a storage pool. For more information, see Creating a Storage Container on page 138.
- *Page selector*. In the Table view, hosts and disks are listed 10 per page. When there are more than 10 items in the list, left and right paging arrows appear on the right, along with the total count and the count for the current page.
- *Export table content*. In the Table view, you can export the table information to a file in either CSV or JSON format by clicking the gear icon on the right and selecting either **Export CSV** or **Export JSON** from the pull-down menu. (The browser must allow a dialog box for export to work.) Chrome, Internet Explorer, and Firefox download the data into a file; Safari opens the data in the current window.

Storage Overview View

The Storage Overview view displays storage-specific performance and usage statistics on the left plus the most recent storage-specific alert and event messages on the right. Several fields include a slide bar on the right to view additional information in that field. The displayed information is dynamically updated to remain current.

> **Note:** For information about how the statistics are derived, see Understanding Displayed Statistics on page 70.

Table 31: Storage Overview Widgets

Name	Description
Storage Summary	Displays information about the physical storage space utilization (in GiB or TiB) and resilient capacity of the cluster. Placing the cursor anywhere on the horizontal axis displays a breakdown view of the storage capacity usage. The **View Details** link displays the resiliency status and storage information of all the individual nodes in the cluster. For more information, see Storage Details Page on page 126. You can also configure a threshold warning for the resilient capacity utilization in the cluster by clicking the gear icon. For more information, see Configuring a Warning Threshold for Resilient Capacity on page 113.
Storage Containers	Displays the number of storage containers, number of VMs, and number of hosts on which the storage containers are mounted in the cluster.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1975

Name	Description
Capacity Optimization	Displays the data reduction ratio (compression, deduplication, and erasure coding), data reduction savings (compression, deduplication, and erasure coding), and the current gained by enabling compression, deduplication, and erasure coding features.
Cluster-wide Controller IOPS	Displays I/O operations per second (IOPS) in the cluster. The displayed time period is a rolling interval that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. (These display features also apply to the I/O bandwidth and I/O latency monitors.)
Cluster-wide Controller IO B/W	Displays I/O bandwidth used per second in the cluster. The value is displayed in an appropriate metric (MBps, KBps, and so on) depending on traffic volume. For more in depth analysis, you can add this chart (and any other charts on the page) to the analysis page by clicking the blue link in the upper right of the chart. For more information, see Analysis Dashboard on page 334.
Cluster-wide Controller Latency	Displays the average I/O latency (in milliseconds) in the cluster.
Cache Deduplication	**Note:** Cache deduplication is not supported in AOS 6.6 and later versions.
Storage Critical Alerts	Displays the five most recent unresolved storage-specific critical alert messages. Click a message to open the Alert screen at that message. You can also open the Alert screen by clicking the **view all alerts** button at the bottom of the list. For more information, see Alerts Dashboard in *Prism Element Alerts and Events Reference Guide*.
Storage Warning Alerts	Displays the five most recent unresolved storage-specific warning alert messages. Click a message to open the Alert screen at that message. You can also open the Alert screen by clicking the **view all alerts** button at the bottom of the list.
Storage Events	Displays the ten most recent storage-specific event messages. Click a message to open the Event screen at that message. You can also open the Event screen by clicking the **view all events** button at the bottom of the list.
Storage Over-provisioning	Displays the storage over-provisioning ratio (calculated based on the provisioned storage and the available raw storage) in the cluster. Note that the time taken for the **Storage Over-provisioning Ratio** widget to reflect the changes made in the cluster varies according to the recent storage operations/activities performed.

Storage Details Page

The Storage Details page displays the resiliency status and physical storage information of all the individual nodes in the cluster.

The Storage Details page is divided into two sections:

- The right section displays a diagrammatic representation of the number of nodes present in the cluster along with the respective storage capacity used.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1976

- The left section provides detailed storage information of the cluster as follows.

Parameter	Description	Values
Failure Domain	Displays the entity (node, block, or rack) which if failed, the cluster can tolerate while still running guest VMs and responding to commands through the management console.	node, block, or rack
Total Capacity	Displays the total capacity of all the disks on all the hosts in the cluster.	xxx [GB|TB]
Resilient Capacity	Displays the total resilient capacity of the cluster.	xxx [GB|TB]
Total Usage	Displays the sum of all the storage space used by the cluster. The total usage is calculated based on the following: • **Used Capacity**: The amount of used storage space in the cluster (by user data). • **Recovery Points**: The capacity occupied by images, clones and recovery points of VMs, Volume Groups. • **Recycle Bin**: The capacity is occupied by deleted VMs and Volume Groups, which are automatically purged after 24 hours. In the event of capacity constraints, this capacity is cleared by the system to service the incoming 10s. • **Others**: Capacity occupied by VM, VG Disks, and Images.	xxx [GB|TB]
Available Capacity	Displays the available storage capacity on all the disks on all the hosts in the cluster.	xxx [GB|TB]

Storage Diagram View

The Storage Diagram view displays information about the physical usage of storage pools and storage containers. The displayed information is dynamically updated to remain current.

The Storage Diagram view screen is divided into two sections:

- The top section is a cascading diagram of the storage units. Initially, a cluster bar appears with storage information about the cluster (used, provisioned, and available storage). You can configure a threshold warning for the resilient capacity utilization in the cluster by clicking the gear icon to the right of the cluster bar. For information, see Configuring a Warning Threshold for Resilient Capacity on page 113. Clicking on a cluster bar displays storage information about the physical usage of storage pool (used, provisioned, and available storage)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1977

and bar with colored blocks for each storage container in that storage pool. Clicking on a storage pool block displays storage information about the storage container and a bar for that storage container. You can edit a storage pool or storage container by clicking the pencil (edit) or X (delete) icon to the right of the name. Clicking the **close** link at the far right hides that storage pool or storage container bar from the display.

- The bottom **Summary** section provides additional information. It includes a details column on the left and a set of tabs on the right. The details column and tab content varies depending on what has been selected.

> **Note:** For information about how the statistics are derived, see Understanding Displayed Statistics on page 70.

Storage Container Details

Selecting a storage container in the diagram displays information about that storage container in the lower section of the screen.

- When a storage container is selected, **Summary: *storage_container_name*** appears below the diagram, and action links appear on the right of this line:
  - Click the **Update** link to update the settings for this storage container.
  - Click the **Delete** link to delete this storage container configuration.

  For more information about these actions, see Modifying a Storage Container on page 142.
- In the **Summary: *storage_container_name*** table, hover your mouse over the value to see additional details of that parameter.
- Four tabs appear that display information about the selected storage container (see following sections for details about each tab): **Storage Container Usage**, **Storage Container Performance**, **Storage Container Alerts**, **Storage Container Events**.

Table 32: Storage Container Details Fields

Parameter	Description	Values
Name	Displays the name of the storage container.	(name)
Replication Factor	Displays the replication factor, which is the number of maintained data copies. The replication factor is specified when the storage container is created.	[1,2,3]
Protection Domain	Displays the name of the protection domain if the you have a configured a protection domain for that storage container.	(name)
Datastore	Displays the name of the datastore.	(name)
VMs	Displays the number of VMs	(number)
Free Space (Physical)	Displays the amount of free physical storage space available to the storage container that is unreserved.	xxx [GB|TB]
Used (Physical)	Displays the amount of used physical storage space in the storage container, including space used by Snapshots and Recycle Bin.	xxx [GB|TB]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1978

Parameter	Description	Values
Max Capacity	Displays the total amount of storage capacity available to the storage container. Nutanix employs a *thin* provisioning model when allocating storage space, which means space is assigned to a storage container only when it is actually needed. The maximum capacity value reflects the total available storage regardless of how many storage containers are defined. Therefore, when you have two storage containers, it can appear that you have twice as much capacity because maximum capacity for both storage containers show the full amount. Maximum capacity is calculated as the total physical capacity in the storage pool, minus any reserved capacity, minus space used by other storage containers.	xxx [TB]
Reserved	Displays the amount of reserved physical storage space in the storage container.	xxx [GB|TB]
Data Reduction Ratio	Displays the ratio of how much the data size is reduced by enabling compression, deduplication, and erasure coding.	
Data Reduction Savings	Displays the data reduction savings by enabling compression, deduplication, and erasure coding.	
Effective Free	Displays the amount of usable free space after data reduction.	
Overall Efficiency	Displays the capacity optimization (as a ratio) that results from the combined effects of data reduction (deduplication, compression, and erasure coding), cloning, and thin provisioning.	
Compression	Displays whether compression is enabled.	[Off|On]
Capacity Deduplication	Displays whether on disk deduplication is enabled on hard disks (HDD).	[Off|On]
Erasure Coding	Displays whether erasure coding is enabled.	[On, Off]
Filesystem Whitelists	Displays whether you have configured filesystem whitelist for this storage container.	[None, On, Off]

Storage Pool Details

Selecting a storage pool in the diagram displays information about that storage pool in the lower section of the screen.

- When a storage pool is selected, **Summary: *`storage_pool_name`*** appears below the diagram, and action links appear on the right of this line:
  - Click the **Update** link to update the settings for this storage pool.

  For more information about this action, see Modifying a Storage Container on page 142.
- Four tabs appear that display information about the selected storage pool (see following sections for details about each tab): **Storage Pool Usage**, **Storage Pool Performance**, **Storage Pool Alerts**, **Storage Pool Events**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1979

Table 33: Storage Pool Details Fields

Parameter	Description	Values
Name	Displays the name of the storage pool.	(name)
Free (Physical)	Displays the total amount of physical storage space that is available.	xxx [GB|TB]
Used (Physical)	Displays the total amount of physical storage space used in the storage pool.	xxx [GB|TB]
Capacity (Physical)	Displays the total physical storage space capacity in the storage pool.	xxx [TB]
Disk Count	Displays the number of disks in the storage pool.	(number)

Cluster Summary Information

When a storage container or storage pool is not selected in the table (or when the word **Summary** is clicked), cluster-wide summary information appears in the lower part of the screen.

- The **Storage Summary** column (on the left) includes five fields:
  - **Free (Physical)**. Displays the amount of physical storage space still available in the cluster.
  - **Used (Physical)**. Displays the amount of physical storage space used currently in the cluster, including the Recycle Bin.
  - **Capacity (Physical)**. Displays the total physical storage capacity in the cluster.
  - **Storage Pool(s)**. Displays the names of the storage pool. Clicking on a name displays the detail information for that storage pool in this section.
  - **Storage Container(s)**. Displays the names of the storage containers. Clicking on a name displays the detail information for that storage container in this section.
- Four tabs appear that display cluster-wide information (see following sections for details about each tab): **Usage Summary**, **Performance Summary**, **Storage Alerts**, **Storage Events**.

Usage Tab

The Usage tab displays graphs of storage usage. The tab label varies depending on what is selected in the table:

- **Usage Summary** (no storage pool or storage container selected). Displays usage statistics across the cluster.
- **Storage Container Usage** (storage container selected). Displays usage statistics for the selected storage container.
- **Storage Pool Usage** (storage pool selected). Displays usage statistics for the selected storage pool.

The Usage tab displays the following two graphs:

- **Cluster-wide Usage Summary**: Displays a rolling time interval usage monitor that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in depth analysis, you can add the monitor to the analysis page by clicking the blue link in the upper right of the graph. For more information, see Analysis Dashboard on page 334.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1980

- **Tier-wise Usage**: Displays a pie chart divided into the percentage of storage space used by each disk tier in the cluster, storage pool, or storage container. Disk tiers can include DAS-SATA, SSD-SATA, and SSD-PCIe depending on the Nutanix model type.

Performance Tab

The Performance tab displays graphs of performance metrics. The tab label varies depending on what is selected in the table:

- **Performance Summary** (no storage pool or storage container selected). Displays storage performance statistics across the cluster.
- **Storage Container Performance** (storage container selected). Displays storage performance statistics for the selected storage container.
- **Storage Pool Performance** (storage pool selected). Displays storage performance statistics for the selected storage pool.

The graphs are rolling time interval performance monitors that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in depth analysis, you can add a monitor to the analysis page by clicking the blue link in the upper right of the graph. For more information, see Analysis Dashboard on page 334. The Performance tab includes the following three graphs:

- **[Cluster-wide Hypervisor|Controller|Disk] IOPS**: Displays I/O operations per second (IOPS) for the cluster, selected storage container, or selected storage pool.
- **[Cluster-wide Hypervisor|Controller|Disk] I/O Bandwidth**: Displays I/O bandwidth used per second (MBps or KBps) for physical disk requests in the cluster, selected storage container, or selected storage pool.
- **[Cluster-wide Hypervisor|Controller|Disk] I/O Latency**: Displays the average I/O latency (in milliseconds) for physical disk requests in the cluster, selected storage container, or selected storage pool.

Storage Alerts Tab

The Alerts tab displays the unresolved alert messages about storage pools or storage containers in the same form as the Alerts page. For more information, see Alerts Summary View. Click the **Unresolved X** button in the filter field to also display resolved alerts.

Storage Events Tab

The Events tab displays the unacknowledged event messages about storage pools or storage containers in the same form as the Events page. For more information, see Events Summary View. Click the **Include Acknowledged** button to also display acknowledged events.

Storage Table View

The Storage Table view displays information about storage pools and storage containers in a tabular form. Click the **Volume Group** tab to display volume group information; click the **Storage Pool** tab in the screen menu bar to display storage pool information; click the **Storage Container** tab to display storage container information. The displayed information is dynamically updated to remain current.

The Storage Table view is divided into two sections:

- The top section is a table. Each row represents a single volume group, storage pool, or storage container and includes basic information about that entity. Click a column header to order the rows by that column value (alphabetically or numerically as appropriate).
- The bottom **Summary** section provides additional information. It includes a details column on the left and a set of tabs on the right. The details column and tab content varies depending on what has been selected.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1981

Note: For more information about how the statistics are derived, see Understanding Displayed Statistics on page 70.

Volume Group tab

Clicking the Volume Group tab displays information about volume groups in the cluster.

- The table at the top of the screen displays information about all the configured volume groups, and the details column (lower left) displays additional information when a volume group is selected in the table. The following table describes the fields in the volume group table and detail column.
- When a volume group is selected, Summary: `volume_group_name` appears below the table, and action links appear on the right of this line:
  - Click the **Update** link to update the settings for this volume group.
  - Click the **Delete** link to delete this volume group.

  For more information about these actions, see Modifying or Deleting a Volume Group on page 149.

  Five tabs appear that display information about the selected volume group (see following sections for details about each tab): Performance Metrics, Virtual Disks, Volume Group Tasks, Volume Group Alerts, and Volume Group Events.

Table 34: Volume Group Table and Detail Fields

Parameter	Description	Values
Volume Group Table Fields (upper screen)		
Name	Displays the name of the volume group.	(name)
Disks	Displays the number of disks in the volume group.	[0–256]
Controller IOPS	Displays the current I/O operations per second (IOPS) for the volume group. The controller IOPS, I/O bandwidth, and I/O latency fields record the I/O requests serviced by the Controller VM. The I/O can be served from memory, cache (SSD), or disk.	[0 - unlimited]
Controller IO B/W	Displays I/O bandwidth used per second for Controller VM-serviced requests in this volume group.	xxx [MBps|KBps]
Controller IO Latency	Displays the average I/O latency for Controller VM-serviced requests in this volume group.	xxx [ms]
Volume Group Details Fields (lower screen)		
Name	Displays the name of the volume group.	(name)
Number of Virtual Disks	Displays the number of virtual disks in the volume group.	[0–256]
Total Size	Displays the total size of the volume group.	xxx [GB|TB]
Flash Mode	Displays whether the flash mode is enabled.	
Shared	Indicates whether the volume group is shared across iSCSI initiators.	[Yes|No]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1982

Parameter	Description	Values
Initiators	Displays the iSCSI initiators to which the volume group is attached.	(None|List of names)
Storage Container	Displays the name of the storage container to which the volume group belongs.	(name)
Target IQN Prefix	Displays the IQN prefix of the target iSCSI.	

Storage Container Tab

Clicking the **Storage Container** tab displays information about storage containers in the cluster (see Creating a Storage Container on page 138).

- The table at the top of the screen displays information about all the configured storage containers, and the details column (lower left) displays additional information when a storage container is selected in the table. The following table describes the fields in the storage container table and detail column.
- When a storage container is selected, **Summary:** ***`storage_container_name`*** appears below the table, and action links appear on the right of this line:
  - Click the **Update** link to update the settings for this storage container.
  - Click the **Delete** link to delete this storage container configuration.

  For more information about these actions, see Modifying a Storage Container on page 142.
- Four tabs appear that display information about the selected storage container (see following sections for details about each tab): **Storage Container Breakdown**, **Storage Container Usage**, **Storage Container Performance**, **Storage Container Alerts**, **Storage Container Events**.

Table 35: Storage Container Table and Detail Fields

Parameter	Description	Values
Storage Container Table Fields (upper screen)		
Name	Displays the name of the storage container.	(name)
Encrypted	Displays the encryption status of the storage container.	[Yes| No]
Replication Factor	Displays the replication factor, which is the number of maintained data copies. The replication factor is specified when the storage container is created.	[1,2,3]
Compression	Displays whether compression is enabled.	[Off|On]
Capacity Deduplication	Displays whether on disk deduplication is enabled on hard disks (HDD).	[On, Off]
Erasure Coding	Displays whether erasure coding is enabled for the storage container or not	[On, Off]
Free Capacity (Physical)	Displays the amount of free physical storage space in the storage container.	xxx [GB|TB]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1983

Parameter	Description	Values
Used Capacity (Physical)	Displays the amount of used physical storage space in the storage container, including space used by the Recycle Bin.	xxx [GB|TB]
Reserved Capacity (Physical)	Displays the amount of reserved physical storage space in the storage container.	xxx [GB|TB]
Max Capacity (Physical)	Displays the total amount of physical storage capacity available to the storage container. Nutanix employs a *thin* provisioning model when allocating storage space, which means space is assigned to a storage container only when it is actually needed. The maximum capacity value reflects total available storage regardless of how many storage containers are defined. Therefore, when you have two storage containers, it can appear you have twice as much capacity because maximum capacity for both storage containers show the full amount. Maximum capacity is calculated as the total physical capacity in the storage pool, minus any reserved capacity, minus space used by other storage containers.	xxx [TB]
Controller IOPS	Displays the current I/O operations per second (IOPS) for the storage container. The controller IOPS, I/O bandwidth, and I/O latency fields record the I/O requests serviced by the Controller VM. The I/O can be served from memory, cache (SSD), or disk.	[0 - unlimited]
Controller IO B/W	Displays I/O bandwidth used per second for Controller VM-serviced requests in this storage container.	xxx [MBps|KBps]
Controller IO Latency	Displays the average I/O latency for Controller VM-serviced requests in this storage container.	xxx [ms]
Storage Container Details Fields (lower screen)		
Name	Displays the name of the storage container.	(name)
Encrypted	Displays the encryption status of the storage container.	
Protection Domain	Displays the data protection domain used for the storage container.	(DR name)
VMs	Displays the number of VMs associated with the storage container.	xxx
Free Capacity (Physical)	Displays the amount of free physical storage space available to the storage container that is unreserved.	xxx [GB|TB]
Used (Physical)	Displays the amount of used physical storage space for the storage container.	xxx [GB|TB]
Snapshot	The total storage capacity in the cluster consumed by snapshots (sum of both local and remote).	xxx [GB|TB]
Max Capacity	Displays the total amount of storage capacity available to the storage container (see the Max Capacity (Physical) for description).	xxx [TB]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1984

Parameter	Description	Values
Reserved	Displays the total reserved storage capacity in the storage container.	xxx [GB|TB]
Replication Factor	Displays the replication factor, which is the number of maintained data copies. The replication factor is specified when the storage container is created.	[1, 2, 3]
Compression	Displays whether compression is enabled.	[Off|On]
Data Reduction Ratio	Displays the ratio of how much the data size is reduced by enabling compression, deduplication, and erasure coding.	x.xx : 1
Data Reduction Savings	Displays the data reduction savings by enabling compression, deduplication, and erasure coding.	xxx [GB|TB]
Effective Free	Displays the amount of usable free space after data reduction.	xxx [GB|TB]
Overall Efficiency	Displays the capacity optimization (as a ratio) that results from the combined effects of data reduction (deduplication, compression, and erasure coding), cloning, and thin provisioning.	xxx [GB|TB]
Capacity Deduplication	Displays whether on disk deduplication is enabled, that is dedup compression applied to data on hard disks (HDD).	[On, Off]
Filesystem Allowlists	Displays whether you have configured filesystem allowlist for this storage container.	[None, On, Off]
Erasure Coding	Displays whether erasure coding is enabled or not.	[On, Off]

Storage Pool Tab

Clicking the **Storage Pool** tab displays information about storage pools in the cluster.

- The table at the top of the screen displays information about the storage pool, and the details column (lower left) displays additional information when a storage pool is selected in the table. The following table describes the fields in the storage pool table and detail column.
- When a storage pool is selected, **Summary: *`storage_pool_name`*** appears below the table, and action links appear on the right of this line:
  - Click the **Update** link to update the settings for this storage pool.

  For more information about these actions, see Modifying a Storage Pool on page 138.
- Four tabs appear that display information about the selected storage pool (see following sections for details about each tab): **Storage Pool Usage**, **Storage Pool Performance**, **Storage Pool Alerts**, **Storage Pool Events**.

Table 36: Storage Pool Table and Detail Fields

Parameter	Description	Values
Storage Pool Table Fields (upper screen)		

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1985

Parameter	Description	Values
Name	Displays the name of the storage pool.	(name)
Disks	Displays the number of disks in the storage pool.	(number)
Free (Physical)	Displays the total amount of physical storage space that is available.	xxx [GB|TB]
Used (Physical)	Displays the total amount of physical storage space used in the storage pool.	xxx [GB|TB]
Max Capacity (Physical)	Displays the total physical storage space capacity in the storage pool.	xxx [TB]
Disk IOPS	Displays the current I/O operations per second (IOPS) for the storage pool. The IOPS, I/O bandwidth, and I/O latency fields record the I/O requests serviced by physical disks across the storage pool.	[0 - unlimited]
Disk IO B/W	Displays the I/O bandwidth used per second for physical disk requests in this storage pool.	xxx [MBps|KBps]
Disk Avg IO Latency	Displays the average I/O latency for physical disk requests in this storage pool.	xxx [ms]
Storage Pool Details Fields (lower screen)		
Name	Displays the name of the storage pool.	(name)
Free (Physical)	Displays the total amount of physical storage space that is available.	xxx [GB|TB]
Used (Physical)	Displays the total amount of physical storage space used in the storage pool.	xxx [GB|TB]
Capacity (Physical)	Displays the total physical storage space capacity in the storage pool.	xxx [TB]
Disk Count	Displays the number of disks in the storage pool.	(number)

Cluster Summary Information

When a storage pool, storage container, or volume group is not selected in the table (or when the word **Summary** is clicked), cluster-wide summary information appears in the lower part of the screen.

- The **Storage Summary** column (on the left) includes five fields:
  - **Available (Physical)**. Displays the amount of physical storage space still available in the cluster.
  - **Used (Physical)**. Displays the amount of physical storage space used currently in the cluster.
  - **Capacity (Physical)**. Displays the total physical storage capacity in the cluster.
  - **Storage Pool**. Displays the name of the storage pool in the cluster. Clicking the name displays detailed information about the storage pool in this section.
  - **Storage Container(s)**. Displays the names of the storage containers. Clicking a name displays detailed information about that storage container in this section.
- Four tabs appear that display cluster-wide information (see following sections for details about each tab): **Usage Summary**, **Performance Summary**, **Storage Alerts**, **Storage Events**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1986

Breakdown Tab

The **Breakdown** tab is displayed in the **Summary** section only when a storage container is selected from the storage container table.

The **Breakdown** tab displays the type (VM or VG), list of virtual disks, the amount of allocated space, and storage space utilized by each in the selected storage container.

Usage Tab

The Usage tab displays graphs of storage usage. The tab label varies depending on what is selected in the table:

- **Usage Summary** (no storage pool, storage container, or volume group selected). Displays usage statistics across the cluster.
- **Storage Container Usage** (storage container selected). Displays usage statistics for the selected storage container.
- **Storage Pool Usage** (storage pool selected). Displays usage statistics for the selected storage pool.
- **Volume Group Usage** (volume group selected). Displays usage statistics for the selected volume group.

The Usage tab displays the following two graphs:

- **Usage Summary**: Displays a rolling time interval usage monitor that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in depth analysis, you can add the monitor to the analysis page by clicking the blue link in the upper right of the graph. For more information, see Analysis Dashboard on page 334.
- **Tier-wise Usage**: Displays a pie chart divided into the percentage of storage space used by each disk tier in the cluster, storage pool, or storage container. Disk tiers can include DAS-SATA, SSD-SATA, and SSD-PCIe depending on the Nutanix model type.

Performance Tab

The Performance tab displays graphs of performance metrics. The tab label varies depending on what is selected in the table:

- **Performance Summary** (no storage pool, storage container, or volume group selected). Displays storage performance statistics across the cluster.
- **Storage Container Performance** (storage container selected). Displays storage performance statistics for the selected storage container.
- **Storage Pool Performance** (storage pool selected). Displays storage performance statistics for the selected storage pool.
- **Volume Group Performance** (volume group selected). Displays storage performance statistics for the selected volume group.

The graphs are rolling time interval performance monitors that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in depth analysis, you can add a monitor to the analysis page by clicking the blue link in the upper right of the graph. For more information, see Analysis Dashboard on page 334. The Performance tab includes the following three graphs:

- **[Cluster-wide Hypervisor|Controller|Disk] IOPS**: Displays I/O operations per second (IOPS) for the cluster, selected storage container, selected storage pool, or selected volume group.
- **[Cluster-wide Hypervisor|Controller|Disk] I/O Bandwidth**: Displays I/O bandwidth used per second (MBps or KBps) for physical disk requests in the cluster, selected storage container, selected storage pool, or selected volume group.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1987

- **[Cluster-wide Hypervisor|Controller|Disk] I/O Latency**: Displays the average I/O latency (in milliseconds) for physical disk requests in the cluster, selected storage container, selected storage pool, or selected volume group.

Alerts Tab

The Alerts tab displays the unresolved alert messages about storage pools, storage containers, or volume groups in the same form as the Alerts page. For more information, see Alerts Summary View. Click the **Unresolved X** button in the filter field to also display resolved alerts.

Events Tab

The Events tab displays the unacknowledged event messages about storage pools, storage containers, or volume groups in the same form as the Events page. For more information, see Events Summary View. Click the **Include Acknowledged** button to also display acknowledged events.

Modifying a Storage Pool

A storage pool is a defined group of physical disks that can be modified as the cluster changes. A storage pool is created automatically when the cluster is created.

About this task

You can only modify the name of the storage pool in the cluster. You cannot delete a storage pool.

To modify the name of the storage pool, do the following.

Procedure

1. Log on to the Prism Element web console.
2. Select **Storage** from the pull-down main menu (upper left of screen) and then select the **Table** and **Storage Pool** tabs.
3. To update the storage pool, select the target storage pool and then click the **Update** link.
   The **Update Storage Pool** window appears displaying the current name and capacity of the storage pool.
4. Enter the new name of the storage pool in the **Name** field.
5. Click **Save**.

Creating a Storage Container

A storage container is a subset of available storage within a storage pool. Storage efficiency features including compression, deduplication, and erasure coding are enabled at the container level.

Before you begin

- Ensure that the cluster is configured to synchronize time with NTP servers. For more information, see Configuring NTP Servers on page 354. Also, ensure that the time on the Controller VMs is synchronized and current. If the time on the Controller VMs is ahead of the current time, cluster services might fail to start. Files within the storage containers might also have timestamps ahead of the current time when viewed from the hypervisor.
- A storage pool and one storage container are created automatically when the cluster is created.
- A storage container is not created if you have not configured the Controller VMs with enough memory. Controller VM memory allocation requirements differ depending on the models and features that are being used. For more information, see CVM Memory Configuration on page 105.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1988

- For replication factor 1 storage container recommendations and limitations, see Replication Factor 1 on page 42.

About this task

AOS automatically creates the correct type of access to the storage container for each hypervisor.

- Hyper-V: The storage container is accessible as an SMB share.

  > **Note:** You cannot create a replication factor 1 storage container on clusters running Hyper-V.

- vSphere: The storage container is accessible as an NFS datastore. This requires access to the vSphere APIs. Ensure that you have appropriate license of vSphere to access the APIs.

  > **Note:** Nutanix supports NFS version 3 with ESXi.

- AHV: The storage container is accessible transparently.

To create a storage container, follow these steps:

Procedure

1. Log on to the Prism Element web console.
2. From the dropdown menu on the left of the main menu, select **Storage**.
   The system displays the **Storage** dashboard.
3. Click **+ Storage Container**.

   For more information on Storage dashboard, see Storage Dashboard on page 124.

   The system displays the **Create Storage Container** dialog box.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1989

4. Enter the following in the indicated fields:

   a. **Name**: Enter a name for the storage container.

   > **Note:** This entity has the following naming restrictions across various hypervisors.
   >
   > **AHV**:
   >
   > - Container Name Length: Maximum length is 75 characters.
   > - Supported Characters: Uppercase and lowercase standard Latin letters (A-Z and a-z), Simplified Chinese, decimal digits (0-9), dots (.), hyphens (-), hash (#), and underscores (_).
   > - Case Sensitivity: Container names are case sensitive.
   >
   > **ESXi**:
   >
   > - Container Name Length: Maximum length is 42 characters.
   > - Supported Characters: Uppercase and lowercase standard Latin letters (A-Z and a-z), Simplified Chinese, decimal digits (0-9), dots (.), hyphens (-), hash (#), and underscores (_).
   > - Case Sensitivity: Container names are case sensitive.
   >
   > **Hyper-V**:
   >
   > - Container Name Length: Maximum length is 32 characters.
   > - Supported Characters: Uppercase and lowercase standard Latin letters (A-Z and a-z), decimal digits (0-9), dots (.), hyphens (-), and underscores(_).
   > - Case Sensitivity: Container names are case insensitive. For example, if there is a container with name *ABCD*, then creating another container with name *abcd* is restricted.

   b. **Storage Pool**: Select a storage pool from the drop-down list.

      The following field, **Max Capacity (Physical)**, displays the amount of free physical space available in the selected storage pool.

   c. (vSphere only) **NFS Datastore**: Select the **Mount on all ESXi hosts** button to mount the storage container on all hosts. Select the **Mount on the following ESXi hosts** button to mount the storage container on a subset of hosts, which displays a list of host IP addresses below this field. Check the boxes of the hosts to be included.

   d. (Hyper-V only) Set this storage container as default store for VMs on Hyper-V hosts.

Depending on your selection, the Create Virtual Machine Wizard of Hyper-V automatically populates the storage location with the relevant storage container.

Option	Description
Make default on all Hyper-V hosts	Makes this storage container a default location for storing virtual machine configuration and virtual hard disk files on all the Hyper-V hosts.
Make default on particular Hyper-V hosts	Provides you with an option to select the hosts to make this storage container a default location for storing virtual machine configuration and virtual hard disk files on all the Hyper-V hosts.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1990

5. To configure additional parameters, click the **Advanced Settings** button.

   Enter the following in the indicated fields:

   a. **Cluster Fault Tolerance** *(Read-Only)*: Displays the fault tolerance of the cluster that you configured when you created the cluster.

   b. **Replication Factor**: Displays the number of copies of data in the container.

      The default value is based on the cluster fault tolerance that you select when you create the cluster. For more information on cluster fault tolerance, see Cluster Fault Tolerance on page 25.

      To modify the replication factor, select the value from the dropdown menu. You can set the replication factor to 1, 2, or 3 depending on the fault tolerance of the cluster. For more information on replication factor, see Replication Factor on page 41.

      Note:

      - You can modify the replication factor of a container in a cluster with 1N&1D or 2N/2D cluster fault tolerance. You cannot modify the replication factor of a container in a cluster with 1N/1D cluster fault tolerance; however, you can modify the replication factor of the container after you increase the fault tolerance of the cluster from 1N/1D to 2N/2D. For more information, see Increasing the Cluster Fault Tolerance Level on page 76.
      - Nutanix supports a replication factor of 1, 2, or 3. Nutanix supports a replication factor of 1 if you enable the replication factor 1 setting only. For more information, see Enabling Replication Factor 1 on page 145. If you do not enable the replication factor 1 setting, Nutanix supports a replication factor of 2 or 3 depending on the fault tolerance configured in the cluster. Setting the replication factor to 3 adds an extra layer of data protection at the cost of storing an additional copy of the data.

   c. **Reserved Capacity (Logical)**: To reserve storage space for this storage container, enter the amount (in GiB) to reserve in this field.

      Reserved Capacity (Physical) *(Read-Only)*: Displays the amount of physical capacity that is reserved based on the logical reserved capacity value.

      You can reserve space for a storage container to ensure a minimum storage capacity is available. Reserving space for a storage container means that space is no longer available to other storage containers even if the reserved space is unused. For more information, see Capacity Reservation Best Practices on page 112.

   d. **Advertised Capacity (Logical)**: Sets a maximum storage space for this storage container, enter the amount (in GiB) to reserve in this field.

      Advertised Capacity (Physical) *(Read-Only)*: Displays shows the amount of physical capacity that is advertised based on the logical advertised capacity value.

      This sets an *advertised* capacity, which is the maximum storage size that the storage container can use. This can be set to any value, but if a reserved capacity is configured, it must be set greater than or equal to the reservation on the storage container. The hypervisor ensures that the storage container storage does not go beyond the advertised capacity. When a storage container reaches a threshold percentage of the actual storage pool size, an alert is issued.

   e. **Compression**: By default, this checkbox is selected.

      Inline compression is enabled by default with the **Delay (In Minutes)** field set to 0. A value of 0 means that data is compressed immediately as it is written. The delay time between write and compression is configurable. For post-process compression, where data is compressed after it is written, Nutanix recommends a delay of 60 minutes. Compression is delayed for 60 minutes after the initial write operation. All data in the storage

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1991

container is compressed when you select **Compression**. For information about using compression, see Compression on page 118.

f. **Deduplication**: Select the **Capacity** checkbox to perform post-process deduplication of persistent data.

Nutanix recommends this option primarily for full clone, persistent desktops, and physical to virtual migration use cases that need storage capacity savings (not just performance savings from deduplication). Nutanix further recommends that the Controller VMs have at least 32GB of RAM and 300GB SSDs for the metadata disk to use this option.

> **Note:** Deduplication is not available when you select **Replication Factor** as 1.

g. **Erasure Coding**: Select the **Enable** checkbox to enable erasure coding.

Erasure coding increases the effective or usable capacity on a cluster. For more information about erasure coding, see Erasure Coding on page 118.

> **Note:** Erasure coding is not available when you select **Replication Factor**as 1.

h. **Filesystem Whitelists**: Enter the comma-separated IP address and netmask value (in the form `ip_address/ netmask`).

A whitelist is a set of addresses that are allowed access to this storage container. Whitelists are used to allow appropriate traffic when unauthorized access from other sources is denied. Setting a storage container level whitelist overrides any global whitelist for this storage container.

Setting an allowlist helps you provide access to the container via NFS. Some manual data migration workflows might require the allowlist to be configured temporally, while some third-party backup vendors might require the allowlist to be configured permanently to access the container via NFS.

> **Caution:**
>
> - User authentication is not available for NFS access, and the IP address in the allowlist has full read or write access to the data on the container.
> - Nutanix recommends to allow single IP addresses (with net mask such as 255.255.255.255) instead of allowing subnets (with netmask such as 255.255.255.0).

6. Click the **Save** button.

Modifying a Storage Container

A storage container is a defined subset of available storage within a storage pool that can be modified as conditions change.

Before you begin

- The *NutanixManagementShare* container is an internal storage container for Nutanix products and services. To ensure seamless operations, external users should avoid accessing, modifying, or deleting this storage container. The *NutanixManagementShare* storage container is not intended to store user data and vDisks, including Nutanix Volumes.
- The web console does not allow you to rename a storage container in an AHV cluster when modifying container details through the **Update Storage Container** dialog box. You cannot rename a storage container if it contains vdisks.

About this task

Storage Containers can be modified to change how the data in that storage container is handled, for example to apply compression.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1992

To modify (or delete) a storage container, do the following:

Procedure

1. Log on to the Prism Element web console.
2. Select **Storage** from the pull-down main menu (upper left of screen) and then select the **Table** and **Storage Container** tabs.
3. To update the storage container, select the target storage container and then click the **Update** link.
   The **Update Storage Container** window appears, which includes the same fields as the **Create Storage Container** window. For more information, see Creating a Storage Container on page 138. Through this window you can specify NFS datastore mounts, reserve storage capacity, enable (or disable) compression, enable or disable erasure coding, select or deselect fingerprinting on writes which enables deduplication on reads, and configure filesystem allowlist.

   Note:

   - For ESXi clusters, if you make changes to any of the parameters that impact the storage container size (such as Advertised Capacity), the information does not get refreshed in the vCenter ESXi nodes by default. You must right-click the container in vCenter and select **Refresh Capacity Information** to refresh the capacity.
   - If the compression policy is changed from compressed to uncompressed (or vice versa), the existing compressed (uncompressed) data in the storage container will be uncompressed (compressed) as a background process when the next data scan detects the data that needs this change.
   - The Prism Element web console does not provide an option to change the container replication factor. That can be done only through the nCLI. For more information, see Increasing the Cluster Fault Tolerance Level on page 76.

4. To delete the storage container, select the target storage container, and then click the **Delete** link.

Replication Factor Configuration

This section describes how to configure the replication factor for a storage container in a Nutanix cluster.

The replication factor of a storage container depends on the fault tolerance of the cluster. The default replication factor of a container in a cluster is based on the cluster fault tolerance that you select when you create the cluster. For example, if you select the fault tolerance of a cluster as 1N&1D when you create the cluster, the system configures replication factor 3 for the storage containers in the cluster, by default.

You can modify the replication factor of a container in a cluster with 1N&1D or 2N/2D cluster fault tolerance. For more information, see Creating a Storage Container on page 138. You cannot modify the replication factor of a container in a cluster with 1N/1D cluster fault tolerance; however, you can modify the replication factor of the container after you increase the fault tolerance of the cluster from 1N/1D to 2N/2D. For more information, see Increasing the Replication Factor using CLI.

To enable or disable replication factor 1, see Enabling Replication Factor 1 on page 145 or Disabling Replication Factor 1 on page 146.

Increasing the Replication Factor using CLI

After you increase the fault tolerance in a cluster to 2N/2D, you must increase the replication factor for the storage containers in the cluster to ensure that all storage containers have three copies of the data. This topic describes how to increase the replication factor to 3.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1993

Before you begin

Ensure that you have increased the cluster fault tolerance to 2N/2D. For more information, see Increasing the Cluster Fault Tolerance Level on page 76.

About this task

To increase the replication factor to 3 using CLI, follow these steps:

Procedure

1. Log in to the Controller VM and type the following command.

```
nutanix@cvm$ ncli
```

2. To locate the storage containers that requires an update, run the following command.

```
ncli> ctr list
```

An output similar to the following is displayed.

```
 Id                        : 00052e5a-bc71-2112-0000-00000000261a::11
                                 Uuid                      : c49eb9af-2eba-41b1-
bae5-08227f7cff13
                                 Name                      : storage_container_name
                                 Storage Pool Id           : 00052e5a-
bc71-2112-0000-00000000261a::10
                                 Storage Pool Uuid         : b785ff57-9d53-4f05-
bad7-3ac3587f2960
                                 Free Space (Logical)      : 10.29 TiB
 (11,316,325,361,581 bytes)
                                 Used Space (Logical)      : 0 bytes
                                 Allowed Max Capacity      : 10.29 TiB
 (11,316,325,361,581 bytes)
                                 Used by other Containers  : 0 bytes
                                 Explicit Reservation      : 0 bytes
                                 Thick Provisioned         : 0 bytes
                                 Replication Factor        : 2
                                 Oplog Replication Factor  : 2
                                 NFS Whitelist Inherited   : true
                                 Container NFS Whitelist   :
                                 VStore Name(s)            : default-container-9754
                                 Random I/O Pri Order      : SSD-PCIe, SSD-SATA, DAS-
SATA
                                 Sequential I/O Pri Order  : SSD-PCIe, SSD-SATA, DAS-
SATA
                                 Compression               : off
                                 Fingerprint On Write      : off
                                 On-Disk Dedup             : none

                                 Erasure Code              : off
```

3. To set the replication factor to 3 for each target storage container, run the following command.

```
ncli> ctr edit name=storage_container_name rf=3
```

Replace *storage_container_name* with the name of the storage container.

Output similar to the following is displayed. This shows that the replication factor is now at the correct state (3) for the storage container.

```
    Id                        : 00052e5a-bc71-2112-0000-00000000261a::1381
                                    Uuid                      : a567b66d-
b356-4883-90c5-c37b2f3e0fad
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1994

```
                                  Name                      : storage_container_name
                                  Storage Pool Id           : 00052e5a-bc71-2112-0000-00000000261a::10
                                  Storage Pool Uuid         : b785ff57-9d53-4f05-bad7-3ac3587f2960
                                  Free Space (Logical)      : 6.86 TiB (7,544,216,907,720 bytes)
                                  Used Space (Logical)      : 0 bytes
                                  Allowed Max Capacity      : 6.86 TiB (7,544,216,907,720 bytes)
                                  Used by other Containers  : 0 bytes
                                  Explicit Reservation      : 0 bytes
                                  Thick Provisioned         : 0 bytes
                                  Replication Factor        : 3
                                  Oplog Replication Factor  : 3
                                  NFS Whitelist Inherited   : true
                                  Container NFS Whitelist   :
                                  VStore Name(s)            : aaa
                                  Random I/O Pri Order      : SSD-PCIe, SSD-SATA, DAS-SATA
                                  Sequential I/O Pri Order  : SSD-PCIe, SSD-SATA, DAS-SATA
                                  Compression               : off
                                  Fingerprint On Write      : off
                                  On-Disk Dedup             : none

                                  Erasure Code              : off
```

Important: Ensure that you increase the replication factor to 3 for all target containers, including containers created by the system such as the SelfServiceContainer or NutanixManagementShare.

To set replication factor 3 for the system storage container NutanixManagementShare, run the following command:

```
ncli> ctr edit name=NutanixManagementShare rf=3 force=true
```

What to do next

The system might take some time to increase the replication factor. Verify the status by viewing the **Cluster Resiliency / Fault Tolerance Status** widget in the dashboard of the Prism Element web console. When the value of **Failures Tolerable** for **Extent Group** (which reflects the container replication level) increases to 2, it confirms that the replication factor for the cluster is 3.

Enabling Replication Factor 1

To enable replication factor 1, first enable the replication factor 1 setting, and then create a dedicated replication factor 1 enabled storage container and associate the replication factor 1 enabled storage container with one node.

About this task

After the replication factor for a container is set to 1, you cannot increase the replication factor on that container.

Before you begin

See Replication Factor 1 on page 42.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1995

Procedure

1. Log on to the Prism Element web console.
2. From the dropdown menu on the left of the main menu, select **Settings**.
   The system displays the **Global Settings** page.
3. From the **Data Resiliency** section in the left navigation pane, click **Cluster Fault Tolerance**.
   The **Cluster Fault Tolerance** page opens, displaying the existing cluster fault tolerance.
4. Select the **Allow selection of Replication Factor 1 on Storage Containers** checkbox.
   The system prompts you to confirm the action.
5. Click **Yes** to confirm the action, and then click **Save**.

What to do next

Create a replication factor 1 enabled storage container and assign it to a node. For more information, see Creating a Storage Container on page 138.

Disabling Replication Factor 1

About this task

Disabling replication factor 1 prevents you from creating a new replication factor 1 enabled storage container. Any existing replication factor 1 enabled containers with associated vDisks remain in place.

Procedure

1. Log on to the Prism Element web console.
2. From the dropdown menu on the left of the main menu, select **Settings**.
   The system displays the **Global Settings** page.
3. From the **Data Resiliency** section in the left navigation pane, click **Cluster Fault Tolerance**.
   The **Cluster Fault Tolerance** page opens, displaying the existing cluster fault tolerance.
4. Clear the **Allow selection of Replication Factor 1 on Storage Containers** checkbox and then click **Save**.
   After disabling replication factor 1, if you create or modify a storage container, your replication factor choices are 2 or 3.

Volume Group Configuration

A volume group is a collection of virtual disks (vDisks). Each volume group is identified by a name and UUID. Each vDisk has a UUID and a SCSI index to specify the ordering of disks within the volume group.

You create a volume group on a storage container and enable access to the volume group in one of the following ways:

iSCSI

iSCSI access to a volume group is provided through Nutanix Volumes. For more information, see the Nutanix Volumes Guide.

Attach Directly to a VM

If the hypervisor is AHV, you can create a volume group and attach it to one or more VMs as a SCSI disk by using the Prism Element web console, the Nutanix REST API, or the nCLI or aCLI commands.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1996

Once the volume group is attached to the VM by using the Prism Element web console, vDisks appear as SCSI devices to the guest operating system. AOS transparently handles load balancing and path resiliency on the guest VM. Directly attached volume groups support Controller VM failover and do not impact VM migration.

You can attach a volume group to a VM at any time. This option is available only to VMs deployed on AHV.

This method of attaching a volume group to a VM has the following limitations:

- The VM must run on the same cluster as the volume group.

Volume groups are managed independently of the VMs to which they are attached. You can configure a directly attached volume group for access by a single VM (exclusive access) or by multiple VMs (shared access).

> **Caution:** Multiple VMs writing to a vDisk that belongs to a shared volume group without additional software to manage the access can lead to data corruption. Use shared access when you are configuring VMs for use with cluster aware software.

Concurrent Access from Multiple Clients

Products, features, or solutions might require concurrent access to volume groups, either by multiple iSCSI initiators or multiple VM attachments.

Multiple iSCSI Initiators

The following products, features, or solutions are supported for concurrent access to volume groups:

- Oracle RAC (bare-metal and virtualized environments)
- Linux VMs
- Windows Failover Clustering
- IBM Spectrum Scale (GPFS)
- Veritas InfoScale Storage

Multiple Directly Attached VMs

The following products, features, or solutions are supported for concurrent access to volume groups:

- Oracle RAC
- Linux VMs
- IBM Spectrum Scale (GPFS)
- Veritas InfoScale Storage
- Windows Failover Clustering
- Linux guest VM clustering (also known as RHEL HA)

Creating a Volume Group

About this task

To create a volume group, do the following:

Procedure

1. Log on to the Prism Element web console.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1997

2. In the **Storage** dashboard, click the **+ Volume Group** button.
   The **Create Volume Group** dialog box is displayed.

3. In **Name**, enter a name for the volume group.

   Note: This entity has the following naming restrictions:

   - The maximum length is 75 characters.
   - Allowed characters are uppercase and lowercase standard Latin letters (A-Z and a-z), decimal digits (0-9), dots (.), and hyphens (-).

4. The **iSCSI Target Name Prefix** is auto-filled with the volume group **Name**. You can accept this prefix or enter your own target name prefix for the volume group. This entity has the same naming restrictions as **Name**.

5. In **Description**, enter a description for the volume group.

6. To add a disk to the volume group, do the following:

   a. In the **Storage** section, click **Add New Disk**.

   b. In the **Add Disk** dialog box, in **Storage Container**, select the storage container to use from the pull-down list.

   c. In **Logical Size (GiB)**, enter the disk size in GiBs.

   d. Click **Add**.

   e. Repeat these steps to add another disk for this volume group, if desired.

7. Do the following in the **Access Settings** section:

   a. Select the **Enable external client access** checkbox if you are allowlisting clients that are external to or not residing in this cluster.

   If you select this checkbox, it remains selected the next time you create a volume group.

   b. If you are using one-way CHAP security, select the **CHAP Authentication** checkbox and type a 12-character to 16-character password (also known as a CHAP secret) in the **Target Password** field.

   Initiators must use the same password to authenticate to the AOS cluster.

   c. Click **Add New Client** to configure the iSCSI initiators, and then enter the client Initiator iSCSI Qualified Name (IQN) in the **Client IQN/IP Address** field to create the allowlist. If you have configured Mutual CHAP authentication on the client, select **CHAP Authentication** and enter the iSCSI client password (secret). Click **Add**.

   Note: Ensure that you enter the client IQN in the **Client IQN/IP Address** field and not the IP address. AOS does not support an allowlist containing IP addresses in a volume group.

   Access Control displays any configured clients. This list includes any clients attached to volume groups in the cluster. Repeat this step to add more initiators allowed to access this storage. For information about which products, features, or solutions are supported for concurrent access to a volume group, see Concurrent Access from Multiple Clients on page 147.

8. To enable the Flash Mode feature, select **Enable Flash Mode**.

   Note: Individual virtual disks of a volume group cannot be excluded from Flash Mode by using the Prism Element web console. However, you can exclude individual virtual disks from flash mode by using aCLI. For more information, see Removing Flash Mode for Virtual Disks of a Volume Group on page 152.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1998

9. Click **Save**.

What to do next

If the hypervisor is AHV, you can now attach the volume group to the VM and start using the vDisks. If you want to use iSCSI and you already allowlisted the host IP addresses, log on to the VMs, and configure iSCSI.

Modifying or Deleting a Volume Group

About this task

To modify a volume group, do the following:

Procedure

1. Log on to the Prism Element web console.
2. Select **Storage** from the pull-down main menu (upper left of screen), and then select the **Table** and **Volume Group** tabs.
3. To update a volume group, select the volume group, and then click the **Update** link.
   The **Update Volume Group** window appears, which includes the same fields as the **Create Volume Group** window. For more information, see Creating a Volume Group on page 147. In this window you can change the volume group name, add and remove disks, configure the volume group for sharing, and add or remove (by clearing) entries from the initiator allowlist. On AHV clusters, you can attach the volume group to a VM as a SCSI disk (described later in this procedure). If you attach a volume group to a VM that is part of a Protection Domain, the volume group is not protected automatically. Add the volume group to the same Consistency Group manually.

   You can increase the size of the volume group. Reducing the size of a volume group is not supported.

   Any unchecked initiator that remains unused by this or any other volume group ultimately disappears from this list.
4. To attach a volume group to a VM, click **Attach to a VM**, and then select the VM from the **Available VMs** list.
5. To manage the iSCSI client list, click the **Summary** link to deselect any volume groups, and then click the **Manage Initiators** link. (This link appears only when no volume groups are selected.)

   The **Manage iSCSI Clients** window appears, which includes a list of the clients and available actions. To modify a client (enable/disable CHAP authentication), click the pencil icon for that client, which displays the **Edit iSCSI client** window. For more information, see the Nutanix Volumes Guide.
6. After updating a volume group, click **Save**.

Deleting a Volume Group

Procedure

1. If any iSCSI clients are attached to the volume group, first disconnect or detach the AOS cluster target for each iSCSI initiator from the iSCSI client (for example, from the Windows or Linux client). See your vendor documentation for specific disconnection procedures.
2. In the web console, select **Storage** from the pull-down main menu (upper left of screen), and then select the **Table** and **Volume Group** tabs.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 1999

3. To detach any iSCSI clients attached to the volume group, first update the volume group by doing these steps. You might need to scroll down the dialog box. If no clients are attached, skip this step.

   a. Select the volume group and click **Update**.

   b. Clear the **Enable External Client Access** checkbox and clear any clients listed in the **Clients** section.

   c. Click **Save**.

4. To delete a volume group, select the volume group, and then click **Delete**.

5. Click **Delete** again to confirm.

Cloning a Volume Group

About this task

To clone a volume group, perform the following steps.

Procedure

1. Log on to the Prism Element web console.

2. Select **Storage** from the drop-down main menu (upper left of screen), and then select **Table** > **Volume Group**. The system displays a list of volume groups created in the cluster.

3. Select the volume group that you want to clone and click **Clone**.
   This displays the **Clone Volume Group** window.

4. Enter the necessary values in the respective fields.

   The fields in the **Clone Volume Group** window is identical to the fields in the **Create Volume Group** window. For more information, see Creating a Volume Group on page 147.

5. Click **Save**.

Flash Mode for Virtual Machines, Disks, and Volume Groups

Flash mode for VM allows you to set the storage tier preference to SSD for a virtual machine or volume group. Flash mode is not enabled by default for all database deployments. But, flash mode allows latency sensitive workloads to remain on the SSD tier and avoid any potential performance impact of down migration of data.

By default, you can use up to 25% of the cluster-wide SSD tier as flash mode space for VMs or VGs. If the data size for flash mode enabled VMs or VGs exceeds 25% of the SSD capacity, the system may down migrate the data. Before performing down-migration, the flash mode feature tries to preserve the excess data on the SSD tier for some reasonable amount of time so that you can take corrective actions on the cluster and bring back to stable state. To reduce flash mode usage, you can disable flash mode on some VMs or VGs or add SSDs.

> **Note:** For information about minimum SSDs requirement for Hybrid HCI Node and All-Flash HCI Node, see HCI Node Field Requirements topic in *Acropolis Advanced Administration Guide*.

If you enable this feature on a VM, all the virtual disks that are attached to the VM are automatically placed on the SSD tier. Also, virtual disks added to this VM are automatically placed on SSD. However, you can update the VM configuration to remove the flash mode from any virtual disks.

You can enable the feature on the VM and VM disks only during the VM update workflow from the Prism Element. For information on how to enable the feature on VMs, see 11 on page 284. However, for VGs, you can enable the feature during the creation of VGs. For information on how to enable the feature on VGs, see Creating a Volume Group on page 147.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2000

Caution: While enabling the flash mode feature for a VM may increase the performance of that VM, it may also lower the performance of VMs that do not have flash mode feature enabled. Nutanix recommends you to consider the performance impact on other VMs and VGs. To mitigate any impact on the performance, you can update the VM configuration and remove the flash mode on individual virtual disks. For example, you can enable flash mode on the applications data disks and disable it on the log disks.

A node failure may cause a reduction in SSD tier capacity that can drive the flash mode usage above the 25% of the tier capacity. In this event, alerts will report the flash usage exceeding 25%.

Note:

- This feature is supported on ESXi and AHV for VMs and on all the hypervisors for VGs.
- For the cluster created using ESXi hosts, you must register your cluster with the vCenter Server. For more information, see Registering a Cluster to vCenter Server on page 366.

Alerts are raised in the following scenarios.

- When the flash usage exceeds 25% of the SSD tier.
- When the VM has the flash mode feature enabled but is in the powered off state.

Conditions for the Flash Mode feature

- If a VM or a VG with flash mode feature enabled is cloned, then the flash mode policies are not automatically applied to the cloned VM or VG.
- The flash mode policies are not automatically applied if a VM or VG is restored from the DR snapshot on the local or the remote site.
- The flash mode policies can be used for controlling down migration from the hot tier to the cold tier. The policies do not restrict the usage for the VM or VG on the hot tier. If space is available on the hot tier, more data from the VM or VG can reside on the hot tier.
- If you enable erasure coding on the cluster, the parity resides on the HDD tier.
- If you replicate a VM or VG to a remote site (by using Metro Availability or Async DR), the remote site does not have flash mode feature enabled automatically. You need to manually enable the flash mode feature again.
- Do not use flash mode feature with capacity tier deduplication. Enabling flash mode feature does not affect performance tier deduplication.
- If you perform a storage migration or storage vMotion, the new virtual disk created on the target datastore will not have the flash mode feature enabled. You need to manually enable the flash mode feature again.
- If you try to upgrade from an AOS version lower than 5.0 to version 5.0 or higher with SSD pinning feature enabled, the upgrade process is blocked. Hence, ensure that you have disabled the SSD pinning feature before performing an upgrade. Also, do not enable the SSD pinning feature during the upgrade process.
- Flash mode is not supported with more than one storage pool in the cluster. If you delete and then create a storage pool in your cluster, you cannot configure the flash mode feature for a small duration of time. In this duration there are two storage pools in the cluster temporarily and the flash mode feature cannot be enabled.
- If you enable flash mode on all-NVMe clusters or a cluster with one or more NVMe, it may result in the following error.

  ```
  Update failed: NfsConfigVDisk RPC returned kInvalidValue: kInvalidValue: 'SSD-SATA'
   supplied for tier params has no associated disk.
  ```

  This error can be safely ignored for all-NVMe clusters and clusters which contain NVMe and/or SSD because the flash mode feature only pins data to the SSD tier and prevents down-migration to the HDD tier. For all-NVMe

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2001

clusters that have neither SSD nor HDD tier and for clusters which have NVMe and any number of HDDs, this error will prevent flash mode from being enabled.

Removing Flash Mode for Virtual Disks of a Volume Group

Individual virtual disks of a volume group cannot be excluded from flash mode by using Prism. However, you can exclude individual virtual disks from flash mode by using aCLI.

Procedure

1. Log in to the Controller VM in your cluster through an SSH session and access the Acropolis command line.
2. (Optional) If you have not enabled the flash mode feature for the VG by using Prism, you can enable it by running the following command.

   ```
   acli> vg.update vg_name flash_mode=true
   ```

   Replace `vg_name` with the name of the VG on which you want to enable the flash mode.
3. Remove the flash mode feature on a particular disk.

   ```
   acli> vg.disk_update vg_name index_value flash_mode=false
   ```

   Replace `vg_name` with the name of the VG and `index_value` with the index value of the VG. For example to disable flash mode for disk at index 0 with name example_vg, use the following command.

   ```
   acli> vg.disk_update example_vg 0 flash_mode=false
   ```

Recycle Bin

Enabled by default and with help from Nutanix Support, the Recycle Bin helps you manage and restore deleted storage entities like guest VMs and volume group vDisks.

> **Note:** To restore a storage entity, contact Nutanix Support.

> **Note:** When Replication Factor 1 is enabled for a storage container, the recycle bin is disabled for that storage container. When you delete a storage entity like a guest VM or volume group vDisk, it is marked for deletion as soon as possible and bypasses the recycle bin. For more information, see Replication Factor on page 41.

When the Recycle Bin is enabled, AOS creates a Recycle Bin associated with the storage container configured in your cluster. If you then delete a storage entity (like a guest VM or volume group vDisk), the Recycle Bin retains vDisk and configuration data files for up to 24 hours.

If you enable the Recycle Bin and then delete a guest VM or volume group vDisk, it retains its contents (deleted vDisks and configuration information) for up to 24 hours, unless the cluster free storage space reaches critical thresholds. After 24 hours, AOS automatically deletes these files. AOS deletes the files in less than 24 hours if your cluster is unable to maintain sufficient free disk space. AOS triggers free disk space alerts when your cluster reaches critical thresholds.

After you disable the Recycle Bin, AOS automatically deletes any entities in the Recycle Bin after 24 hours. Then, when you subsequently delete any storage entities, AOS marks them for deletion as soon as possible. They are not stored in the storage container Recycle Bin folder.

After deleting one or more storage entities, the **Free** storage space shown in the Prism Element web console might not update for 24 hours. To see the space used by the Recycle Bin in the Storage Summary, go to the web console **Storage** dashboard and select the **Diagram** or **Table** view.

For more information about Recycle Bin behavior, see Recycle Bin Limitations and Considerations on page 153.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2002

Recycle Bin Limitations and Considerations

Limitations and guidelines to consider when using the Recycle Bin.

- The Recycle Bin stores vDisk and configuration data for up to 24 hours. After 24 hours, these files are deleted. The files are deleted in less than 24 hours if your cluster is unable to maintain sufficient free disk space.

  The Recycle Bin is temporarily disabled when the Recycle Bin is using more than five percent of cluster storage capacity. AOS triggers free disk space alerts when your cluster reaches critical thresholds. In this case, newly-deleted entities are marked them for deletion as soon as possible. They are not stored in the storage container Recycle Bin folder.

  When the Recycle Bin is cleared manually or automatically and the Recycle Bin is using two percent or less of cluster storage capacity, Recycle Bin is automatically re-enabled and available for use after all Curator service scans are completed. (Among other cluster tasks, the Curator service controls Recycle Bin and storage cleanup.)

- If the Recycle Bin contains more than 2000 files, deleted storage entities guest VMs and volume group vDisks bypass the Recycle Bin. AOS marks them for deletion as soon as possible. They are not stored in the storage container Recycle Bin folder.

- The web console displays the **Clear Recycle Bin** (available on the **Storage** dashboard in Summary view) or **Clear Space** options (available in **Storage Details**) only if the Recycle Bin contains deleted items. If these options are available but the space used by the Recycle Bin is 0, AOS has detected the items but not yet calculated the storage space used.

- After you empty the Recycle Bin with **Clear Recycle Bin** or **Clear Space** or AOS empties the Recycle Bin, these options are not displayed again until you delete storage entities like guest VMs and volume group vDisks.

- When Replication Factor 1 is enabled for a storage container, the recycle bin is disabled for that storage container. When you delete a storage entity like a guest VM or volume group vDisk, it is marked for deletion as soon as possible and bypasses the recycle bin. For more information, see Replication Factor on page 41

- Recycle Bin is not supported on storage containers where metro availability is enabled.

- Recycle Bin is not available for recovering protection domain snapshots.

- When you delete a VM with a thick provisioned vDisk reservation setting, the setting is removed. After recovering this VM, the reservation is not restored and defaults to thin provisioned.

- If you are using the X-Ray application, an automated testing framework and benchmarking application for enterprise-grade datacenters, you must disable the Recycle Bin on your AOS cluster, which is enabled by default.

Enabling and Disabling the Recycle Bin

The Recycle Bin is enabled by default. You can turn the Recycle Bin on or off through the Cluster Details window in the web console.

Procedure

1. Log on to the Prism Element web console.
2. Click the gear icon in the main menu and then select **Cluster Details** in the **Settings** page.
3. To disable the Recycle Bin, clear the **Retain Deleted VMs for 24h** checkbox.

   After you disable the Recycle Bin, AOS automatically deletes any entities in the Recycle Bin after 24 hours. Then, when you subsequently delete any storage entities, AOS marks them for deletion as soon as possible. They are not stored in the storage container Recycle Bin folder. See also Recycle Bin on page 152.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2003

4. To enable the Recycle Bin, select the **Retain Deleted VMs for 24h** checkbox.

   If you enable the Recycle Bin and then delete a guest VM or volume group vDisk, it retains its contents (deleted vDisks and configuration information) for up to 24 hours, unless the cluster free storage space reaches critical thresholds.

5. Click **Save** to save the values and close the window.

Viewing Space Used by the Recycle Bin

The Prism Element web console shows the space used by the Recycle Bin in the Storage dashboard.

Before you begin

See also Storage Overview View on page 125, Storage Diagram View on page 127, and Storage Table View on page 131.

Procedure

1. Log on to the Prism Element web console.
2. Go to the **Storage** dashboard by clicking **Home** > **Storage**.
3. To view the space used by the Recycle Bin, click the **Diagram** or **Table** tab.
   The Storage Summary panel shows the space used by the Recycle Bin. If the **Clear Recycle Bin** option is available but the space used by the Recycle Bin is 0, AOS has detected the deleted items but not yet calculated the storage space used.
4. Also, from the **Home** dashboard, at the **Storage Summary** widget, click **View Details**.
   The Recycle Bin shows the space used. If the **Clear Space** option is available but the space used by the Recycle Bin is 0, AOS has detected deleted items but not yet calculated the storage space used.

Clearing Storage Space Used by the Recycle Bin

You can clear the storage space used by the Recycle Bin from the Home or Storage dashboards.

Before you begin

See also Storage Table View on page 131. Do these steps from the Prism Element web console.

- The web console displays the **Clear Recycle Bin** (available on the **Storage** dashboard in Summary view) or **Clear Space** options (available in **Storage Details** from the **Storage Summary** widget) only if the Recycle Bin contains deleted items. If these options are available but the space used by the Recycle Bin is 0, AOS has detected the items but not yet calculated the storage space used.
- After you empty the Recycle Bin with **Clear Recycle Bin** or **Clear Space** or AOS empties the Recycle Bin, these options are not displayed again until you delete storage entities like guest VMs and volume group vDisks.

Procedure

1. Log on to the Prism Element web console.
2. From the **Home** dashboard: at the **Storage Summary** widget, click **View Details**.
   a. Under Recycle Bin, click **Clear Space**.
   b. In the confirmation pop-up, click **Delete**.
      You cannot undo this action. Any entities in the Recycle Bin are marked for deletion immediately.
   c. Click **Close**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2004

3. From the **Storage** dashboard: Click the **Table** tab.

   a. To clear the space used by the Recycle Bin, Click **Clear Recycle Bin**.

   b. In the confirmation pop-up, click **Delete**.
   You cannot undo this action. Any entities in the Recycle Bin are marked for deletion immediately.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2005

NETWORK MANAGEMENT

Nutanix provides several features to manage and monitor network settings for the cluster.

- To configure network connections in clusters through the web console with Nutanix virtualization management (such as those running AHV as the hypervisor), see Network Configuration for Cluster on page 156.
- To enable LAG and LACP on the T0R switch, see Enabling LACP and LAG (AHV Only) on page 174.
- To configure the network interfaces for a VM, see Network Configuration for VM Interfaces on page 167.
- To track and record networking statistics for a cluster, the cluster requires information about the first-hop network switches and the switch ports being used. You can configure one or more network switches for statistics collection. For more information, see Configuring Network Switch Information on page 172.
- A network visualizer is provided that presents a consolidated graphical representation of the network formed by the VMs and hosts in a Nutanix cluster and first-hop switches. You can use the visualizer to monitor the network and to obtain information that helps you troubleshoot network issues. For more information, see Network Visualization on page 178.

Network Configuration for Cluster

You can view and configure network connections for the cluster in the **Network Configuration**. To display the **Network Configuration** page, click the gear icon in the main menu and then select **Network Configuration** in the **Settings** page.

Network Connections

Each VM network interface is bound to a virtual network, and each virtual network is bound to a single VLAN. Information about the virtual networks configured currently appears in the **Network Configuration** page.

The **Network Configuration** page includes three tabs.

- The **Subnets** tab displays a list of the configured networks.
- The **Internal Interfaces** tab displays a list of LAN interfaces.
- The **Virtual Switch** tab displays a list of virtual switches configured, including the default system-generated virtual switch vs0.

The following table describes the fields in each tab.

Table 37: Network Configuration Fields

Parameter	Description	Values
Networks Tab		
Subnet Name	Displays the name of the virtual network.	(name)
Virtual Switch	Displays the name of the virtual switch in the form vs#, for example vs0 for virtual switch 0 which is the default virtual switch.	(vs<number>)
VLAN ID	Displays the VLAN identification number for the network in the form vlan.#, for example vlan.27 for virtual LAN number 27.	(ID number)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2006

Parameter	Description	Values
Used IP Addresses	Displays the number of IP addresses in the subnet that are used, for example IP address of a VM or any other entity. This parameter is applicable only when you have configured a managed network or subnet.	(number of IP addresses)
Free IPs in Subnets	Displays the number of free or unused IP addresses in the subnet. This parameter is applicable only when you have configured a managed network or subnet.	(number of IP addresses)
Free IPs in Pool	Displays the number of free or unused IP addresses in the configured pool. This parameter is applicable only when you have configured a managed network or subnet.	(number of IP addresses)
Actions	Action link for editing or deleting a network configuration.	(Edit/Delete)
Internal Interfaces Tab		
Descriptive Name	Displays a name for the LAN.	(LAN name)
Subnet (Gateway IP / Prefix Length)	Displays the subnet that the internal interface belongs to in the form `<IP Address>`/<number (prefix)>	(IP Address/prefix number)
Features	Displays the features available on the internal interfaces.	
Interface	Displays the interface designation such as eth0 or eth1.	(interface name)
Virtual Switch		
Name	Displays the name of the switch in the form vs#	(vs<number>)
Bridge	Displays the name of the bridge associated with the virtual switch in the form br#, for example br0 for the default bridge.	(br<number>)
MTU (bytes)	Displays the MTU set for the virtual switch in bytes. The default MTU is 1500.	(number)
Bond Type	Displays the uplink bond type associated with the virtual switch. See the *Bond Type* table. For example, Active-Backup	(<bond_type>)

LAG and LACP on the ToR Switch

For information on LAG and LACP on the ToR Switch, see Enabling LACP and LAG (AHV Only) on page 174.

Creating or Updating a Virtual Switch

This section provides the procedure to create or update a virtual switch.

About this task

For more information about virtual switch, see Layer 2 Network Management in the *AHV Administration Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2007

You can create or update a virtual switch using the **Create Virtual Switch** or **Update Virtual Switch** dialog box. The **Create Virtual Switch** and **Update Virtual Switch** dialog boxes have identical parameters and settings.

Perform the following steps to create or update a virtual switch.

Procedure

1. Log in to the Prism Element web console.
2. Perform one of the following:
   - » Go to **VM** > **Network Config**.
   - » Go to **Settings** > **Network** > **Network Configuration**.
3. On the **Network Configuration** page, click the **Virtual Switch** tab.
4. To create a virtual switch, click **+ Create VS** and perform the following steps in the **Create Virtual Switch** dialog box.

   To update a virtual switch, click the edit option (pencil icon) and perform the following steps in the **Edit Virtual Switch** dialog box.
5. Provide the necessary information in the **General** tab.

Field	Description
Virtual Switch Name	Enter a name for the virtual switch.
Description	Provide a description for the virtual switch that helps identify the virtual switch.
Physical NIC MTU (bytes)	MTU must be a value in the range 1500 ~ 9000 inclusive.
Select Configuration Method	Select the **Standard (Recommended)** method to implement the VS configuration: This method ensures no disruptions occur to the workloads by putting the hosts in maintenance mode and migrating the VMs out of the host before applying the configuration. **Note:** When the **Standard** method is selected, only the hosts that have been updated with virtual switch configurations are rebooted. This process requires a longer duration of time to complete. The time required depends on the number and configuration of VMs. In this method, the VS configuration is deployed in the rolling update process.

6. Click **Next** to go to the **Uplink Configuration** tab.

   On the **Uplink Configuration** tab, provide the following details:

Field	Description and Value
Bond Type	Select an appropriate bond type. See the *Bond Types* table for details about the bond types.
Select Hosts	Select the hosts that can host VMs.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2008

Field	Description and Value
Select Uplink Ports	Select the criteria that need to be satisfied for the uplink ports. The available uplink ports that satisfy the criteria are displayed in the (Host port) table at the bottom of this tab.
Show	(Port Type) Select one of the following: **Connected and Unconnected Uplink Ports**: Select this if you want to use ports that are not currently connected but may be connected later. **Only Connected Uplink Ports**: Select this option if you want to use only the connected ports. You must also select in the **On Switches (with LLDP)** drop down box the switches with LLDP.
Uplink Port Speeds	Select a speed to display the ports that have the selected speed. You can select speeds such as **1G**, **10G** or both (**All Speeds**). The speeds displayed depend on the NIC type that is installed on the host. Based on your selection the columns in the (Host Port) table change dynamically to display the ports with the speeds you selected.
(Host Port) table	Based on the Selections you made in this Select Uplink Ports section, a table displays the hosts that have the uplink ports that satisfy the selected criteria. Select the ports you need for this configuration from the list. Click the down arrow on the right side of the table to display the ports listed for each host. Click the check box of a port to select the port. When the check box is already checked, click check box to clear the selection. Clearing the selection removes the uplink port (NIC) from the virtual switch. **Note:** A port listing is greyed out if it is unavailable because it is already associated with another virtual switch. Click **Select All** to select all the ports available and listed. Click **Clear All** to unselect all the ports available and listed.

Table 38: Bond Types

Bond Type	Use Case	Maximum VM NIC Throughput	Maximum Host Throughput
Active-Backup	Recommended. Default configuration, which transmits all traffic over a single active adapter.	10 Gb	10 Gb
Active-Active with MAC pinning Also known as balance-slb	Works with caveats for multicast traffic. Increases host bandwidth utilization beyond a single 10 Gb adapter. Places each VM NIC on a single adapter at a time. Do not use this bond type with link aggregation protocols such as LACP.	10 Gb	20 Gb

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2009

Bond Type	Use Case	Maximum VM NIC Throughput	Maximum Host Throughput
Active-Active Also known as LACP with balance-tcp	LACP and link aggregation required. Increases host and VM bandwidth utilization beyond a single 10 Gb adapter by balancing VM NIC TCP and UDP sessions among adapters. Also used when network switches require LACP negotiation. The default LACP settings are: • Speed—Fast (1s) • Mode—Active fallback-active-backup • Priority—Default. This is not configurable.	20 Gb	20 Gb
No Uplink Bond	No uplink or a single uplink on each host. Virtual switch configured with the No uplink bond uplink bond type has 0 or 1 uplinks. When you configure a virtual switch with any other bond type, you must select at least two uplink ports on every node.	-	-

Note: The Maximum VM NIC Throughput and Maximum Host Throughput values are not restricted to the value provided in this table. The values in the table are indicated for an assumption of 2 x 10 Gb adapters with simplex speed.

For more information about uplink configuration, see Virtual Switch Workflow in the *AHV Administration Guide*.

7. Click **Create** to create the virtual switch or **Save** to update an existing virtual switch.

   Click **Cancel** to exit without creating or updating the virtual switch.

   Click **Back** to go back to the **General** tab.

Deleting a Virtual Switch

About this task

For more information about virtual switch, see Layer 2 Network Management in the *AHV Administration Guide*.

You can delete a VS on the **Virtual Switch** tab in the **Network Configuration** dialog box. When you delete a virtual switch, the bridge created by the virtual switch is also removed completely.

You can also disable all the virtual switches. However, you can do so only using CLI. Prism does not support disabling virtual switches. Use the net.disable_virtual_switch to disable the virtual switch functionality and remove all the virtual switches including the default virtual switch vs0. However, the bridge and uplink bond or interface configurations are not affected by this command. This action cannot be undone either.

To delete a virtual switch, do the following:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2010

Procedure

1. Click the **Delete** icon (trash icon) next to the virtual switch listed in the list on the **Virtual Switch** tab in the **Network Configuration** dialog box.

   The **Delete Virtual Switch** dialog box opens. Deletion cannot be undone or reversed. Therefore, you must confirm the deletion in this dialog box.

2. Click **Delete** to confirm deletion.

   Click **Cancel** to close the **Delete Virtual Switch** dialog box without deleting the virtual switch.

What to do next

Check if the virtual switch is deleted from the list on the **Virtual Switch** tab.

Migrating Bridges after Upgrade

Before you begin

Ensure the following prerequisites are satisfied before migrating or converting a bridge to a VS.

- The bridge intended to be converted to a Virtual Switch must have consistent configurations across all the nodes in the cluster in terms of bond-type, MTU and LACP parameters.
- Within a virtual switch, the VLAN IDs must be exclusive across networks. An exception to this configuration is when a network is IPAM enabled and the other network is not IPAM enabled. In a scenario where an existing bridge has duplicate VLAN IDs, only one of these networks (per IPAM state) will get migrated under the virtual switch. The additional networks remains as is with no visible impact to the functionality.

  Note:

  Networks with same the VLAN IDs can exist across different virtual switches.

About this task

You can migrate or convert the bridges other than br0 in the cluster to virtual switches after you upgraded the minimum or compatible version of AOS and AHV.

Note: You cannot migrate any bridges using Prism Central. Use Prism Element web console or aCLI to migrate or convert the bridges.

You can convert only one bridge at a time. You need to repeat the workflow for every bridge that you want to convert to a virtual switch.

Note: The migration process creates new virtual switches which host the bridges that are being migrated or converted.

To migrate the bridges after upgrade, perform the following.

Procedure

1. Log on to the Prism Element web console.
2. Click the **Convert Bridges to VS** link at the bottom left of the **Network** dashboard.

   If there are any bridges that you can migrate, the system displays the **Convert Bridges to VS** dialog box.

   If there are no bridges that you can migrate, the system displays the There are no OVS bridges that can be converted to virtual switches message.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2011

3. On the **Convert Bridges to VS** dialog box, select the bridge you want to migrate in the **Select a Bridge** drop down field.

   The **Select a Bridge** drop down field provides a list of bridges you can migrate. Select the bridge you want to migrate and complete the following steps.

   a. Provide a **Name** and a **Description** for the virtual switch that you want to create by migrating the bridge.

      For example, if you select `br1` in **Select a Bridge**, you can provide `vs1` as the name for the virtual switch.

4. Click **Convert**.

   The converted virtual switch is available in the **Network** page in Prism Element web console and the **Virtual Switch** tab on the **Network Configuration** page in Prism Central.

Re-Configuring Bonds Across Hosts Manually

If you are upgrading AOS to 5.20, 6.0, or later versions, you need to migrate the existing bridges to virtual switches. If there are inconsistent bond configurations across hosts before the migration of the bridges, then after the migration of bridges, the virtual switches might not be properly deployed. To resolve such issues, you must manually configure the bonds to make them consistent.

Before you begin

Ensure that you meet the following prerequisites before you reconfigure the bonds:

- Place the affected AHV host where you want to reconfigure the bonds into maintenance mode.

  Log on to any CVM using SSH, and run the following command:

  ```
  nutanix@cvm$ acli host.enter_maintenance_mode hypervisor-IP-address [wait="{ true |
   false }" ] [non_migratable_vm_action="{ acpi_shutdown | block }" ]
  ```

  Replace `hypervisor-IP-address` with either the IP address or host name of the AHV host you want to shut down.

  The following are optional parameters for running the `acli host.enter_maintenance_mode` command:

  - **wait**: Set the **wait** parameter to **true** to wait for the host evacuation attempt to finish.
  - **non_migratable_vm_action**: By default the **non_migratable_vm_action** parameter is set to **block**, which means the non-migratable VMs are shut down when you put a node into maintenance mode. For more information on non-migratable VMs, see Non-Migratable VMs.

    Note: VMs with host affinity policies are also not migrated to other hosts in the cluster, if any of the following condition is met:

    - The hosts that are configured as part of VM-Host affinity policy are not available.
    - The hosts that are part of VM-Host affinity policy does not have the sufficient resources to run the VM.

    If you want to automatically shut down such VMs, set the **non_migratable_vm_action** parameter to **acpi_shutdown**.

  For more information, see Putting a Node into Maintenance Mode using CLI.

- Check the **Cluster Resiliency / Fault Tolerance Status** widget in the Prism Element web console dashboard to ensure that the cluster is healthy and resilient to any brief interruptions to network connectivity during uplink changes. For more information, see Home Dashboard on page 63.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2012

About this task

Important:

- Perform the bond changes only on one host at a time. Ensure that you get the completed host out of maintenance mode before you proceed to work on any other affected hosts.
- Use this procedure only when you need to modify the inconsistent bonds in a migrated bridge across hosts in a cluster, that is preventing Acropolis (AOS) from deploying the virtual switch for the migrated bridge.

  Do not use **nmcli** commands to make the bridge level changes. Use the **manage_ovs** commands, instead.

  The manage_ovs command allows you to update the cluster configuration. The changes are applied and retained across host restarts. The nmcli command allows you to update the live running host configuration but does not update the AOS cluster configuration and the changes are lost at host restart. This behavior of nmcli introduces connectivity issues during maintenance, such as upgrades or hardware replacements.

  nmcli is typically used in cases where a host might be isolated on the network and requires a workaround to gain connectivity before the cluster configuration can actually be updated using manage_ovs.

Note: Disable the virtual switch before you attempt to change the bonds or bridge.

If you face an issue where the virtual switch is automatically re-created after it is disabled (with AOS versions 5.20.0 or 5.20.1), follow steps 1 and 2 below to disable such an automatically re-created virtual switch again before migrating the bridges. For more information, see KB-3263.

Be cautious when using the disable_virtual_switch command because it deletes all the configurations from the IDF, not only for the default virtual switch vs0, but also any virtual switches that you may have created (such as vs1 or vs2). Therefore, before you use the disable_virtual_switch command, ensure that you check a list of existing virtual switches, that you can get using the acli net.get_virtual_switch command.

Complete this procedure on each host Controller VM that is sharing the bridge that needs to be migrated to a virtual switch.

Procedure

1. To list the virtual switch, use the following command.

   ```
   nutanix@cvm$ acli net.list_virtual_switch
   ```

2. Disable all the virtual switches.

   ```
   nutanix@cvm$ acli net.disable_virtual_switch
   ```

   All the virtual switches in the cluster are disabled.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2013

3. Change the bond type to align with the same bond type on all the hosts for the specified virtual switch

```
nutanix@cvm$ manage_ovs --bridge_name bridge-name --bond_name bond_name --
bond_mode bond-type update_uplinks
```

Where:

- *bridge-name*: Provide the name of the bridge, such as **br0** for the virtual switch on which you want to set the uplink bond mode.
- *bond-name*: Provide the name of the uplink port such as **br0-up** for which you want to set the bond mode.
- *bond-type*: Provide the bond mode that you require to be used uniformly across the hosts on the named bridge.

Use the `manage_ovs --help` command for help on this command.

> **Note:** To disable LACP, change the bond type from LACP Active-Active (balance-tcp) to Active-Backup/Active-Active with MAC pinning (balance-slb) by setting the *bond_mode* using this command as active-backup or balance-slb.
>
> Ensure that you turn off LACP on the connected ToR switch port as well. To avoid blocking of the bond uplinks during the bond type change on the host, ensure that you follow the ToR switch best practices to enable LACP fallback or passive mode.
>
> To enable LACP, configure *bond-type* as balance-tcp (Active-Active) with additional variables `--lacp_mode fast` and `--lacp_fallback true`.

4. Exit the host from maintenance mode, using the following command:

```
nutanix@cvm$ acli host.exit_maintenance_mode hypervisor-IP-address
```

Replace *hypervisor-IP-address* with the IP address of the AHV host.

This command migrates (live migration) all the VMs that were previously running on the host back to the host. For more information, see Exiting a Node from the Maintenance Mode Using CLI.

5. Repeat the above steps for each host for which you intend to reconfigure bonds.
6. (If migrating to AOS version earlier than 5.20.2) Check if the issue in the note and disable the virtual switch.

What to do next

After making the bonds consistent across all the hosts configured in the bridge, migrate the bridge or enable the virtual switch. For more information, see:

- Re-Configuring Bonds Across Hosts Manually on page 162.
- Network Configuration in the *Prism Central Infrastructure Guide*.

To check whether LACP is enabled or disabled, use the following command.

```
nutanix@cvm$ manage_ovs show_uplinks
```

MAC Address Prefix

You can avoid duplicate IP addresses in a single-cluster or multi-cluster environment by implementing one of two possible configurations:

- Nutanix recommends that you assign a set of unique VLANs for guest VMs on each AHV cluster. Ensure these VLANs do not overlap with the VLANs on other AHV clusters. Assigning unique VLAN ranges for each cluster reduces the risk of MAC address conflicts. Such an assignment also ensures compliance with the general best practice of maintaining small Layer 2 broadcast domains with limited numbers of endpoints.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2014

- If multiple AHV clusters need to share the same VLAN, or when guest VM MAC addresses need be globally unique among multiple AHV clusters, configure a predefined MAC address prefix for each AHV cluster.

Nutanix does not guarantee unique MAC address assignment by default between Nutanix clusters with VLAN networks.

Sample Design Scenario with Multiple Sites and Clusters

Using locally administered MAC addresses, you can ensure unique MAC addresses for VMs in an environment made up of multiple sites and clusters.

A MAC address is usually a 6-octet hexadecimal address block. The notation for a MAC address is `XX:XX:XX:XX:XX:XX`. In this 6-octet address, the first 3 octets are the organizationally unique identifier (OUI) octets or the MAC address prefix OUI. The second bit of the 1st octet (the first hexadecimal number `XX`) is set to 1 to make the MAC address a locally administered MAC address. The next 3 octets are NIC specific octets, `XX:XX:XX`, represents the useable hexadecimal range for endpoints within each AHV cluster.

> **Note:** Nutanix AHV clusters use the MAC address prefix OUI `50:6B:8D` by default.
>
> By default, Acropolis leader generates MAC address for a VM on AHV. The first 24 bits of the MAC address (OUI) is set to `50-6b-8d` (0101 0000 0110 1101 1000 1101) and are reserved by Nutanix, the 25th bit is set to 1 (reserved by Acropolis leader), the 26th bit to 48th bits are auto generated random numbers.

Consider this sample design of a deployment with three sites and five clusters in each site. Define a unique MAC address prefix for Site1-Cluster1 such as 02:01:01, where:

- 02—Defines the MAC address as a unicast address that is locally administered. This value could be a hexadecimal number defined by X2, X3, X6, X7, XA, XB, or XE series, where X is any valid hexadecimal value such that the second binary bit (binary bits being counted from right to left, right most is the first bit) of the binary equivalent of this hexadecimal number `XX` is set to 1 to make the MAC address a locally administered MAC address.
- 01—Used to identify, for example, the site number. This value could be any valid hexadecimal value.
- 01—Used to identify, for example, the AHV cluster within the site. This value could be any valid hexadecimal value

The NIC specific octets, `XX:XX:XX`, are auto-assigned to the VM NICs or the endpoints within each AHV cluster. Thus, for Site1, the clusters would have the following prefixes:

- Site1-Cluster1: 02:01:01
- Site1-Cluster2: 02:01:02
- Site1-Cluster3: 02:01:03
- Site1-Cluster4: 02:01:04
- Site1-Cluster5: 02:01:05

  ... and so on for the other clusters at Site1.

Similarly for Site2, if you define, for example 02:02:01 as the MAC address prefix for the first cluster - Cluster1, you get the series of predefined MAC address prefixes for the clusters and VMs or endpoints in Site2, Cluster1.

- Site2-Cluster1-VM1: 02:02:01:00:00:01
- Site2-Cluster1-VM2: 02:02:01:00:00:02
- ...
- Site2-Cluster1-VM10: 02:02:01:00:00:0A

  ... and so on for the other clusters at Site2.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2015

Adding a MAC Address Prefix

Before you begin

Ensure that you meet the following requirements before you add a MAC address prefix:

- Guest VMs in the cluster do not have any NICs that have MAC addresses with the default prefix.
- Check the #unique_208/unique_208_Connect_42_section_ktr_3mw_1dc.

About this task

Use aCLI to configure the MAC address prefix for a cluster.

Procedure

1. Log on to a Controller VM in your cluster with SSH.
2. Access Acropolis CLI using the `acli` command.

   ```
   nutanix@cvm$ acli
   ```

   The prompt changes to `<acropolis>`.
3. Add the MAC address prefix for the cluster using the following command.

   ```
   <acropolis> net.set_mac_prefix XX:XX:XX
   ```

   > **Note:** Ensure that the VMs in the cluster do not have any NICs that have MAC addresses with the default prefix.

   > **Warning:**
   >
   > Ensure that you do not set the MAC address prefix to `52:6b:8d` as this might lead to a conflict due to one of the guest VMs acquiring `52:6b:8d:00:00:00` IP, which AHV uses internally for packet probing purposes.

   Replace *XX:XX:XX* by the MAC address prefix for the cluster.

   Using the example discussed in MAC Address Prefix on page 164, the following sample command adds the `02:01:01` as the MAC address prefix for Site1-Cluster1

   ```
   <acropolis> net.set_mac_prefix 02:01:01
   ```

What to do next

Verify if the MAC address prefix is configured using the `net.get_mac_prefix` command.

The output displays the hexadecimal prefix that you configured.

Using the configuration example, the output would show `"02:01:01"` as follows:

```
<acropolis> net.get_mac_prefix
"02:01:01"
<acropolis>
```

Repeat this procedure to add MAC address prefixes to other clusters that share the same VLAN (defining the common broadcast domain) that you want to avoid duplicate MAC addresses in.

Removing the MAC Address Prefix

You can remove the MAC address prefix. The cluster then uses the default MAC prefix, `"50:6b:8d"`.

Before you begin

Remove the MAC addresses with the configured prefix from the VM NICs in the cluster.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2016

About this task

Use aCLI commands to remove the MAC address prefix for a cluster.

Procedure

1. Log on to a Controller VM in your cluster with SSH.
2. Access Acropolis CLI using the `acli` command.

   ```
   nutanix@cvm$ acli
   ```

   The prompt changes to `<acropolis>`.
3. Remove the MAC address prefix for the cluster using the following command.

   ```
   <acropolis> net.clear_mac_prefix
   ```

   > **Note:** Ensure that the VMs in the cluster do not have any NICs that have MAC addresses with the configured prefix.

What to do next

Verify that the MAC address prefix is removed. When you use the `net.get_mac_prefix` command, the output displays the default MAC address prefix, `"50:6b:8d"`.

```
<acropolis> net.get_mac_prefix
"50:6b:8d"
<acropolis>
```

Network Configuration for VM Interfaces

In clusters with Nutanix virtualization management (such as those running AHV), you can configure network connections through the web console. Each VM network interface is bound to a virtual network, and each virtual network is bound to a single VLAN. Additionally, on AHV, Hyper-V, and ESXi, you can secure intra-cluster communications by segmenting the virtual network on the cluster.

About this task

To configure a virtual network for VM interfaces, do one of the following:

Procedure

- To configure virtual networks for user VM interfaces, see Configuring a Virtual Network for Guest VM Interfaces on page 167.
- To secure intra-cluster communications by configuring network segmentation, see Securing Traffic Through Network Segmentation in the *Nutanix Security Guide*.

Configuring a Virtual Network for Guest VM Interfaces

Follow this procedure to configure a virtual network for guest VMs. You can associate the network with a VLAN and configure IP address management for interfaces on the network.

About this task

> **Note:** Do not add any other device (including guest VMs) to the VLAN to which the CVM and hypervisor host are assigned. Isolate guest VMs on one or more separate VLANs.

Perform the following steps to configure a virtual network for guest VM interfaces.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2017

Procedure

1. Log in to the Prism Element web console.
2. Perform one of the following:
   - » Go to **VM** > **Network Config**.
   - » Go to **Settings** > **Network** > **Network Configuration**.

     Note: This option only appears in clusters that support this feature.

   The **Network Configuration** window appears.
3. Click the **Subnets** tab and then click the **+ Create Subnet** button.
   The **Create Subnet** dialog box appears. Do the following in the indicated fields:
   a. **Subnet Name**: Enter a name for the subnet or network.
      Nutanix recommends that you enter a unique name for each VLAN that you create. Unique names help in easy identification of the VLANs. Using duplicate names for the VLANs is not prohibited. If you use

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2018

duplicate names for the VLANs, the list of VLANs displays several VLANs with the same name but with different UUIDs.

b. **Virtual Switch**: Select the virtual switch that you want to associate with the subnet.

c. **VLAN ID**: Enter the number of the VLAN.

Enter just the number in this field, for example 1 or 27. Enter 0 for the native VLAN. The value appears as vlan.1 or vlan.27 in displays.

d. **Enable IP Address Management**: Select the checkbox to have the cluster control IP addressing in the network.

Selecting this checkbox displays more fields. If you do not select the checkbox, Files does not attempt network management. In this case, it is assumed management for this virtual LAN is handled outside the cluster.

> **Note:** If you do not enable this option while creating a network, you cannot enable or disable IP address management (IPAM).
>
> IP Address Management (IPAM) is a feature of AHV that allows it to assign IP addresses automatically to VMs by using DHCP. For more information, see IP Address Management in the *AHV Administration Guide*.

e. **Network IP Address/Prefix Length**: Enter the IP address of the gateway for the network and prefix with the network prefix (CIDR notation, for example, 10.1.1.0/24).

f. **Gateway IP Address**: Enter the VLAN default gateway IP address.

g. **Configure Domain Settings**: Select this checkbox to display fields for defining a domain.

Selecting this checkbox displays fields to specify DNS servers and domains. Clearing the checkbox hides those fields.

h. **Domain Name Servers (comma separated)**: Enter a comma-delimited list of DNS servers.

i. **Domain Search (comma separated)**: Enter a comma-delimited list of domains.

j. **Domain Name**: Enter the VLAN domain name.

k. **TFTP Server Name**: Enter the host name or IP address of the TFTP server from which virtual machines can download a boot file. Required in a Pre-boot eXecution Environment (PXE).

l. **Boot File Name**: Name of the boot file to download from the TFTP server.

4. To define a range of addresses for automatic assignment to virtual NICs, click the **Create Pool** button (under **IP Address Pools**) and enter the following in the **Add IP Pool** dialog box:

If you do not assign a pool, assign IP addresses to VMs manually.

a. Enter the starting IP address of the range in the **Start Address** field.

b. Enter the ending IP address of the range in the **End Address** field.

c. Click the **Submit** button to close the window and return to the **Create Subnet** dialog box.

5. To configure a DHCP server, select the **Override DHCP server** checkbox and enter an IP address in the **DHCP Server IP Address** field.

This address (reserved IP address for the Acropolis DHCP server) is visible only to VMs on this network and responds only to DHCP requests. If you do not check the box, the **DHCP Server IP Address** field does not display, and the DHCP server IP address generates automatically. The automatically generated address is `network_IP_address_subnet.254`, or if the default gateway is using that address, `network_IP_address_subnet.253`.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2019

6. When all the information is correct, click the **Save** button to configure the network connection, close the **Create Subnet** dialog box, and return to the **Network Configuration** window.

> **Note:**
>
> - You can also specify network mapping to control network configuration for the VMs when they start on the remote site. For more information about configuring networking mapping on remote site, see Configuring a Remote Site (Physical Cluster) in the *Data Protection and Recovery with Prism Element Guide*.
> - Verify (or update as needed) that the physical switch configuration allows traffic for the same VLAN's that are configured for the virtual networks.

Verifying IPAM Address Pool for Sufficient IP Addresses

This procedure verifies the IPAM managed IP address pool for sufficient IP addresses and checks when the IP pool is close to running out of IP addresses.

About this task

To verify the IPAM managed IP address pool for sufficient IP addresses, do the following:

Procedure

1. Click the gear icon in the main menu and then select **Network Configuration** in the **Setting** page.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2020

2. Select the **Networks** tab (default) to view networks for the VMs in the **Network Configuration** dialog box. It consists of the following:

   a. **Network Name**: Displays the networks configured on the VM.

   b. **Virtual Switch**: Displays the virtual Switch configured on the VM.

   c. **VLAN ID**: Displays the VLAN ID configured on the VM.

   d. **Used IP Addresses**: Displays the number of IP addresses in use by the IPAM enabled network. Click on the value displayed to view which VM is using which IP addresses from the IPAM enabled network.

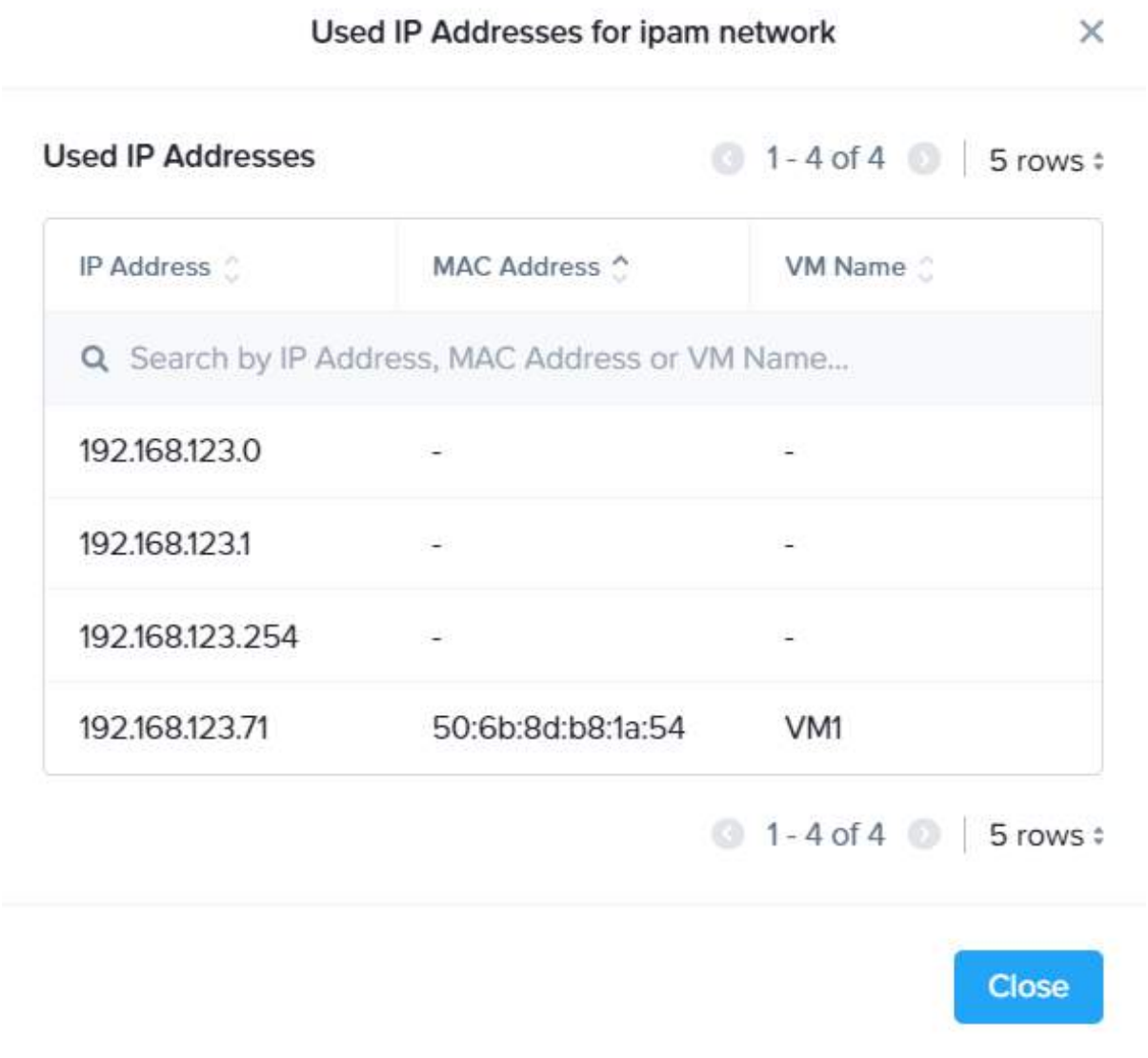


Figure 30: Used IP Address for IPAM Network

   e. **Free IPs in Subnets**: Displays the number of IP addresses configured in the subnet.

   f. **Free IPs in Pool**: Displays the number of free IPs available in the IP Pool configured for the subnet. The value in this field dynamically changes every time the network dynamically assigns a new IP to a VM.

   g. **Actions**: You can select either the **Edit** or **Delete** actions to update the Network configuration.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2021

Modifying Network Connections

Follow this procedure to modify network connections defined through the Nutanix virtualization management.

About this task

To modify or delete a network configuration, do the following:

Procedure

1. Log in to the Prism Element web console.
2. Perform one of the following:
   - » Go to **VM** > **Network Config**.
   - » Go to **Settings** > **Network** > **Network Configuration**.
3. To modify a network configuration, in the **Subnet** tab, click the **Edit** option associated with the subnet.

   The **Update Subnet** dialog box appears, which contains the same fields as the **Create Subnet** dialog box. For more information, see Configuring a Virtual Network for Guest VM Interfaces on page 167. Do the following:

   > **Note:** Changing the VLAN ID of a network in use is not allowed; only the name can be changed.

   a. Update the field values as desired.

   b. When the configuration is correct, click the **Save** button to close the page, update the network configuration, and return to the **Network Configuration** page.
4. To delete a network configuration, select the target line and click the X icon (on the right).

   A window prompt appears to verify the action; click the **OK** button. The network configuration is removed from the list.

Network Segmentation

You can segment the network on a Nutanix cluster by using Prism Element.

For more information, see Securing Traffic Through Network Segmentation in the *Security Guide*.

Configuring Network Switch Information

About this task

To track and record networking statistics for a cluster, the cluster requires information about the first-hop network switches and the switch ports being used. Switch port discovery is supported with switches that are RFC 2674 compliant. Switch port discovery involves obtaining statistics from the Q-BRIDGE-MIB on the switch and then identifying the MAC address that corresponds to the host. Such discovery is currently best-effort, so it is possible that, at times, an interface might not be discovered.

Before you begin

Before you configure network switch information in the Prism Element web console, configure the corresponding SNMP settings on the first-hop network switch.

About this task

To configure one or more network switches for statistics collection, do the following:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2022

Procedure

1. Log on to the Prism Element web console.
2. Click the gear icon in the main menu and then select **Network Switch** in the **Settings** page.

   > **Note:** Network switch configuration is supported only for AHV clusters.

   The **Network Switch Configuration** dialog box appears.
3. Click the **Switch Configuration** tab and then click the **Add Switch Configuration** button.
4. Do the following in the indicated fields:
   a. **Switch Management IP Address**: Enter the Management IP address of the switch or the fully qualified switch name.
   b. **Host IP Addresses or Host Name (separated by commas)**: Enter the IP address or fully qualified host name of each host in the cluster that uses this switch to route traffic.

      When there are multiple hosts, enter the addresses in a comma separated list. Failing to add the host list might result in issues with switch port discovery.
   c. **SNMP Profile**: Select the SNMP profile to apply (or **None**) from the drop-down list.

      Any SNMP profiles you have created appear in the list.

      > **Note:** Selecting a profile populates the remaining fields automatically with the profile values. If you have not created a profile (or select **None** from the list), you must enter the values in the remaining fields manually.

   d. **SNMP Version**: Select the SNMP version to use from the drop-down list.

      The options are **SNMPv2c** and **SNMPv3**.
   e. **SNMP Security Level** (SNMPv3 only): Select the security level to enforce from the drop-down list.

      The options are **No Authorization No Privacy**, **Authorization But No Privacy**, and **Authorization and Privacy**. This field appears only when SNMPv3 is selected as the version.
   f. **SNMP Community Name**: Enter the SNMP community name to use.
   g. **SNMP Username**: Enter the SNMP user name.
   h. **SNMP Authentication Type**: Select the authentication protocol to use from the drop-down list.

      The options are **None** and **SHA**.

      > **Note:** This field and the following three fields are set to **None** or left blank (and read only) when the version is SNMPv2c or the security level is set to no authorization.

   i. **SNMP Authentication Pass Phrase**: Enter the appropriate authentication pass phrase.
   j. **SNMP Privacy Type**: Select the privacy protocol to use from the drop-down list.

      The options are **None**, **AES**, and **DES**.
   k. **SNMP Privacy Pass Phrase**: Enter the appropriate privacy pass phrase.
   l. When all the fields are correct, click the **Save** button.

      This saves the profile and displays the new entry in the Switch Configuration tab.

      > **Note:** As a security protection, the **SNMP Authentication Pass Phrase** and **SNMP Privacy Pass Phrase** fields appear blank after saving (but the entered phrases are saved).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2023

Enabling LACP and LAG (AHV Only)

This section describes the procedure to enable LAG and LACP in AHV nodes and the Top-of-Rack (ToR) switch or any switch that is directly connected to the Nutanix node.

Procedure

To enable LACP and LAG, perform the following steps:

1. Login to the Prism Element web console and go to **Settings** > **Network Configuration** > **Virtual Switch**.

   You can also login to Prism Central, select the **Infrastructure** application from Application Switcher Function, and go to **Network & Security** > **Subnets** > **Network Configuration** > **Virtual Switch** from the navigation bar.

   The system displays the **Virtual Switch** tab.

2. Click the Edit icon ( ) for the target virtual switch on which you want to configure LACP and LAG.

   The system displays the **Edit Virtual Switch** window.

3. In the **General** tab, choose **Standard (Recommended)** option in the **Select Configuration Method** field, and click **Next**.

   > **Important:** When you select the **Standard** method, only the hosts that have been updated are restarted.
   >
   > The **Standard** configuration method puts each updated node in maintenance mode before applying the updated settings. After applying the updated settings, the node exits from maintenance mode. For more information, see Virtual Switch Workflow.

4. In the **Uplink** Configuration tab, select `Active-Active` in the **Bond Type** field, and click **Save**.

   > **Note:** The `Active-Active` bond type configures all AHV hosts with the fast setting for LACP speed, causing the AHV host to request LACP control packets at the rate of one per second from the physical switch. In addition, the `Active-Active` bond type configuration sets LACP fallback to `Active-Backup` on all AHV hosts. You cannot modify these default settings after you have configured them in Prism, even by using the CLI.

   This completes the LAG and LACP configuration on the cluster. At this stage, cluster starts the Rolling Reboot operation for all the AHV hosts. Wait for the reboot operation to complete before you put the node and CVM in maintenance mode and change the switch ports.

   For more information about how to manually perform the rolling reboot operation for an AHV host, see Rebooting an AHV Node in a Nutanix Cluster.

Perform the following steps on each node, one at a time:

5. Put the node and the Controller VM into maintenance mode.

   > **Note:** Before you put a node in maintenance mode, see Verifying the Cluster Health and carry out the necessary checks.

   The Step 6 in Putting a Node into Maintenance Mode using Web Console section puts the Controller VM in maintenance mode.

6. Change the settings for the interface on the switch that is directly connected to the Nutanix node to match the LACP and LAG settings made in the Edit Virtual Switch window above.

   For more information about how to change the LACP settings of the switch that is directly connected to the node, refer to the vendor-specific documentation of the deployed switch.

   Nutanix recommends you perform the following configurations for LACP settings on the switch:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2024

Table 39: Nutanix Recommendations for LACP Settings

Nutanix Recommendations	Description
Enable LACP fallback	Nutanix recommends you enable LACP fallback to set up a workaround for the port, using which the port establishes a link before the switch receives the LACP Bridge Protocol Data Units (BPDUs). The LACP fallback helps avoid link failures if either AHV host or switch that is connected to the AHV node does not negotiate LACP. LACP fallback provides seamless discovery of new nodes in an active or passive capacity setup and reduces the impact on the node operation. When LACP fallback is enabled, you can have a minimal business impact as VMs and applications remain healthy in case of an LACP status mismatch between the AHV host and the ToR switch port. As LACP fallback ensures connectivity during initial deployment, so it is crucial when you do not have LACP in discoveryOS. **Caution:** When LACP fallback occurs, the port runs in fallback mode, and this might lead to an unbalanced utilization of ports and lack of redundancy in your site deployment. Based on your internal networking policies, you can decide whether LACP fallback is helpful for you, and enable or disable it.
Consider the LACP time options *(slow and fast)*	If the switch has a fast configuration, Nutanix recommends you set the LACP time to fast on AHV host. Nutanix recommends the LACP time to match on both; switch and AHV host, for L2 failure detection at the same time on the switch and AHV host. If the switch has a fast configuration, set the LACP time to fast on AHV host. When the LACP time setting matches on AHV host and switch, the detachment of a failed interface occurs at the same time, and both switch and the AHV host do not use the failed interface. When the LACP time is set to: • *fast* - Failure detection occurs faster within 3 seconds • *slow* - Failure detection occurs slowly and takes up to 90 seconds The matching LACP time helps to prevent the outage.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2025

7. Verify that LACP negotiation status is `Negotiated`.

   Perform the SSH to the CVM as a nutanix user, and run the following commands:

   ```
   nutanix@CVM$ ssh root@[AHV host IP] "ovs-appctl bond/show bond-name"
   ```

   ```
   nutanix@CVM$ ssh root@[AHV host IP] "ovs-appctl lacp/show bond-name”
   ```

   - Replace the following attributes in the above commands:
     - `bond-name` with the actual name of the uplink port such as br0-up in the above commands.
     - `[AHV host IP]` with the actual AHV host IP at your site.
   - Search for the string `negotiated` in the status lines.

8. Remove the node and Controller VM from maintenance mode. For more information, see Exiting a Node from the Maintenance Mode using Web Console.

   The Controller VM exits maintenance mode during the same process.

What to do next

Do the following after completing the procedure to enable LAG and LACP in all the AHV nodes the connected ToR switches:

- Verify that the status of all services on all the CVMs are Up. Run the following command and check if the status of the services is displayed as **Up** in the output:

  ```
  nutanix@cvm$ cluster status
  ```

- Log in to the Prism Element web console of the node and ensure that the **Cluster Resiliency / Fault Tolerance Status** widget displays **OK**.

Creating SNMP Profiles

About this task

If you need to configure multiple network switches, it may be useful to create one or more SNMP profiles that can be applied when configuring the switches. For information on configuring a network switch, see Configuring Network Switch Information on page 172.

To create an SNMP profile, do the following:

Procedure

1. Log on to the Prism Element web console.
2. Click the gear icon in the main menu and then select **Network Switch** in the **Settings** page.

   > **Note:** Network switch configuration is supported only for AHV clusters.

   The **Network Switch Configuration** dialog box appears.
3. Click the **SNMP Profile** tab and then click the **Add SNMP Profile** button.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2026

4. Do the following in the indicated fields:

   a. **Profile Name**: Enter a name for the profile.
      The name can be anything as it is for display purposes only.

   b. **SNMP Version**: Select the SNMP version to use from the pull-down list.
      The options are **SNMPv2c** and **SNMPv3**.

   c. **SNMP Security Level** (SNMPv3 only): Select the security level to enforce from the pull-down list.
      The options are **No Authorization No Privacy**, **Authorization But No Privacy**, and **Authorization and Privacy**. This field appears only when SNMPv3 is selected as the version.

   d. **SNMP Community Name**: Enter the SNMP community name to use.

   e. **SNMP Username**: Enter the SNMP user name.

   f. **SNMP Authentication Type**: Select the authentication protocol to use from the pull-down list.
      The options are **None** and **SHA**.

      > **Note:** This field and the following three fields are set to **None** or left blank (and read only) when the version is SNMPv2c or the security level is set to no authorization.

   g. **SNMP Authentication Pass Phrase**: Enter the appropriate authentication pass phrase.

   h. **SNMP Privacy Type**: Select the privacy protocol to use from the pull-down list.
      The options are **None**, **AES**, and **DES**.

   i. **SNMP Privacy Pass Phrase**: Enter the appropriate privacy pass phrase.

   j. When all the fields are correct, click the **Save** button.
      This saves the profile and displays the new entry in the SNMP Profile tab.

Modifying Switch Information

About this task

To modify the information about a network switch (or the SNMP profile used in the switch information), do the following:

Procedure

1. Click the gear icon in the main menu and then select **Network Switch** in the **Settings** page.

   > **Note:** Network switch configuration is supported only for AHV clusters.

   The **Network Switch Configuration** dialog box appears.

2. To modify a switch configuration (or SNMP profile), select the **Switch Configuration** (or **SNMP Profile**) tab, go to the target switch (or profile) entry in the table, and click the pencil icon.
   This displays the configuration fields. Edit the entries as desired and then click the **Save** button.

3. To delete a switch configuration (or SNMP profile), select the **Switch Configuration** (or **SNMP Profile**) tab, go to the target switch (or profile) entry in the table, and click the X icon.
   This deletes the entry and removes it from the table.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2027

Network Visualization

The network visualizer is a consolidated graphical representation of the network formed by the VMs and hosts in a Nutanix cluster and first-hop switches. You can use the visualizer to monitor the network and to obtain information that helps you troubleshoot network issues.

You can use the visualizer to view the following:

- Physical and logical network topology.
- Summary of the number and types of devices in the network.
- Network configuration of the devices in the topology and of components such as physical and virtual NICs.
- Real-time usage graphs of physical and virtual interfaces.

> **Caution:** You cannot use the visualizer to configure the network. The network visualizer is available only on AHV clusters.

Prerequisites

Before you use the network visualizer, do the following:

- Configure network switch information on the Nutanix cluster. For more information, see Configuring Network Switch Information on page 172.
- Enable LLDP or CDP on the first-hop switches. The visualizer uses LLDP or CDP to determine which switch port is connected to a given host interface. If LLDP or CDP is unavailable, SNMP data is used on a commercially reasonable effort. For information about configuring LLDP or CDP, see the switch manufacturer's documentation.
- (Optional) Configure SNMP v3 or SNMP v2c on the first-hop switches if you want the network visualizer to display the switch and switch interface statistics. The visualizer uses SNMP for discovery and to obtain real-time usage statistics from the switches. For information about configuring SNMP, see the switch manufacturer's documentation.

  > **Note:** This is not a mandatory requirement to use the network visualizer. This is a prerequisite only if you want the network visualizer to display the switch and switch interface statistics.

> **Note:** Network visualization depends on a functional internal DNS system to map switch hostnames and IP addresses based on the LLDP responses. Incorrect or partial DNS configuration displays inaccurate network details in the UI. To troubleshoot the network visualization issues, see *KB-4085* in the Nutanix Support portal.

Network Visualizer

The network visualizer displays interactive visual elements for the networked devices and for network components such as physical and logical interfaces. It also provides filtering and grouping capabilities that you can use to limit the display to a specific set of networked devices and connections.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2028

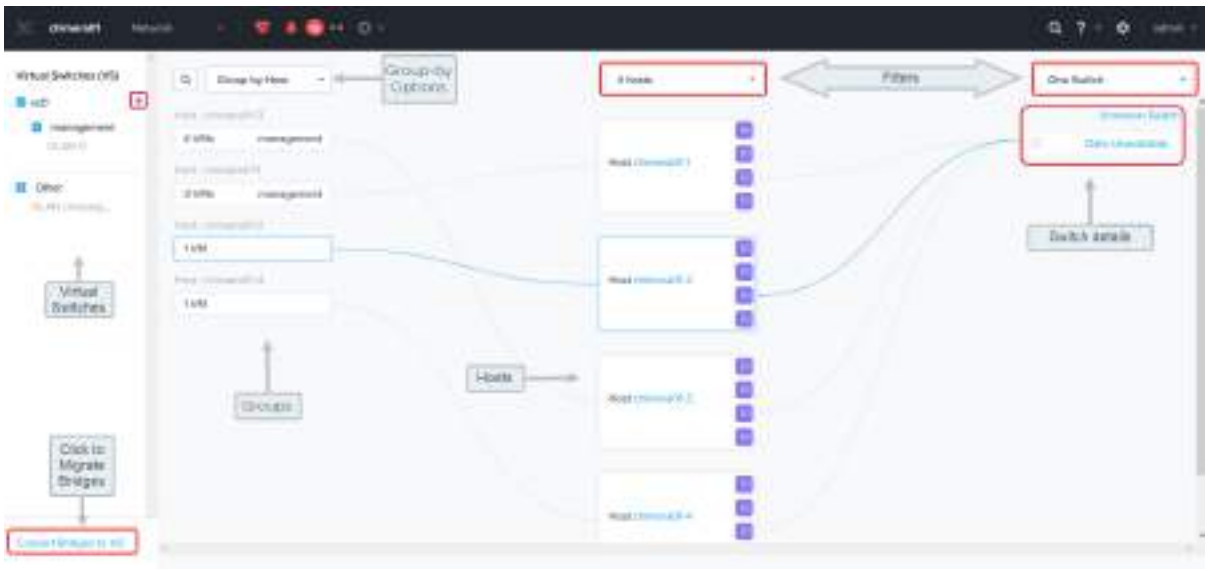


Figure 31: Network Visualizer

The network visualizer includes the virtual networks pane and the topology view.

Virtual Networks Pane

Lists the virtual switches (VSs) configured on the Nutanix cluster. Selecting a VS includes the VMs on that VS in the topology view. Conversely, clearing a check box excludes the VMs on that VS from the topology view. You can show up to five VSs at a time.

The check box titled Other corresponds to VMs that are not on any VS. At a minimum, this check box is associated with the Controller VMs in the cluster.

Topology View

Displays the network topology. The topology view shows the following entities:

Virtual Switch (VS)
: VSs are configured on the cluster. The visualizer displays a different color for each VS. It shows the VSs to which a VM or the VMs in a VM group belong. It also shows which VSs are configured on a first-hop switch.

VMs
: VMs on the VSs that are selected in the virtual networks pane. Filter and group-by options enable you to customize the topology view.

Hosts
: Hosts in the Nutanix cluster. The filter above the hosts enables you to specify which hosts you want to show in the topology view.

Switches
: First-hop switches and the VSs configured on each of them. The filter above the switches enables you to specify which switches you want to show in the topology view.

Viewing the Network Visualizer

About this task

To view the network visualizer, do the following:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2029

Procedure

1. Log on to the web console.
2. Click **Network** in the main menu.
   The system displays interactive visual elements for the networked devices and for network components such as physical and logical interfaces.

Customizing the Topology View

You can group VMs by a VM property or use a search filter to specify which network devices you want to show or exclude.

About this task

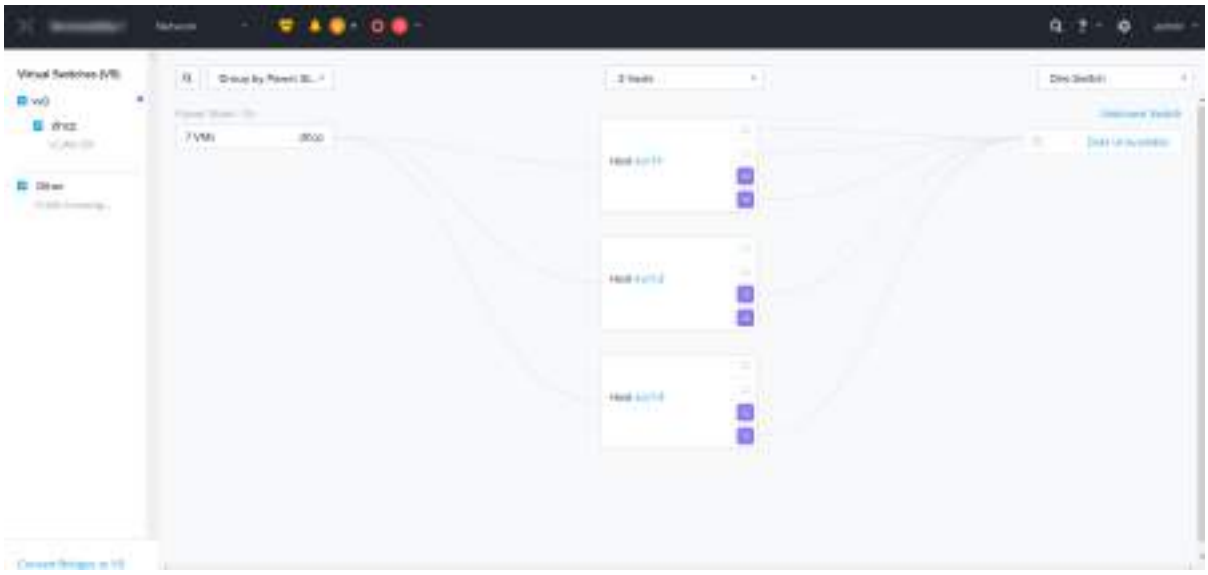


Figure 32: Network page

To customize the topology view, do the following:

Procedure

1. Log on to the Prism Element web console.
2. Click **Network** in the main menu.
3. Specify which virtual switches you want to show in the topology view:
   - In the **Virtual Switch (VS)** pane, select the checkboxes associated with the virtual switches and the networks in each virtual switch that you want to display in the topology view and clear those that you do not want to display.
   - Select or clear the **Other** checkbox if you want to include or exclude, respectively, the VMs that are not on any VLANs.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2030

4. Specify which VMs you want to display in the topology view:
   - Select a group-by option from the menu at the top of the VMs. The following group-by options are available:
     - **Power State**. Groups VMs by states such as On and Off. By default, the VMs are grouped by power state.
     - **Host**. Groups VMs by the host on which they are running.
     - **VM Type**. Groups VMs into guest VMs and Controller VMs.
   - Enter a string in the search filter field to filter VMs that match the search string.
   - If the group-by and filter operations result in a VM group, click the VM group to show the VMs in the group.

     When you click a VM group, the visualizer displays ten VMs at first. To load ten more VMs, click **Load More VMs**.

     To group the VMs again or to clear the filter, click **Back** beside the group-by menu.
5. Specify which Nutanix hosts you want to display in the topology view:
   a. Click the menu above the Nutanix hosts.
   b. Select the hosts that you want to show and clear those that you want to exclude.
6. Specify which switches you want to display in the topology view:
   a. Click the menu above the switches.
   b. Select the switches that you want to show and clear those that you want to exclude.

Viewing VM Information

In the visualizer, you can view the settings and real-time statistics of a virtual NIC.

About this task

To view VM information, do the following:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2031

Procedure

1. Use the group-by and filtering capabilities of the visualizer to display the VM you want, and then click the name of the VM.

   For information on how to group VMs or use a search filter, see Customizing the Topology View on page 180.

   The VM network information window appears.

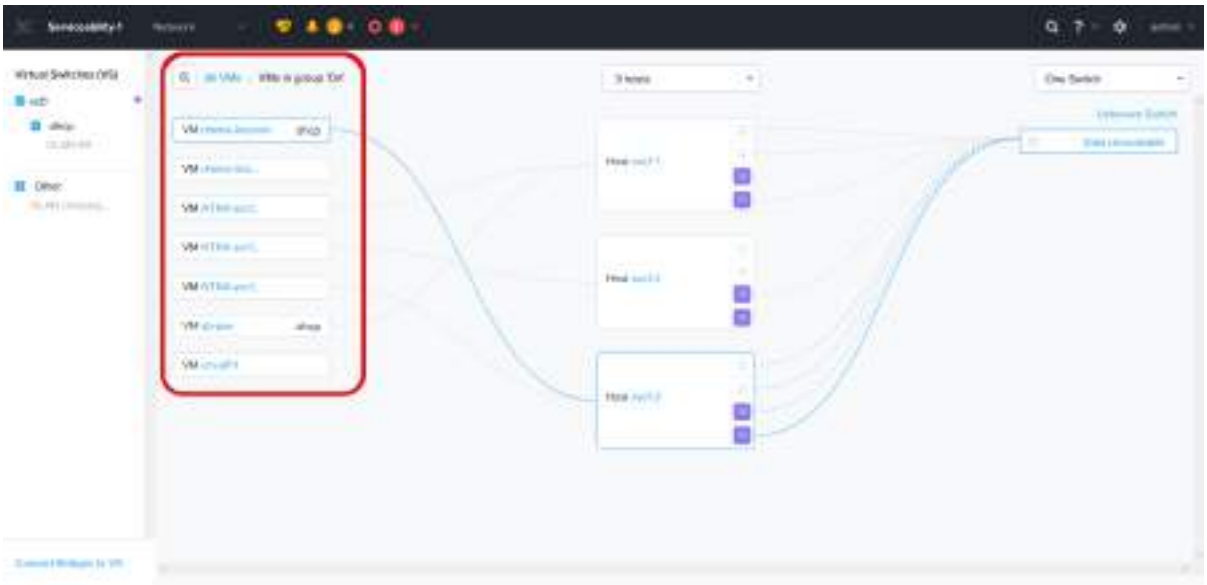


Figure 33: VM Network

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2032

2. From the virtual NIC list at the top of the dialog box, select the NIC for which you want show settings and statistics.

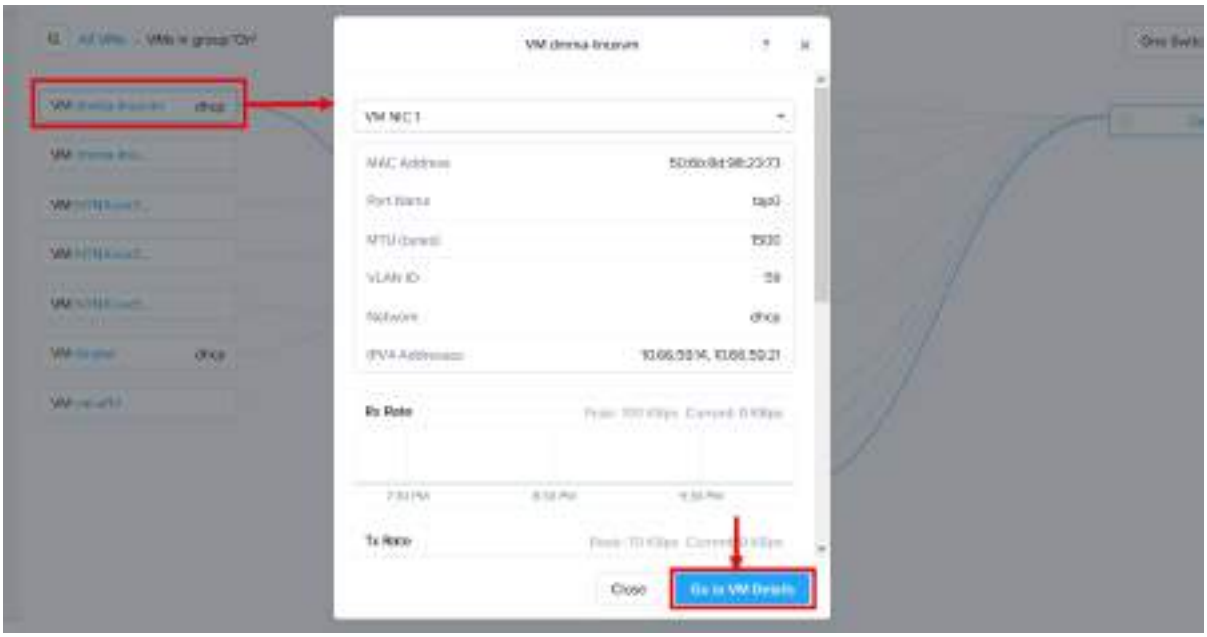


Figure 34: VM Details

For information about the statistics that are displayed for the virtual NICs, see VM NICs Tab on page 271.

3. Optionally, point to a location on a graph to view the value at that point in time.

4. If you want additional information about the VM, click **Go to VM Details**.
The **VM** table view on the **VM** page is displayed.

> **Tip:** You can return to the visualizer by pressing the back button in your browser.

Viewing Host Information

In the visualizer, you can view the internal network diagram of a Nutanix host. You can click a network component, such as a bridge or bond, to view the settings and statistics of that component.

About this task

To view host information, do the following:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2033

Procedure

1. In the topology view, hover on or click a host interface to view the settings of the interface.

   For a host interface, statistics are shown in addition to interface settings. Point to a location on a graph to view the value at that point in time.

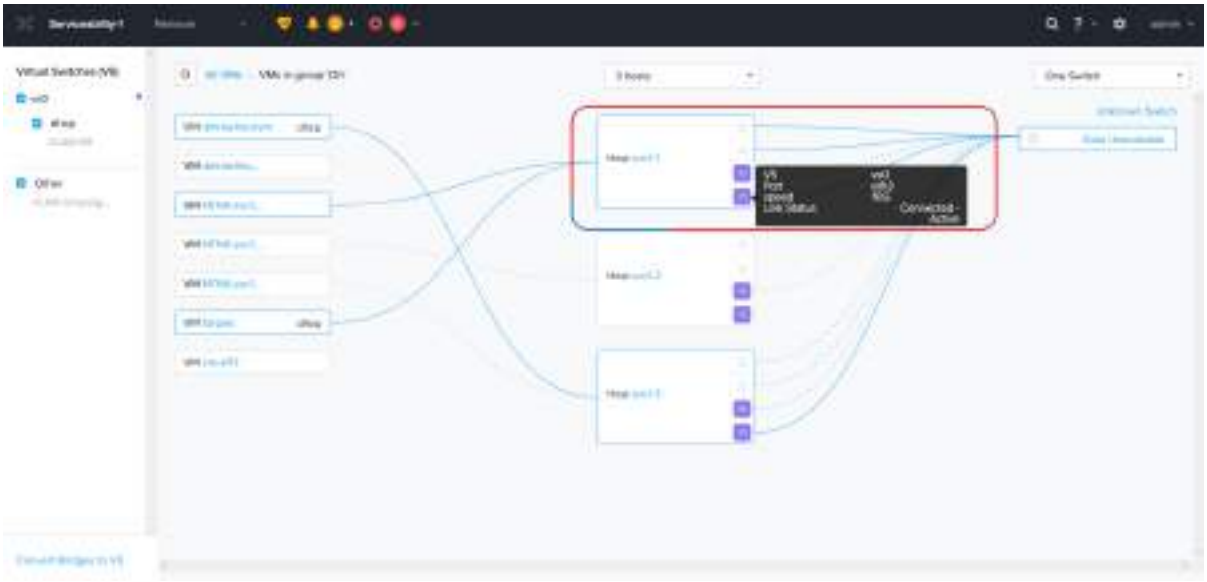


Figure 35: Host Interface Information

For information about the statistics that are displayed for the host NICs, see Host NICs Tab on page 201.

These lines are highlighted because they are related to the host of selected VM. A solid line leading from a bond to a host interface indicates the uplink is connected and is an active connection. A dotted line indicates a connected but unconfigured passive bond interface. A dotted line also indicates an uplink on a virtual switch with the bond type configured as No Uplink Bond.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2034

2. Click the name of a host.
   The host network information window appears. The window shows a diagram of the host's internal network. The right pane displays host network information.

Figure 36: Host Network

3. Click any network component in the diagram and view its network settings and statistics in the right pane.

   » Click the Controller VM, and then, in the right pane, select a virtual NIC from the list to view settings and statistics of that virtual interface. Optionally, point to a location on a graph to view the value at that point in time.

   For information about the statistics that are displayed for the virtual NICs, see VM NICs Tab on page 271.

   » Click a virtual switch to view the configuration details of the virtual switch.

   » Click a bridge to view the configuration details of the bridge.

   A solid rectangle indicates an external bridge. A dotted rectangle indicates an internal bridge.

   » Click a bond to view the settings of the bond.

4. If you want additional information about the host, click **Go to VM Details**.
   The **Host** table view on the **Hardware** page is displayed.

> **Tip:** You can return to the visualizer by pressing the back button in your browser.

Viewing Switch Information

In the visualizer, you can view both switch-level information and interface-level information.

Viewing Switch-Level Information

Switch-level information includes details such as switch name, vendor, and management IP address.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2035

About this task

To view switch-level information, do the following:

Procedure

1. In the topology view, click the name of a switch.
   The switch information window is displayed.
2. To view additional switch information, click **Go to Switch Details**.

   > **Note:** When you open the network visualizer to view switch details in the Prism Element web console, it might take up to 30 seconds for the switch port statistics to populate. This issue might also cause the same delay in the Switch Details table view.

   The **Switch** view on the **Hardware** page is displayed.

   > **Tip:** You can return to the visualizer by pressing the back button in your browser.

Viewing Interface-Level Information

Interface-level information includes details such as interface name, physical address, and interface type. The visualizer also displays statistics for each interface.

About this task

To view interface-level information, do the following:

Procedure

1. Click a switch interface.
   The switch port information window is displayed. The window shows both network settings and interface statistics.

   For information about the statistics that are displayed for switch interfaces, see Switch Tab on page 198.
2. Optionally, to show the value at any given point in time in a graph, point to the location on the graph.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2036

HARDWARE MANAGEMENT

A Nutanix block is a 1U or 2U chassis that contains one to four independent nodes, each optimized for high-performance compute, memory, and storage. Each node includes CPUs, DIMMs, SSD and HDD storage, fans, network connectors (multiple 10 and 1GbE ports), and other typical hardware components. Each block also includes dual power supplies. A Nutanix cluster can contain an unlimited number of nodes (and blocks), and you can expand the cluster size at any time.

- You can monitor hardware configurations and status across the cluster through the web console. For more information, see Hardware Dashboard on page 187.
- You can expand the cluster through the web console. For more information, see Expanding a Cluster on page 201.

Hardware Dashboard

The Hardware dashboard displays dynamically updated information about the hardware configuration in a cluster. To view the Hardware dashboard, select **Hardware** from the drop-down list on the far left of the main menu.

Menu Options

In addition to the main menu, the Hardware screen includes a menu bar with the following options:

- **View selector**: The Hardware dashboard provides three viewing modes.
  - Click the **Overview** option on the left to display hardware information in a summary view. For more information, see Hardware Overview View on page 188.
  - Click the **Diagram** option to display a diagram of the cluster nodes from which you get detailed hardware information by clicking on a component of interest. For more information, see Hardware Diagram View on page 188.
  - Click the **Table** option to display hardware information in a tabular form. The Table screen is further divided into host, disk, and switch views; click the **Host** tab to view host information, the **Disk** tab to view disk information, or the **Switch** tab to view switch information. For more information, see Hardware Table View on page 194.
- **Add NVMe Devices**: Click this option to attach an NVMe drive to the cluster.

  > **Note:** This option appears only if your hardware supports NVMe software serviceability. For more information, see Completing NVMe Drive Replacement (Software Serviceability) in *Hardware Replacement Documentation*.

- **Expand Cluster**: Click this option to add nodes to the cluster. For more information on how to expand a cluster, see Expanding a Cluster on page 201.
- **Repair Host Boot Device**: Click this option to repair the boot drive of your hosts.
- **Page selector**: In the Table view, hosts and disks are listed 10 per page. When there are more than 10 items in the list, left and right paging arrows appear on the right, along with the total count and the count for the current page.
- **Export table content**: In the Table view, you can export the table information to a file in either CSV or JSON format by clicking the gear icon on the right and selecting either **Export CSV** or **Export JSON** from the pull-down menu. (The browser must allow a dialog box for export to work.) Chrome, Internet Explorer, and Firefox download the data into a file; Safari opens the data in the current window.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2037

Hardware Overview View

The Hardware Overview view displays hardware-specific performance and usage statistics on the left plus the most recent hardware-specific alert and event messages on the right. Several fields include a slide bar on the right to view additional information in that field. The displayed information is dynamically updated to remain current.

> **Note:** For information about how the statistics are derived, see Understanding Displayed Statistics on page 70.

Table 40: Hardware Overview View Fields

Name	Description
Hardware Summary	Displays the number of hosts and blocks in the cluster. It also displays the Nutanix model number.
Hosts	Displays the number of hosts in the cluster broken down by on, off, and suspended states. It also displays the number of discovered nodes that have not yet been added to the cluster.
Disks	Displays the total number of disks in the cluster broken down by tier type (SSD-PCIe, SSD-SATA, DAS-SATA).
CPU	Displays the total amount of CPU capacity (in GHz) in the cluster.
Memory	Displays the total amount of memory (in GBs) in the cluster.
Top Hosts by Disk IOPS	Displays I/O operations per host for the 10 most active hosts.
Top Hosts by Disk IO Bandwidth	Displays I/O bandwidth used per host for the 10 most active hosts. The value is displayed in an appropriate metric (MBps, KBps, and so on) depending on traffic volume.
Top Hosts by Memory Usage	Displays the percentage of memory capacity used per host for the 10 most active hosts.
Top Hosts by CPU Usage	Displays the percentage of CPU capacity used per host for the 10 most active hosts.
Hardware Critical Alerts	Displays the five most recent unresolved hardware-specific critical alert messages. Click a message to open the Alert screen at that message. You can also open the Alert screen by clicking the **view all alerts** button at the bottom of the list. For more information, see Alerts Dashboard in *Prism Element Alerts and Events Reference Guide*.
Hardware Warning Alerts	Displays the five most recent unresolved hardware-specific warning alert messages. Click a message to open the Alert screen at that message. You can also open the Alert screen by clicking the **view all alerts** button at the bottom of the list.
Hardware Events	Displays the ten most recent hardware-specific event messages. Click a message to open the Event screen at that message. You can also open the Event screen by clicking the **view all events** button at the bottom of the list.

Hardware Diagram View

The Hardware Diagram view displays information about hosts and disks. The displayed information is dynamically updated to remain current.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2038

The Hardware Diagram view screen is divided into two sections:

- The top section is an interactive diagram of the cluster blocks. Clicking on a disk or host (node) in the cluster diagram displays information about that disk or host in the summary section.
- The bottom **Summary** section provides additional information. It includes a details column on the left and a set of tabs on the right. The details column and tab content varies depending on what has been selected.

> **Note:** For information about how the statistics are derived, see Understanding Displayed Statistics on page 70.

Host Details

Selecting a host in the diagram displays information about that host in the lower section of the screen.

- When a host is selected, **Summary:** ***`host_name`*** appears below the diagram, and action links appear to the right of this line:
  - Click the **Turn On LED** link to light up the host LED light on the chassis.
  - Click the **Turn Off LED** link to turn off the host LED light on the chassis.
  - Click the **Remove Host** link to remove this host from the cluster.
- Five tabs appear that display information about the selected host: **Host Performance**, **Host Usage**, **Host Alerts**, **Host Events**, and **Host NICs**.

Table 41: Host Detail Fields

Parameter	Description	Values
Host Name	Displays the name of the host.	(host name)
Hypervisor IP	Displays the IP address assigned to the hypervisor running on the host.	(IP address)
Controller VM IP	Displays the IP address assigned to the Controller VM.	(IP address)
IPMI IP	Displays the IP address of the Intelligent Platform Management Interface (IPMI) port. An IPMI port is used for the hypervisor host console. This field does not appear in Prism Central.	(IP address)
Node Serial	Displays the node serial number. The node serial is a unique number passed through from the manufacturer. (The form can vary because it is determined by each manufacturer.)	(manufacturer serial number)
Block Serial	Displays the block serial number.	(block serial number)
Block Model	Displays the block model number.	(model series number)
Storage Capacity	Displays the total amount of storage capacity on this host.	xxx [GB|TB]
Disks	Displays the number of disks in each storage tier in the host. Tier types vary depending on the Nutanix model type.	DAS-SATA: (number), SSD-SATA: (number), SSD-PCIe: (number)
Memory	Displays the total memory capacity for this host.	xxx [MB|GB]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2039

Parameter	Description	Values
CPU Capacity	Displays the total CPU capacity for this host.	xxx [GHz]
CPU Model	Displays the CPU model name	(CPU model name)
No. of CPU Cores	Displays the number of CPU cores on this host.	(number of CPU cores)
No. of Sockets	Displays the number of sockets.	(number of sockets)
No. of VMs	Displays the number of VMs running on this host.	(number)
Oplog Disk %	Displays the percentage of the operations log (oplog) capacity currently being used. The oplog resides on the metadata disk.	[0 - 100%]
Oplog Disk Size	Displays the current size of the operations log. (The oplog maintains a record of write requests in the cluster.) A portion of the metadata disk is reserved for the oglog, and you can change the size through the nCLI.	xxx [GB]
Monitored	Displays whether the host is high availability (HA) protected. A **true** value means HA is active for this host. A **false** value means VMs on this host are not protected (will not be restarted on another host) if the host fails. Normally, this value should always be **true**. A **false** value is likely a sign of a problem situation that should be investigated.	[true|false]
Hypervisor	Displays the name and version number of the hypervisor running on this host.	(name and version #)
Datastores	Displays the names of any datastores. This field does not appear in Prism Central.	(name)

Disk Details

Selecting a disk in the diagram displays information about that disk in the lower section of the screen.

- When a disk is selected, **Summary: *`disk_name`*** appears below the diagram, and action links appear to the right of this line:
  - Click the **Turn On LED** link to light up the LED light on the disk.
  - Click the **Turn Off LED** link to turn off the LED light on the disk.
  - Click the **Remove Disk** link to remove this disk from the cluster.
- Four tabs appear that display information about the selected storage container (see following sections for details about each tab): **Disk Usage**, **Disk Performance**, **Disk Alerts**, **Disk Events**.

Table 42: Disk Detail Fields

Parameter	Description	Values
ID	Displays the disk identification number.	(ID number)
Serial Number	Displays the disk serial number.	(serial number)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2040

Parameter	Description	Values
Model	Displays the disk model number.	(model number)
Storage Tier	Displays the disk type (tier name). Nutanix models can contain disk tiers for PCIe solid state disks (SSD-PCIe), SATA solid state disks (SSD-SATA), and direct attach SATA hard disk drives (DAS-SATA) depending on the model type.	[SSD-PCIe | SSD-SATA | DAS-SATA]
Used (Physical)	Displays the amount of used space on the drive.	xxx [GB|TB]
Capacity (Physical)	Displays the total physical space on the drive.	xxx [GB|TB]
Hypervisor	Displays the IP address of the hypervisor controlling the disk.	(IP address)
Storage Pool	Displays the name of the storage pool in which the disk resides.	(name)
Status	Displays the operating status of the disk. Possible states include the following: • **Normal**. Disk is operating normally. • **Data migration initiated**. Data is being migrated to other disks. • **Marked for removal, data migration is in progress**. Data is being migrated in preparation to remove disk. • **Detachable**. Disk is not being used and can be removed.	Normal; Data migration initiated; Marked for removal, data migration is in progress; Detachable
Mode	Displays whether the disk is currently online or offline.	[online|offline]
Self Encryption Drive	Displays whether this is a self encrypting drive (SED).	[present|not present]
Password Protection Mode [SED only]	Displays whether data-at-rest encryption is enabled for the cluster. When it is enabled, a key is required to access (read or write) data on the drive. This field appears only when the drive is a SED.	[protected|not protected]

Cluster Summary Information

When a host or disk is not selected in the diagram (or when the word **Summary** is clicked), cluster-wide summary information appears in the lower part of the screen.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2041

- The **Hardware Summary** column (on the left) includes the following fields:
  - **Blocks**. Displays the number of blocks in the cluster.
  - **Hosts**. Displays the number of hosts in the cluster.
  - **Total Memory**. Displays the total memory capacity (GBs) in the cluster.
  - **Total CPU Capacity**. Displays the total CPU capacity (GHz) in the cluster.
  - **Disks**. Displays the number of disks in each storage tier (DAS-SATA, SSD-SATA, and SSD-PCIe) in the cluster. Tier types vary depending on the Nutanix model type.
  - **Network Switches**. Displays the number of network switches being used in the cluster.
  - **GPUs**. (AHV only) Comma-separated list of GPUs installed on the host. GPU information includes the model name and a count in parentheses if multiple GPUs of the same type are installed on the host. If the firmware on the GPU is in compute mode, the string *compute* is appended to the model name. No string is appended if the GPU is in graphics mode.

    The field is hidden if no GPUs are configured or if the hypervisor is not AHV.
- Three tabs appear that display cluster-wide information (see following sections for details about each tab): **Performance Summary**, **Hardware Alerts**, **Hardware Events**.

Host Performance Tab

The Host Performance tab displays graphs of performance metrics. The tab label and number of graphs varies depending on what is selected in the diagram:

- **Performance Summary** (no host or disk selected). Displays resource performance statistics (CPU, memory, and disk) across the cluster.
- **Host Performance** (host selected). Displays resource performance statistics (CPU, memory, and disk) for the selected host.
- **Disk Performance** (disk selected). Displays disk performance statistics for the selected disk.

The graphs are rolling time interval performance monitors that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in depth analysis, you can add a monitor to the analysis page by clicking the blue link in the upper right of the graph. For more information, see Analysis Dashboard on page 334. The Performance tab includes the following graphs:

- **[Cluster-wide] CPU Usage**: Displays the percentage of CPU capacity currently being used (0 - 100%) either across the cluster or for the selected host. (This graph does not appear when a disk is selected.)
- **[Cluster-wide] Memory Usage**: Displays the percentage of memory capacity currently being used (0 - 100%) either across the cluster or for the selected host. (This graph does not appear when a disk is selected.)
- **[Cluster-wide] IOPS**: Displays I/O operations per second (IOPS) for the cluster, selected host, or selected disk.
- **[Cluster-wide] I/O Bandwidth**: Displays I/O bandwidth used per second (MBps or KBps) for physical disk requests in the cluster, selected host, or selected disk.
- **[Cluster-wide] I/O Latency**: Displays the average I/O latency (in milliseconds) for physical disk requests in the cluster, selected host, or selected disk.

Host Usage Tab

The Host Usage tab displays graphs of storage usage. This tab appears only when a host or disk is selected. The tab label varies depending on what is selected in the diagram:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2042

- **Host Usage** (host selected). Displays usage statistics for the selected host.
- **Disk Usage** (disk selected). Displays usage statistics for the selected disk.

The Usage tab displays one or both of the following graphs:

- **Usage Summary**: Displays a rolling time interval usage monitor that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in depth analysis, you can add the monitor to the analysis page by clicking the blue link in the upper right of the graph. For more information, see Analysis Dashboard on page 334.
- **Tier-wise Usage** (host only): Displays a pie chart divided into the percentage of storage space used by each disk tier on the host. Disk tiers can include DAS-SATA, SSD-SATA, and SSD-PCIe depending on the Nutanix model type.

Host Alerts Tab

The Host Alerts tab displays the unresolved alert messages about hosts, disks, and other hardware in the same form as the Alerts page. For more information, see Alerts Summary View. Click the **Unresolved X** button in the filter field to also display resolved alerts.

Host Events Tab

The Host Events tab displays the unacknowledged event messages about hosts, disks, and other hardware in the same form as the Events page. For more information, see Events Summary View. Click the **Include Acknowledged** button to also display acknowledged events.

Host NICs Tab

The Host NICs tab displays information in tabular form about the host NICs used to support traffic through the virtual NICs. (This tab appears only when a host is selected and the hypervisor is ESXi.) Each line represent a host NIC, and the following information is displayed for each NIC:

- **Host NIC**. Displays the host NIC name.
- **Speed (in KBps)**. Displays the host NIC transmission speed.
- **MAC Address**. Displays the host NIC MAC address.
- **Received Packets**. Displays the number of packets received by the host NIC.
- **Transmitted Packets**. Displays the number of packets transmitted by the host NIC.
- **Dropped Rx Packets**. Displays the number of received packets dropped by the host NIC.
- **Dropped Tx Packets**. Displays the number of transmitted packets dropped by the host NIC.
- **Rx Rate**. Displays the host NIC received packets rate.
- **Tx Rate**. Displays the host NIC transmitted packets rate.
- **Network Usage Rate**. Displays the host NIC total network usage rate.

When you click a host NIC entry, a set of usage graphs about that NIC appear below the table:

- **Total Packets Received**. Displays a monitor of the total packets received over time. Place the cursor anywhere on the line to see the rate for that point in time. (This applies to all the monitors in this tab.)
- **Total Packets Transmitted**. Displays a monitor of the total packets that were transmitted.
- **Dropped Packets Received**. Displays a monitor of received packets that were dropped.
- **Dropped Packets Transmitted**. Displays a monitor of transmitted packets that were dropped.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2043

- **Error Packets Received**. Displays a monitor of error packets that were received.

Hardware Table View

The Hardware Table view displays information about hosts and disks in a tabular form. Click the **Host** tab in the screen menu bar to display host information; click the **Disk** tab to display disk information; click the **Switch** tab to display switch information. The displayed information is dynamically updated to remain current.

The Hardware table view is divided into two sections:

- The top section is a table. Each row represents a single host or disk and includes basic information about that host or disk. Click a column header to order the rows by that column value (alphabetically or numerically as appropriate).
- The bottom **Summary** section provides additional information. It includes a details column on the left and a set of tabs on the right. The details column and tab content varies depending on what has been selected.

> **Note:** For information about how the statistics are derived, see Understanding Displayed Statistics on page 70.

Host Tab

Clicking the **Host** tab displays information about hosts in the cluster.

- The table at the top of the screen displays information about all the hosts, and the details column (lower left) displays additional information when a host is selected in the table. The following table describes the fields in the host table and detail column.
- When a host is selected, **Summary:** ***`host_name`*** appears below the table, and action links appear on the right of this line:
  - Click the **Turn On LED** link to light up the host LED light on the chassis.
  - Click the **Turn Off LED** link to turn off the host LED light on the chassis.
  - Click the **Enter Maintenance Mode** link to put the host in maintenance mode.
  - Click the **Repair Host Boot Device** link to repair the boot drive of the selected host.
  - Click the **Remove Host** link to remove this host from the cluster.
- Five tabs appear that display information about the selected host: **Host Performance**, **Host Usage**, **Host Alerts**, **Host Events**, and **Host NICs**.

Table 43: Host Table and Detail Fields

Parameter	Description	Values
Host Table Fields (upper screen)		
Host Name	Displays the name of the host.	(host name)
Host IP	Displays the IP address assigned to the hypervisor running on the host.	(IP address)
CVM IP	Displays the IP address assigned to the Controller VM.	(IP address)
Hypervisor	Displays the hypervisor type.	[ESXi|AHV|Hyper-V]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2044

Parameter	Description	Values
CPU Usage	Displays the percentage of CPU capacity currently being used.	0 - 100%
CPU Capacity	Displays the CPU capacity of this host.	xxx [GHz]
Memory Usage	Displays the percentage of memory capacity currently being used by this host.	0 -100%
Memory Capacity	Displays the memory capacity of this host.	xxx [MiB|GiB]
Total Disk Usage	Displays the storage space used and total disk capacity of this host.	xxx [MiB|GiB|TiB] of xxx [MiB|GiB|TiB]
Disk Usage	Displays the disk usage in percentage.	xx %
Disk IOPS	Displays I/O operations per second (IOPS) for this host.	[0 - unlimited]
Disk IO B/W	Displays I/O bandwidth used per second for this host.	xxx [MBps|KBps]
Disk IO Latency	Displays the average I/O latency (in milliseconds) for this host.	xxx [ms]
Host Detail Fields (lower screen)		
Host Name	Displays the name of the host.	(host name)
Hypervisor IP	Displays the IP address assigned to the hypervisor running on the host.	(IP address)
Controller VM IP	Displays the IP address assigned to the Controller VM.	(IP address)
IPMI IP	Displays the IP address of the Intelligent Platform Management Interface (IPMI) port. An IPMI port is used for the hypervisor host console. This field does not appear in *Prism Central*.	(IP address)
Node Serial	Displays the node serial number. The node serial is a unique number passed through from the manufacturer. (The form can vary because it is determined by each manufacturer.)	(manufacturer serial number)
Block Serial	Displays the block serial number.	(block serial number)
Block Model	Displays the block model number.	(model series number)
Storage Capacity	Displays the total amount of storage capacity on this host.	xxx [GB|TB]
Disks	Displays the number of disks in each storage tier in the host. Tier types vary depending on the Nutanix model type.	DAS-SATA: (number), SSD-SATA: (number), SSD-PCIe: (number)
Memory	Displays the total memory capacity for this host.	xxx [MB|GB]
CPU Capacity	Displays the total CPU capacity for this host.	xxx [GHz]
CPU Model	Displays the CPU model name	(CPU model name)
No. of CPU Cores	Displays the number of CPU cores on this host.	(number of CPU cores)
No. of Sockets	Displays the number of sockets.	(number of sockets)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2045

Parameter	Description	Values
No. of VMs	Displays the number of VMs running on this host.	(number)
Oplog Disk %	Displays the percentage of the operations log (oplog) capacity currently being used. The oplog resides on every SSD.	[0 - 100%]
Oplog Disk Size	Displays the current size of the operations log. (The oplog maintains a record of write requests in the cluster.) A portion of every SSD is reserved for the oplog.	xxx [GB]
Monitored	Displays whether the host is high availability (HA) protected. A **Yes** value means HA is active for this host. A **No** value means VMs on this host are not protected (will not be restarted on another host) if the host fails. Normally, this value should always be **Yes**. A **No** value is likely a sign of a problem situation that should be investigated.	[Yes|No]
Hypervisor	Displays the name and version number of the hypervisor running on this host.	(name and version #)
Datastores	Displays the names of any datastores.	(name)
Secure Boot Enabled	Displays whether the host is secure boot enabled.	[Yes|No]

Disk Tab

Clicking the **Disk** tab displays information about disks in the cluster.

- The table at the top of the screen displays information about all the disks, and the details column (lower left) displays additional information when a disk is selected in the table. The following table describes the fields in the disk table and detail column.
- When a disk is selected, **Summary: *`disk_name`*** appears below the table, and action links appear on the right of this line:
  - Click the **Turn On LED** link to light up the LED light on the disk.
  - Click the **Turn Off LED** link to turn off the LED light on the disk.
  - Click the **Remove Disk** link to remove this disk from the cluster.
- Four tabs appear that display information about the selected storage container (see following sections for details about each tab): **Disk Usage**, **Disk Performance**, **Disk Alerts**, **Disk Events**.

Table 44: Disk Table and Detail Fields

Parameter	Description	Values
Disk Table Fields (upper screen)		
Disk ID	Displays the disk identification number.	(ID number)
Serial Number	Displays the disk serial number.	(serial number)
Host Name	Displays the host name.	(host name)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2046

Parameter	Description	Values
Hypervisor IP	Displays the IP address assigned to the hypervisor running on the host.	(IP address)
Tier	Displays the disk type (tier name). Nutanix models can contain disk tiers for PCIe solid state disks (SSD-PCIe), SATA solid state disks (SSD-SATA), and direct attach SATA hard disk drives (DAS-SATA) depending on the model type.	[SSD-PCIe | SSD-SATA | DAS-SATA]
Status	Displays the operating state of the disk.	online, offline
Disk Usage	Displays the percentage of disk space used and total capacity of this disk.	[0 - 100%] of xxx [GB|TB]
Disk IOPS	Displays I/O operations per second (IOPS) for this disk.	[0 - unlimited]
Disk IO B/W	Displays I/O bandwidth used per second for this disk.	xxx [MBps|KBps]
Disk Avg IO Latency	Displays the average I/O latency for this disk.	xxx [ms]
Disk Detail Fields (lower screen)		
ID	Displays the disk identification number.	(ID number)
Serial Number	Displays the disk serial number.	(serial number)
Model	Displays the disk model number.	
Storage Tier	Displays the disk type (tier name). Nutanix models can contain disk tiers for PCIe solid state disks (SSD-PCIe), SATA solid state disks (SSD-SATA), and direct attach SATA hard disk drives (DAS-SATA) depending on the model type.	[SSD-PCIe | SSD-SATA | DAS-SATA]
Used (Physical)	Displays the amount of used space on the drive.	xxx [GB|TB]
Capacity (Logical)	Displays the total physical space on the drive.	xxx [GB|TB]
Hypervisor	Displays the IP address of the hypervisor controlling the disk.	(IP address)
Storage Pool	Displays the name of the storage pool in which the disk resides.	(name)
Status	Displays the operating status of the disk. Possible states include the following: • **Normal**. Disk is operating normally. • **Data migration initiated**. Data is being migrated to other disks. • **Marked for removal, data migration is in progress**. Data is being migrated in preparation to remove disk. • **Detachable**. Disk is not being used and can be removed.	Normal; Data migration initiated; Marked for removal, data migration is in progress; Detachable
Mode	Displays whether the disk is currently online or offline.	[online|offline]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2047

Parameter	Description	Values
Self Encryption Drive	Displays whether this is a self encrypting drive (SED).	[present|not present]
Password Protection Mode [SED only]	Displays whether data-at-rest encryption is enabled for the cluster. When it is enabled, a key is required to access (read or write) data on the drive. This field appears only when the drive is a SED.	[protected|not protected]

Switch Tab

Clicking the **Switch** tab displays information about the physical switches used by the host NICs to support traffic through the virtual NICs. The table at the top of the screen displays information about the switches, and the lower portion of the screen displays additional information when a switch is selected in the table. You can configure any number of switches, but only the switches that are actually being used for virtual NIC traffic appear in this table. For more information on how to configure a switch, see Configuring Network Switch Information on page 172. The following table describes the fields in the switch table, in the detail column (lower left), and in the Physical Switch Interfaces tab (lower right).

Table 45: Switch Table and Detail Fields

Parameter	Description	Values
Switch Table Fields (upper screen)		
Switch ID	Displays the switch identification number.	(ID value)
Switch Name	Displays the switch name.	(name)
Management Addresses	Displays the switch management IP address(es).	(IP address)
Vendor Name	Displays the name of the switch vendor.	(company name)
Location Info	Displays the switch vendor location.	(company address)
Contact Info	Displays the switch vendor contact information.	(company contact)
Description	Describes the switch model and type.	(switch description)
Switch Detail Fields (lower left screen)		
Name	Displays the switch name.	(name)
Vendor Name	Displays the name of the switch vendor.	(company name)
Management Addresses	Displays the IP address(es) for the switch management ports.	(IP address)
Services	Displays the number of services being used.	(number)
Physical Switch Interfaces Fields (lower right screen)		
Physical Switch Interface	Displays the interface name.	(name)
Switch ID	Displays the switch identification number.	(ID value)
Index	Displays the index value.	(number)
MTU (in bytes)	Displays the size in bytes of the largest protocol data unit (maximum transmission unit) that the layer can pass onwards.	(number)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2048

Parameter	Description	Values
MAC Address	Displays the interface MAC address	(mac address)
Unicast Rx Pkts	Displays the number of unicast packets received.	(number)
Unicast Tx Pkts	Displays the number of unicast packets transmitted.	(number)
Error Rx Pkts	Displays the number of received packets with an error.	(number)
Error Tx Pkts	Displays the number of transmitted packets with an error.	(number)
Discard Rx Pkts	Displays the number of received packets that were discarded.	(number)
Discard Tx Pkts	Displays the number of transmitted packets that were discarded.	(number)

When you click a physical switch interface entry, usage graphs about that interface appear below the table:

- **Unicast Packets Received**: Displays a monitor of the received unicast packets over time. Place the cursor anywhere on the line to see the value for that point in time. (This applies to all the monitors in this tab.)
- **Unicast Packets Transmitted**: Displays a monitor of the transmitted unicast packets.
- **Error Packets Received**: Displays a monitor of error packets received.
- **Dropped Packets Received**: Displays a monitor of received packets that were dropped.
- **Dropped Packets Transmitted**: Displays a monitor of transmitted packets that were dropped.

Cluster Summary Information

When a host or disk is not selected in the table (or when the word **Summary** is clicked), cluster-wide summary information appears in the lower part of the screen.

- The **Hardware Summary** column (on the left) includes the following fields:
  - **Blocks**. Displays the number of blocks in the cluster.
  - **Hosts**. Displays the number of hosts in the cluster.
  - **Total Memory**. Displays the total memory capacity (GBs) in the cluster.
  - **Total CPU Capacity**. Displays the total CPU capacity (GHz) in the cluster.
  - **Disks**. Displays the number of disks in each storage tier (DAS-SATA, SSD-SATA, and SSD-PCIe) in the cluster. Tier types vary depending on the Nutanix model type.
  - **Network Switches**. Displays the number of network switches being used in the cluster.
  - **GPUs**. (AHV only) Comma-separated list of GPUs installed on the host. GPU information includes the model name and a count in parentheses if multiple GPUs of the same type are installed on the host. If the firmware on the GPU is in compute mode, the string *compute* is appended to the model name. No string is appended if the GPU is in graphics mode.

    The field is hidden if no GPUs are configured or if the hypervisor is not AHV.
- Three tabs appear that display cluster-wide information (see following sections for details about each tab): **Performance Summary**, **Hardware Alerts**, **Hardware Events**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2049

Host Performance Tab

The Host Performance tab displays graphs of performance metrics. The tab label and number of graphs varies depending on what is selected in the table:

- **Performance Summary** (no host or disk selected). Displays resource performance statistics (CPU, memory, and disk) across the cluster.
- **Host Performance** (host selected). Displays resource performance statistics (CPU, memory, and disk) for the selected host.
- **Disk Performance** (disk selected). Displays disk performance statistics for the selected disk.

The graphs are rolling time interval performance monitors that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in depth analysis, you can add a monitor to the analysis page by clicking the blue link in the upper right of the graph. For more information, see Analysis Dashboard on page 334. The Performance tab includes the following graphs:

- **[Cluster-wide] CPU Usage**: Displays the percentage of CPU capacity currently being used (0 - 100%) either across the cluster or for the selected host. (This graph does not appear when a disk is selected.)
- **[Cluster-wide] Memory Usage**: Displays the percentage of memory capacity currently being used (0 - 100%) either across the cluster or for the selected host. (This graph does not appear when a disk is selected.)
- **[Cluster-wide] IOPS**: Displays I/O operations per second (IOPS) for the cluster, selected host, or selected disk.
- **[Cluster-wide] I/O Bandwidth**: Displays I/O bandwidth used per second (MBps or KBps) for physical disk requests in the cluster, selected host, or selected disk.
- **[Cluster-wide] I/O Latency**: Displays the average I/O latency (in milliseconds) for physical disk requests in the cluster, selected host, or selected disk.

Host Usage Tab

The Host Usage tab displays graphs of storage usage. This tab appears only when a host or disk is selected. The tab label varies depending on what is selected in the table:

- **Host Usage** (host selected). Displays usage statistics for the selected host.
- **Disk Usage** (disk selected). Displays usage statistics for the selected disk.

The Usage tab displays one or both of the following graphs:

- **Usage Summary**: Displays a rolling time interval usage monitor that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in depth analysis, you can add the monitor to the analysis page by clicking the blue link in the upper right of the graph. For more information, see Analysis Dashboard on page 334)
- **Tier-wise Usage** (host only): Displays a pie chart divided into the percentage of storage space used by each disk tier on the host. Disk tiers can include DAS-SATA, SSD-SATA, and SSD-PCIe depending on the Nutanix model type.

Host Alerts Tab

The Host Alerts tab displays the unresolved alert messages about hosts, disks, and other hardware in the same form as the Alerts page. For more information, see Alerts Summary View. Click the **Unresolved X** button in the filter field to also display resolved alerts.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2050

Host Events Tab

The Host Events tab displays the unacknowledged event messages about hosts, disks, and other hardware in the same form as the Events page. For more information, see Events Summary View. Click the **Include Acknowledged** button to also display acknowledged events.

Host NICs Tab

The Host NICs tab displays information in tabular form about the host NICs used to support traffic through the virtual NICs. (This tab appears only when a host is selected.) Each line represents a host NIC, and the following information is displayed for each NIC:

- **Host NIC**. Displays the host NIC name.
- **Speed (in KBps)**. Displays the host NIC transmission speed.
- **MAC Address**. Displays the host NIC MAC address.
- **Received Packets**. Displays the number of packets received by the host NIC.
- **Transmitted Packets**. Displays the number of packets transmitted by the host NIC.
- **Dropped Rx Packets**. Displays the number of received packets dropped by the host NIC.
- **Dropped Tx Packets**. Displays the number of transmitted packets dropped by the host NIC.
- **Rx Packet Errors**. Displays the number of error packets received by the host NIC.
- **Tx Packet Errors**. Displays the number of error packets transmitted by the host NIC.

When you click a host NIC entry, a set of usage graphs about that NIC appear below the table:

- **Total Packets Received**. Displays a monitor of the total packets received by the host NIC (in KBs or MBs) over time. Place the cursor anywhere on the line to see the value for that point in time. (This applies to all the monitors in this tab.)
- **Total Packets Transmitted**. Displays a monitor of the total packets transmitted by the host NIC (in KBs or MBs) .
- **Dropped Packets Received**. Displays a monitor of received packets that were dropped.
- **Dropped Packets Transmitted**. Displays a monitor of transmitted packets that were dropped.
- **Error Packets Received**. Displays a monitor for error packets received.

Expanding a Cluster

A cluster is a collection of nodes. You can add new nodes to a cluster at any time after physically installing and connecting them to the network on the same subnet as the cluster. The cluster expansion process compares the AOS version on the existing and new nodes and performs any upgrades necessary for all nodes to have the same AOS version.

Before you begin

Ensure that the following prerequisites are met before you expand the cluster:

- Review the relevant sections in Prerequisites and Requirements on page 206 before attempting to add a node to the cluster. The process for adding a node varies depending on several factors. This section covers specific considerations based on your AOS, hypervisor, encryption, and hardware configuration.
- Check the **Health Dashboard**. If any health checks are failing, resolve them before adding any nodes. As a final check, run NCC to ensure that the cluster is healthy.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2051

- Allow any current expand cluster operations to complete.
- All nodes are in the correct metadata state by checking the **Hardware** dashboard. If any nodes show Metadata store disabled on the node or Node is removed from metadata store, enable the metadata store by clicking **Enable Metadata Store**.
- Observe the SSDs requirements for Hybrid HCI Node and All-Flash HCI Node specified in HCI Node Field Requirements topic in *Acropolis Advanced Administration Guide*.

About this task

To add one or more nodes to an existing cluster (you can add multiple nodes at the same time), do the following:

> **Note:** Steps 9-12 are for special cases (rack fault tolerance, data-at-rest encryption, and Hyper-V), and they are not in proper sequence. Refer to these steps as needed during the procedure for any that apply.

Procedure

1. Log on to the Prism Element web console.
2. Do one of the following:
   - » Click the gear icon in the main menu and then select **Expand Cluster** in the **Settings** page.
   - » Go to the **Hardware** dashboard and click the **Expand Cluster** button.
3. In the **Expand Cluster** window, select (click the radio button for) the desired option and then click the **Next** button:
   - » Select **Expand Cluster** to begin the expansion immediately (after you complete the remaining configuration steps).
   - » Select **Prepare Now and Expand Later** to prepare the nodes now but delay adding them to the cluster until a later time. Preparing the nodes includes imaging the hypervisor (if needed), upgrading the AOS version (if needed), and preparing new node network configuration (if needed).

   The network is searched for Nutanix nodes and then the **Select Host** tab appears with a graphical list of the discovered blocks and nodes. Discovered blocks are blocks with one or more unassigned factory-prepared nodes (hypervisor and Controller VM installed) residing on the same subnet as the cluster. Discovery requires that IPv6 multicast packets are allowed through the physical switch. If you see a failure message, review the requirements in Prerequisites and Requirements on page 206.
4. Do one of the following:
   - » If the list includes all desired nodes, go to the next step.
   - » If IPv6 is not supported for the cluster or the list does not include all desired nodes, go to the bottom of the list, click the **Discover Hosts Manually** button, and do the following to retry discovery using IPv4:
     1. In the **Manual Host Discovery** window, click the **+Add Host** link. A line appears in the table below the link.
     2. Enter the Controller VM IP address on that host (or the host IP address for compute-only nodes) and then click **Save**.
     3. Add more hosts as desired.
     4. When the list of hosts is complete, click the **Discover and Add Hosts** button. Manual discovery uses IPv4 to find and add the hosts to the list.

        > **Note:** For an ESXi or Hyper-V cluster, manual host discovery requires that the target node has the same hypervisor type and version. In addition, the AOS version must be lower than or equal to that of the cluster.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2052

5. Select the checkbox for each block to be added to the cluster. All nodes within a checked block are also checked automatically; clear the checkbox associated with any nodes you do not want added to the cluster.

   When a block is checked, more fields appear below the block diagram. A separate line for each node (host) in the block appears under each field name.

6. Do the following in the indicated fields for each checked block:

   a. **Host Name** (if present): Enter the name of the host.

      Enter just the host name, not the fully qualified domain name. The host name is required for Hyper-V clusters, but you can ignore the field for ESXi and AHV clusters.

   b. **Controller VM [IPv4|IPv6]**: Review the Controller VM IP address assigned to each host and do one of the following:

      > **Note:** For Controller VM, hypervisor, and IPMI, both IPv6 and IPv4 address fields appear to account for either protocol. When entering addresses, be sure to enter each IP address in the correct field for the relevant protocol. Usually you can ignore the IPv6 field and only update the IPv4 address if needed.

      - If the address is correct, do nothing in this field.
      - If the address is not correct, either change the incorrect address or enter a starting address on the top line (for multiple hosts). The entered address is assigned to the Controller VM of the first host, and consecutive IP addresses (sequentially from the entered address) are assigned automatically to the remaining hosts.

   c. **Hypervisor [IPv4|IPv6]**: Repeat the previous step for this field.

      This field sets the hypervisor IP addresses for all the hosts to be added.

   d. **IPMI IP [IPv4|IPv6]**: Repeat the previous step for this field.

      This field sets the IPMI port IP addresses for all the hosts to be added. An IPMI port is used for the hypervisor host console.

   e. When all the node values are correct, click the **Next** button (lower right).

   The network addresses are validated before continuing. If an issue is discovered, the problem addresses are highlighted in red.

7. In the **Choose Node Type** tab, select the node type (**HCI Node** or **Storage-only**) for each node from the pull-down list and then click the **Next** button.

   Selecting **HCI Node** means that the node will be added as a standard node in the cluster. Selecting **Storage-only** means that the node will be added as a storage-only node. Storage-only nodes have specific requirements. Review Storage-Only Nodes on page 233 before adding a storage-only node.

8. In the **Host Networking** tab, configure the uplinks for each management bridge or vSwitch to be created or updated for the nodes.

   The **Host Networking** tab displays a list of the target nodes where you can specify the status (active or standby) for each node's uplinks to the management bridge or vSwitch. The uplink list depends on the hypervisor of the node to be added, while the listed bridge or vSwitch is for the base cluster. The standard form for AHV uplinks is ethx (eth0, eth1, eth2, and so on); the standard form for ESXi uplinks is vmnicx (vmnic0, vmnic1, and so on.) For example, if the hypervisor is ESXi on the node but AHV on a three-node base cluster, each entry displays the AHV vSwitch name (br0 or br1), ESXi uplink name (vmnic0, vmnic1, or vmnic2),

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2053

and status (active or standby). For hypervisor-specific information, see Prerequisites and Requirements on page 206.

> **Note:** To skip network configuration, click the **Skip Networking** button.

a. Click the **Add Uplink** button for the first node.

b. Select the target link from the pull-down list in the first field.

c. Select **Active** or **Standby** for the link status from the pull-down list in the second field.

d. Repeat for all the links to configure for the node.

e. Repeat steps for each node.

f. After configuring all nodes in the list, click the **Next** button.

9. In the **Configure Host** tab, specify the hypervisor image and allowlist for nodes that require imaging.

» If the detected hypervisor and AOS version are the same as the cluster, no imaging is required and a message acknowledging that fact appears. Skip to the next step.

» If a hypervisor image is listed in the **Hypervisor: `<type>`** field and it is the desired one, skip to the next step. If you uploaded a hypervisor image when adding nodes previously (and it is still compatible for imaging the new nodes), that image appears here. You can use that image or upload a different one.

» If no hypervisor image is listed or the listed one is not the desired one, click the **Choose File** (no listed file) or **Change File** (file listed already) button. In the search window, find the image file on your workstation, and then click the **Open** button (in the search window) to upload that image file.

You must provide an ISO file for imaging ESXi or Hyper-V. You can get the required AHV image from the **Downloads** > **AHV** page of the Nutanix Support portal. For information on how to access the portal, see Accessing the Nutanix Support Portal on page 395. From AOS 6.8 release onwards, AOS does not include the AHV installation bundle. The AHV bundle on the portal is named as: AHV-DVD-x86_64-*`elx`*.nutanix.*`AHV-version`*.iso.

- Replace *`elx`* with Enterprise Linux version as el7 or el8.
- Replace *`AHV-version`* with actual AHV version.

For example, AHV-DVD-x86_64-el8.nutanix.20230302.1011.iso or AHV-DVD-x86_64-el7.nutanix.20220304.478.iso.

» If a message appears that the hypervisor image is not compatible, either select (choose and upload) a hypervisor image that is compatible or update the hypervisor ISO whitelist.

The cluster includes a hypervisor ISO allowlist, which lists the approved hypervisor images. You can only use an image that is in the approved list. For more information about the allowlist, see Hypervisor ISO Images in the *Field Installation Guide*. If your hypervisor image does not appear in the whitelist (because you created the cluster before the image was approved), you can update the whitelist as follows:

1. Download the latest hypervisor ISO whitelist from the **Downloads** > **Foundation** page of the Nutanix Support portal.
2. Click the **Update** link in the **Hypervisor ISO Whitelist** field.
3. Click the **Choose File** button (which opens a search window), find and select the whitelist file on your workstation, and then click the **Open** button.
4. Click the **Upload** button. The incompatible message disappears and you can continue provided the hypervisor image is on the uploaded whitelist.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2054

10. [rack fault tolerance only] In the **Assign Rack** tab, select the block and the rack (from the **Assign to Rack** drop-down menu) to map the block placement in that rack. To add a rack to the list, click **Create Rack**.

    This tab appears only when rack fault tolerance is enabled. For more information, see Configuring Rack Fault Tolerance on page 35.

11. [data-at-rest encryption only] In the **Encrypt Host** tab, do the following.

    This tab appears only when data-at-rest encryption is enabled with an external KMS. For more information, see Data-At-Rest Encryption. You can apply encryption licenses after the new nodes are added to the cluster.

    a. In the **Certificate Signing Request Information** field, click the **Generate and Download** link for each node to be added.

       Clicking the link generates a certificate signing request (CSR) named csr_for_discovered_node for the node, which you download to your workstation.

    b. Get the CSRs signed by a certificate authority (CA).

    c. Click the **select files** link for each key management server and upload the signed certificates for the nodes to be added.

    d. Click the **Next** button.

12. [Hyper-V only] Specify the credentials to join the new nodes to Active Directory and to a failover cluster.

    a. Specify the name of the Hyper-V failover cluster in the **Failover Cluster Name** text box.

    b. Specify the user name and password of the domain account that has the privileges to create a new or modify an existing computer account in the Active Directory domain. The user name must be in the DOMAIN \USERNAME format.

13. When all the fields are correct, click the **Run Checks** button to verify that the nodes are ready.

    This runs a set of precheck tests on the nodes. Progress messages appear in the **Expand Cluster** window. You can also monitor progress from the **Tasks** dashboard. For more information, see View Task Status on page 89.

14. When the checks pass successfully, do one of the following:

    » Click the **Expand Cluster** button to begin the cluster expansion process. (This button appears if you selected **Expand Cluster** in step 2.)

    » Click the **Prepare Node(s)** button to begin preparing the nodes. (This button appears if you selected **Prepare Now and Expand Later** in step 2.)

    The expand cluster or node preparation process begins. As with the prechecks, progress messages appear in the **Expand Cluster** window, and you can also monitor progress from the **Tasks** dashboard. Nodes are processed (upgraded or reimaged as needed) and added in parallel. Adding nodes can take some time. Imaging a node typically takes a half hour or more depending on the hypervisor.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2055

15. If the cluster has multiple storage pools, assign the new storage capacity to a storage pool after the nodes are added successfully:

    Note: When the cluster has only one storage pool, you can ignore this step because the new storage is added to that storage pool automatically.

    a. Select **Storage** from the pull-down main menu (upper left of screen) and then select the **Table** and **Storage Pool** tabs.

    b. Select the target storage pool (upper display) and then click the **update** link.

    c. In the **Update Storage Pool** window, check the **Use unallocated capacity** box in the **Capacity** line and then click the **Save** button.

    This step adds all the unallocated capacity to the selected storage pool.

    d. Go to the Tasks dashboard and monitor progress until the node addition completes successfully.

    Cluster expansion is not complete until the node is added to the metadata ring.

What to do next

One or more of the following items might apply to the added nodes. Also, see Prerequisites and Requirements on page 206.

- Nondefault timezones are not updated on added nodes and must be reconfigured manually.
- If the Controller VM password for the cluster was changed from the default, the password on any new nodes gets updated automatically to match the cluster password.
- To check Controller VM memory compatibility after cluster expansion, run the `cvm_same_mem_level_check` and `cvm_memory_check` NCC checks. For more information, see Running Checks by Using Prism Element Web Console on page 261.

  - If the `cvm_same_mem_level_check` result is FAIL, the memory size in the added nodes is not the same as the other Controller VMs in the cluster. If the memory is less than the common size, increase the memory to match.
  - If the `cvm_memory_check` result is FAIL, the Controller VM memory is less than the minimum required for the workload. Increase the memory to (at least) the minimum size.

  For information about increasing the memory of the Controller VM, see Increasing the Controller VM Memory Size on page 106. For information about the Controller VM memory size recommendations, see CVM Memory Configuration on page 105.

Prerequisites and Requirements

The process for adding a node varies depending on the AOS version, hypervisor host type, data-at-rest encryption status, and certain hardware configuration factors.

AOS Considerations

The following apply to any cluster:

- Ensure that the total number of nodes per cluster does not exceed the Cluster Maximums defined in Maximum System Values on page 51. Note that the maximum number of nodes per cluster differ per the hypervisor type and in case it is a pure hypervisor cluster (cluster with only one type of hypervisor) or mixed hypervisor cluster (cluster with more than one type of hypervisor).
- The expand cluster process does not support compute-only node preparation.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2056

- The expand cluster discovery step (finding nodes to add) requires that IPv6 multicast packets are allowed through the physical switch. Therefore, the expand cluster process does not work when IPv6 is disabled in your network. If IPv6 is not enabled currently, do one of the following:
  - Enable IPv6 in your network and retry the expand cluster operation.
  - If enabling IPv6 is not an option, the expand cluster procedure allows you to enter the IP addresses of nodes to add manually and run discovery using IPv4. This requires that you have the IP addresses before starting the expand cluster operation.
- If the Controller VM memory on a new node is less than the current nodes in the cluster, the expand cluster process increases the memory on the new node to the same base value as the current nodes. The new Controller VM is upgraded to a maximum of 32 GB.

  The Controller VM is upgraded to a maximum of 28 GB for ESXi nodes with 64 GB or less of total physical memory. With total physical memory greater than 64 GB, the existing Controller VM memory is increased by 4 GB.
- A new node is reimaged automatically before being added under certain conditions. The following table describes those conditions.

Table 46: Node Imaging Criteria

Configuration	Description
Same AOS and hypervisor versions	The node is added to the cluster without reimaging it.
Same hypervisor version but different AOS version	The node is automatically reimaged before it is added. However, if the AOS version on the node is higher than the version on the cluster, you can upgrade the cluster to the higher version. If you do not upgrade the base cluster to match the node AOS version, the node is reimaged automatically to match the lower AOS version of the cluster. For more information about how to upgrade your cluster, see the Life Cycle Manager Guide.
Same AOS version but different hypervisor version	The node is automatically reimaged before it is added.

Note: If you are expanding a cluster (now) on which the network is segmented only by traffic type (management and backplane), see Network Segmentation During Cluster Expansion in the *Security Guide*.

AHV Considerations

The following apply to clusters running AHV:

- If the Controller VMs in the cluster reside in a VLAN configured network, the discovery process still finds any factory-prepared nodes regardless of their current VLAN status (configured or not configured).
- You cannot reimage a node running discovery OS when Link Aggregation Control Protocol (LACP) is enabled on the cluster. Discovery OS is a pre-installed software on Nutanix nodes that allows the nodes to be discovered. Prepare the node with LACP using a Foundation VM.
- If you plan to use an NVIDIA host driver on the host that you want to add to an existing cluster with GPU nodes, do not install the driver before adding the host to the cluster. Instead, first add the new hosts to the cluster and then use the install_host_package script to install the driver on the host. For more information on using the script, see Installing the NVIDIA GRID Driver.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2057

- Network configuration has the following restrictions and requirements:
  - You cannot migrate management from br0 to other bridges.
  - You can only have the Controller VM management interface (eth0) and hypervisor management interface deployed on the br0 bridge.

ESXi Considerations

The following apply to clusters running ESXi:

- Before adding a host running ESXi 7.0U2 and later versions, with Trusted Platform Module (TPM) 2.0 enabled, to a cluster, Nutanix recommends that you backup the recovery key created when encrypting the host with TPM. For information on how to generate and backup the recovery key, see *KB 81661* in the *VMware documentation*. Ensure that you use this recovery key to restore the host configuration encrypted by TPM 2.0 if it fails to start after adding the host to your cluster. For information on how to restore an encrypted host, see *KB 81446* in the *VMware documentation*. If you don't have the recovery key, and if the host fails to start, contact Nutanix Support.
- If the ESXi root user password was changed from the default, the expand cluster operation might fail. In this case, reset the ESXi root user password to the default, and then retry the expand cluster procedure. For default cluster credentials, see KB 1661.
- While expanding a Nutanix cluster running NSX enabled ESXi hosts, add the newly imaged node to the Nutanix cluster where the host and CVM management network are configured with a standard vSwitch, and then add the node in NSX manager. Otherwise, the cluster expansion operation fails with the following error. For information on how to expand a cluster, see Expanding a Cluster on page 201.

  ```
  Failed to get VLAN tag of node <MAC Address of the node>
  ```

- The expand cluster operation supports mixed node (ESXi + storage-only) clusters only if network segmentation is not enabled. If network segmentation is enabled for the mixed cluster, you cannot use the expand cluster operation. However, you can use the expand cluster operation for a mixed cluster that has backplane segmentation enabled and the storage-only nodes are hosted with AOS 6.1 or newer release.
- Network configuration has the following restrictions and requirements:
  - You cannot configure the network when either a target node or the base cluster has LACP enabled. Prepare LACP nodes offline using a Foundation VM.
  - You cannot migrate management from vSwitch0 to another standard vSwitch.
  - Management interfaces must either be on a VSS or a DVS; a mixed setup is not supported.
  - If on VSS, the Controller VM management interface (eth0) and the hypervisor management interface must be deployed on vSwitch0 and connected to port group VM Network and Management Network, respectively.
  - If on DVS, all Controller VM management interfaces and all host management interfaces must be connected to the same distributed virtual switch and same port group. (However, the Controller VM interfaces can be connected to a different DVS port group than the host management interfaces.)
  - Segmented network interfaces (backplane, volume, DR) must be on same vSwitch type (VSS or DVS) as the management.
  - If network segmentation is enabled on the base cluster and the backplane is deployed on a separate vSwitch than management, you can create vSwitches (VSS or DVS) and prepare the required Controller VM interfaces. (Manual switch configuration is required for expand now but is integrated into the expand later work flow.)
  - If the base cluster is on DVS and you are doing an expand later, you can migrate the target nodes from the default vSwitch0 to that DVS.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2058

- If the Controller VMs in the cluster reside in a VLAN configured network, you must first configure the new nodes in the same VLAN before attempting to add them. Otherwise, the discovery process does not find these nodes. For more information about VLAN configuration instructions, see Discovering Nodes in a VLAN-Segmented Network in the *Field Installation Guide*.
- To expand a cluster (now) configured with DVS for Controller VM external communication, ensure that you do the following:
  - Expand DVS with the new node.
  - Make sure both the host and the CVM are configured with DVS.
  - Make sure that host to CVM and CVM to CVM communications are working.
  - Follow the cluster expansion procedure.
- After adding the new nodes, note the following:
  - The common Nutanix datastores are mounted on the new nodes by default after cluster expansion.
  - The target storage containers must be set to mount on the new hosts. You can check the mount status from the **Storage** dashboard. Click the **Storage Container** tab, select the target storage container, click the **Update** button, and verify that **Mount on all ESXi Hosts** (or the new hosts are checked in **Mount/Unmount on the following ESXi Hosts**) is selected in the **NFS DATASTORE** field.
  - If an added node has an older processor class than the existing nodes in the cluster, cluster downtime is required to enable EVC (enhanced vMotion compatibility) with the lower feature set as the baseline. For an indication of the processor class of a node, see the **Block Serial** field in the **Hardware** dashboard. For more information, see Hardware Diagram View on page 188 or Hardware Table View on page 194. For more information on enabling EVC, see vSphere EVC Settings in the *vSphere Administration Guide for Acropolis*.

    Caution: If you mix processor classes without enabling EVC, vMotion/live migration of VMs is not supported between processor classes. If you add the host with the newer processor class to vCenter Server before enabling EVC, cluster downtime is required to enable EVC later because all VMs (including the Controller VM) must be shut down.
  - Add the new nodes to the appropriate vCenter Server cluster. If an added node has a newer processor class (for example, Haswell) than the existing nodes in the cluster (Ivy Bridge or Sandy Bridge), enable EVC with the lower feature set as the baseline before adding the node to vCenter.
  - If you are adding multiple nodes to an existing EVC-enabled vCenter cluster, which requires powering off the Controller VM for each node to complete the addition, add just one node at a time and wait for data resiliency to return to *OK* before adding the next node to vCenter.

    Caution: Adding multiple nodes to vCenter simultaneously can cause a cluster outage when all the Controller VMs are powered off at the same time.
  - If you are adding a node to a cluster where HA is enabled with APD and VMCP is enabled, you must enable APD and APD timeout on the new host.
  - If you are adding new nodes to vCenter EVC configured cluster, ensure the following requirements.
    - Enabling EVC requires ESXi version 6.0 or above.
    - All ESXi nodes should be on same version and build.

Hyper-V Considerations

The following apply to clusters running Hyper-V:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2059

- Network preparation is not supported. To bypass this step and prepare the nodes otherwise, click the **Skip Networking** button when you get to the **Networking** tab. In addition, imaging to AHV or ESXi is not possible if the node or base cluster is Hyper-V.
- If the Controller VMs in the cluster reside in a VLAN configured network, you must first configure the new nodes in the same VLAN before attempting to add them. Otherwise, the discovery process does not find these nodes. For more information about VLAN configuration instructions, see Discovering Nodes in a VLAN-Segmented Network in the *Field Installation Guide*.
- After adding the new nodes, if you manage your Hyper-V cluster by using Microsoft System Center VM Manager (SCVMM), do not use the Prism Element web console or Microsoft Failover Cluster Manager to add the new node to the failover cluster. Instead, use SCVMM to add the node to the Hyper-V cluster and then perform the following steps in the SCVMM user interface.
  1. Open the SCVMM user interface.
  2. Refresh the cluster in SCVMM. The new node is displayed under the failover cluster in the **Pending** state.
  3. Right-click the node and select **Add to host cluster**.
  4. Choose a run-as account that has the local administrator permissions on the new node.
  5. Click **OK**. The SCVMM agent is installed on the node and file shares are registered to the new node.
  6. Update the networking and other settings of the node to match your standard configuration.

For Microsoft Windows Server 2012 R2 deployments, after adding the node to the cluster in SCVMM, ensure that node disks are not added as clustered resources. Open the Failover Cluster Manager and click **Storage** > **Disks** to check.

Data-At-Rest Encryption Considerations

The following apply to clusters with data-at-rest encryption enabled. For more information, see Data-At-Rest Encryption.

- Configure data-at-rest encryption for the new nodes. The new nodes must have self-encrypting disks or software-only encryption.
- If the cluster uses an external key manager server (KMS), either with self-encrypting drives or software only, then reimaging cannot be done through the expand cluster workflow. In this case, any nodes to add must already have the correct hypervisor and AOS version. Use Foundation to image the nodes (if needed) before attempting to add them to the cluster.
- If an encrypted cluster uses an external KMS, the new node might not be able to resolve the DNS name of the KMS. Therefore, you must manually update the resolv.conf file on the new node to enable communication between the node and the KMS.
- Adding a node to a cluster with self-encrypting drives (SED) where the added node is running a different hypervisor is not supported. In this case, image the node to the same hypervisor by using Foundation before adding it to the SED cluster. For more information, see KB 4098.

Nutanix Clusters Considerations

The following apply to clusters hosted on a cloud platform:

- When expanding a cluster on AWS, the nodes are not added to the Cassandra ring (wait in a queue) until there are enough nodes to extend the ring. In addition, new nodes are added to the Cassandra ring only when they are do not break domain awareness. (Other services remain unaffected.)

Hardware Considerations

Note the following when it applies to the nodes you are adding:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2060

- Ensure that you use the minimum version of Foundation required by your hardware platform. To determine whether Foundation needs an upgrade for a hardware platform, see the respective system specifications guide. If the nodes you want to include in the cluster are of different models, determine which of their minimum Foundation versions is the most recent version, and then upgrade Foundation on all the nodes to that version.
- When adding all-SSD nodes to an existing cluster, the minimum number of all-SSD nodes added must be equal to the maximum replication factor in the cluster.
- If you are adding a node with a different processor class to the cluster, ensure that there are no running VMs on the node and the host has the following configuration:
  - ESXi: Verify that EVC is enabled on the cluster.
  - Hyper-V: If you want to move the VMs between the nodes, ensure that you have selected the **Migrate to a physical computer with a different processor version** option for each VM by browsing to **Settings** > **Processor** > **Compatibility** in the **Action** pane of the Hyper-V Manager.

    Note: Do not shut down more than one Controller VM at the same time.
- If you expand a cluster by adding a node with older generation hardware to a cluster that was initially created with later generation hardware, power cycle (do not reboot) any guest VMs before migrating them to the added older generation node or before upgrading the cluster.

  Guest VMs are migrated during hypervisor and firmware upgrades (but not AOS upgrades).

  For example, if you are adding a node with G4 Haswell CPUs to a cluster that also has newer G5 nodes with Broadwell CPUs, you must power cycle guest VMs hosted on the G5 nodes before you can migrate the VMs to the node with G4 CPUs. Power cycling the guest VMs enables them to discover a CPU set compatible with older G4 processors.

  In rare cases, certain CPU features might be deprecated in the new generation of CPUs. For example, Intel introduced MPX in Skylake class of CPUs and deprecated it with Ice Lake. In such cases, introduction of Ice Lake (newer) CPUs to an all-Skylake cluster can cause problems with existing VMs that are running with MPX. Such VMs must be power cycled.

  Power cycle guest VMs from the Prism Element web console VM dashboard. Do not perform a Guest Reboot; a VM power cycle is required in this case.
- If you physically add a node to a block (for example, a single node shipped from Nutanix is placed into an empty slot in an existing chassis), log on to the Controller VM for that node, and update the following parameters in the /etc/nutanix/factory_config.json file:
  - rackable_unit_serial: Set it to the same value as the other Controller VMs in the same block.
  - node_position: Set it to the physical location of the node in the block (A, B, C, D).

  After changing the configuration file, restart Genesis with the `genesis restart` command.

Expand a Cluster with Flow Virtual Networking Enabled

Check if the cluster uses non-default virtual switches

If you use non-default virtual switches for VPC (Flow Virtual Networking) traffic in an AHV cluster, prepare the new nodes and the existing AHV clusters accordingly. For the steps to check if the cluster uses non-default virtual switches for VPC traffic, see Verifying if the Cluster uses Non-Default Virtual Switch on page 212.

Important:

If the check result (output of the acli atlas_config.get command) shows the `vpc_east_west_traffic_config` section with `dvs_uuid` displaying the UUID of a non-default virtual switch, follow the procedure in this section.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2061

If the `vpc_east_west_traffic_config` section does not exist, do not follow the procedure in this section.

Cluster Network

This procedure assumes the following cluster network configuration:

- vs0 is the default virtual switch for Controller VM and AHV communications.
- All bridges are configured with Active-Active with LACP.

- To prepare the new clusters for cluster expansion, see Preparing the New Nodes for Addition to Existing AHV Cluster on page 213.
- To verify that the new node is adequately prepared for expansion of the existing cluster, see Verifying the New Node Setup on page 213.
- To expand the cluster with the new node you prepared, see Expanding a Cluster with Flow Virtual Networking Enabled on page 215.

Verifying if the Cluster uses Non-Default Virtual Switch

This section provides the steps to check if the cluster uses non-default virtual switches to route VPC traffic.

About this task

Use the acli atlas_config.get command to check if the cluster uses non-default virtual switches to route VPC traffic.

Procedure

1. Log on to the CVM and run the following command.

```
nutanix@cvm$ acli
acli>
```

2. Run the following command at the `acli` prompt.

```
acli> atlas_config.get
```

A sample output is as follows:

```
config {
  anc_domain_name_server_list: "10.xxx.xxx.xxx"
  dvs_physnet_mapping_list {
    dvs_uuid: "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
    physnet: "physnet1"
  }
  enable_atlas_networking: True
  logical_timestamp: 54
  minimum_ahv_version: "20201105.2016"
  ovn_cacert_path: "/home/certs/OvnController/ca.pem"
  ovn_certificate_path: "/home/certs/OvnController/OvnController.crt"
  ovn_privkey_path: "/home/certs/OvnController/OvnController.key"
  ovn_remote_address: "ssl:anc-ovn-external.default.xxxx.nutanix.com:6652"
  vpc_east_west_traffic_config {
    dvs_uuid: "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
    permit_all_traffic: True
  }
}
```

Check if the vpc_east_west_traffic_config section is displayed in the output.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2062

3. Run the following command at the `acli` prompt to verify the UUIDs of all virtual switches.

   ```
   acli> net.get_virtual_switch *
   ```

   The sample output provides the UUIDs of all the virtual switches. Check the virtual switch UUID that matches the value of `dvs_uuid` available in the output of the previous step. Check if `default: True` attribute is not available for this virtual switch in the output, this virtual switch is the non-default virtual switch.

   For information on commands for managed networks, see the Command Reference.

Preparing the New Nodes for Addition to Existing AHV Cluster

About this task

Before imaging each new node with Foundation software, perform these steps to prepare all the new nodes you are adding to the existing cluster:

- (If Secure Boot is used in the cluster) Ensure that the node is booting with UEFI and not in Legacy BIOS. Ensure that Foundation does not change the node to boot mode back to Legacy BIOS. Change the Foundation settings if required.
- Ensure that the firmware on the node is consistent with the firmware on the existing nodes in the cluster. If feasible, update the firmware on the node to match the firmware version on the nodes in the cluster.
- Use the appropriate Foundation version to image the node with the same AOS and AHV versions as those on *the cluster* to which you are adding the node. This is essential to prevent the cluster expansion process from running another Foundation imaging process and wiping out all prepared elements.

After imaging each node with Foundation software, perform these steps to prepare all the new nodes you are adding to the existing cluster:

Procedure

1. (If Secure Boot is used in the cluster) Enable Secure Boot for the node.
2. Check all the physical port to Ethernet port mappings to ensure that the physical connectivity matches the logical configuration. Check if these mappings are consistent with the mappings in the existing nodes. This is to ensure that AHV enumerates the Ethernet port numbering and, hence, the Ethernet to bridge (virtual switch) mapping correctly.
3. Configure default virtual switch vs0 (and bridge br0) and the uplinks to be consistent with the existing nodes. Any non-default virtual switches such as vs1 and vs2 (with bridges br1 and br2 respectively) that are created after the cluster expansion need not be created pre-created in the new nodes. Pre-create and configure on the new node only those non-default virtual switches that already exist on the nodes in the cluster.

What to do next

Verify the new node setup to ensure that it is adequately prepared for cluster expansion.

Verifying the New Node Setup

About this task

Before you expand the existing cluster with the new node, verify that the new node is adequately prepared.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2063

Procedure

1. Ensure that the new node is physically installed at the required location. To verify that the new node is physically installed correctly, do the following.
   a. Ensure that redundant power cables are connected and power failover is tested after powering on the node.
   b. Ensure that the node boots in AHV.
   c. Ensure that the physical network connections are made in accordance with the physical connections on the existing nodes in the cluster.
      Ensure that:
      - Each virtual switch on the new node has dual redundant uplinks.
      - The NICs have the same speed across all the nodes in the cluster.
      - All the physical connections have the link lights on.
2. Log on to Controller VM on the new node and run the manage ovs show interfaces command to check if the necessary interfaces are up and displaying the necessary speed.
3. Perform network reachability tests to ensure that AHV, Controller VM and IPMI (management connectivity) are reachable over the network.
4. Perform NIC failover tests for the bridge (br0) on the default virtual switch vs0. Perform these tests from a local console that has access to the new AHV host.
   a. Log on to AHV via a shell session.
   b. Ping the default gateway of the network. Check the response for connectivity and latency. A good response would show low latency.
   c. Disconnect both the uplinks for the default virtual switch. The ping responses display failure.
   d. Reconnect only the first uplink and check the duration between the link light coming up and the positive ping response. Nutanix recommends a duration of less than two seconds.
   e. Disconnect the first uplink. The pings fail again.
   f. Reconnect only the second uplink and check the duration between the link light coming up and the positive ping response.
   g. Reconnect the first uplink and check whether the pings fail. The pings must continue to display positive responses with low latencies.

   Repeat these steps after logging on to the Controller VM on the new node.

   If you find any issues with the failover, resolve the same before proceeding further with cluster expansion.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2064

5. To check Secure Boot and vs0 configurations, do the following:

   a. Log on to the AHV host using a shell session and run the following command:

      ```
      AHV# mokutil --sb-state
      ```

      The output of the command indicates that Secure Boot is enabled.

   b. Check the LACP status on the AHV using the following command:

      ```
      AHV# ovs-appctl lacp/show
      ```

      The status of each uplink bond must be displays as **Negotiated** and not as **Active**.

   c. Log on to the Controller VM on the new node and run the following command to display the uplink status.

      ```
      nutanix@cvm$ manage ovs show uplinks
      ```

      Check the bridges, Ethernet and uplink bond configurations

      Ensure that all issues found at this stage are resolved before proceeding to cluster expansion.

Expanding a Cluster with Flow Virtual Networking Enabled

Use this procedure when you are expanding an AHV cluster registered to a Prism Central and where the Flow Virtual Networking Network Controller enabled in Prism Central and GENEVE traffic is moved to non-default virtual switches.

Before you begin

For cluster network configuration assumed for this procedure, see Expand a Cluster with Flow Virtual Networking Enabled on page 211.

See Prerequisites and Requirements before expanding a cluster using Prism Element web console .

Before expanding the existing cluster, prepare the new nodes. For more information, see Preparing the New Nodes for Addition to Existing AHV Cluster on page 213 and Verifying the New Node Setup on page 213.

About this task

The procedure laid out in the following steps can be implemented only if the new node is not re-imaged by Foundation during cluster expansion.

> **Note:** The Flow Virtual Networking networking stack (Network Controller with brAtlas) does not exist in the new node. Any VM migrations to the new node fail.

Procedure

1. Disable Acropolis Dynamic Scheduling (ADS). This step ensures that no VMs are migrated to the new node during the cluster expansion.

   Log on to the CVM and run the following commands to check the current status of ADS:

   ```
   nutanix@cvm$ acli
   acli> ads.get
   ```

   Check if ADS status is enabled or disabled.

   Run the following command to disable ADS:

   ```
   acli> ads.update enable=false
   ```

   Check the status of ADS by running the `ads.get` command to ensure that ADS is disabled.

2. Log on to the Prism Element web console of the cluster. You need a minimum of Cluster Admin privileges to run the cluster expansion workflow in Prism Element web console.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2065

3. Do one of the following:

   » Click the gear icon in the main menu and then select **Expand Cluster** in the **Settings** page.

   » Go to the **Hardware** dashboard and click the **Expand Cluster** button.

4. Select the **Expand Cluster** option and click **Next**.
   This starts the discovery process that searches for Nutanix nodes and blocks. The result of this discovery process provides a list of discovered nodes.

   Discovery requires that IPv6 multicast packets are allowed through the physical switch. If you see a failure message, review the requirements in Prerequisites and Requirements on page 206.

5. Do one of the following:

   » If the list includes all specified prepared nodes, go to the next step.

   » If IPv6 is not supported for the cluster or the list does not include all desired nodes, go to the bottom of the list, click the **Discover Hosts Manually** button, and do the following to retry discovery using IPv4:

   - In the **Manual Host Discovery** window, click the **+Add Host** link. A line appears in the table below the link.
   - Enter the Controller VM IP address on that host (or the host IP address for compute-only nodes) and then click **Save**.
   - Add more hosts as desired.
   - When the list of hosts is complete, click the **Discover and Add Hosts** button. Manual discovery uses IPv4 to find and add the hosts to the list.

6. In the **Select Host** tab, select the check box for each node that you need to add to the cluster.
   Check the **Host Name**, **Controller VM [IPv4|IPv6]**, **Hypervisor [IPv4|IPv6]**, and **IPMI IP [IPv4|IPv6]** fields. Ensure that the details are displayed correctly. Resolve any discrepancies before you proceed.

7. In the **Choose Node Type** tab, select the node type as **HCI Node**.

8. In the **Host Networking** tab, click **Skip Host Networking**.

9. In the **Configure Host** tab, if the detected AHV and AOS version on the selected new nodes are the same as versions on the existing nodes in the cluster, no imaging is required and a message acknowledging that fact appears. Skip to the next step.
   Since the nodes were prepared with the correct AHV and AOS versions, this message is expected to be displayed, allowing you to skip to the next step.

10. When all the fields are correct, click the **Run Checks** button to verify that the nodes are ready.

    This runs a set of precheck tests on the nodes. Progress messages appear in the **Expand Cluster** window. You can also monitor progress from the **Tasks** dashboard. For more information, see View Task Status on page 89.

11. Click the **Expand Cluster** button to begin the cluster expansion process.

    After the first round of tasks is complete, a second round of tasks to add the nodes into the metadata ring automatically starts.

    Check whether the nodes are added to the metadata ring by logging on to any Controller VM in the cluster and running the following commands:

    ```
    nutanix@cvm$ nodetool -h 0 ring
    ```

    The output lists all the controller VMs in the cluster and displays their status as Up.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2066

12. Place all the new nodes in maintenance mode using aCLI. Do not use Prism Element web console.
    Log on to any Controller VM in the cluster, enter `acli>` mode and run the aCLI command as follows:

    ```
    acli> host.enter_maintenance_mode <host IP address>
    ```

    Replace `<host IP address>` with the Controller VM IP address of the new node.

    Run this command for each new node.

13. Update each virtual switch to include the new nodes.

    a. Update the uplinks of the virtual switches for the new nodes.
       For information on how to update the uplink configuration, see Creating or Updating a Virtual Switch on page 157.

    b. Retrieve the UUID of the new node.

       ```
       acli> host.list
       ```

       Note the UUID of the new host in the aCLI command output.

    c. Run the following command at the `acli>` prompt to configure the IP addresses for new nodes.

       ```
       acli> net.update_virtual_switch virtual-switch-name host_ip_addr_config='{<new-host-uuid1>:<new-host_ip_address/prefix>}'
       ```

       Replace

       - `<new-host-uuid1>` with the UUID of the new node noted in the previous step.
       - `<new-host_ip_address/prefix>` with the IP address with prefix for new node.

       To add the IP addresses of multiple new nodes to the host IP address configuration, use the following command format:

       ```
       acli> net.update_virtual_switch vs1 host_ip_addr_config='{<new-host-uuid1>:<host_ip_address1/prefix>;<new-host-uuid2>:<host_ip_address2/prefix>;<new-host-uuid3>:<host_ip_address3/prefix>}'
       ```

    d. If the IP address of the new node does not belong to the default VLAN and the new node generates VPC traffic, tag the VLAN of the new node to the bridge of the non-default virtual switch. Log on to the new host with `root` privileges and run the following command.

       ```
       root@ahv$ ovs-vsctl set port <brX> tag= <VLAN-ID>
       ```

       Replace `<brX>` with the non-default bridge such as br1 or br2.

       Replace `<VLAN-ID>` with the ID of the non-default VLAN that the new node IP address belongs to.

       For more information, see Assigning an AHV Host to a VLAN.

    For information on how to update the virtual switches, see Modifying Switch Information.

14. Reconfigure Flow Virtual Networking (Network Controller) on the new nodes.

    a. Ensure that the new node is placed to the maintenance mode (see previous step).

    b. Verify that the `Connected` status of the new node is True.
       Run the aCLI host.list command and check the `Connection` status of the new node in the table in the output.

       ```
       acli> host.list
       ```

       A sample output of this command is as follows:

       ```
       ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2067

```
Hypervisor IP   Hypervisor DNS Name  Host UUID                              Node
 state              Connected  Node type       Schedulable  Hypervisor Name  CVM
 IP
xx.xx.xx.1      xx.xx.xx.1           xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx1
 AcropolisNormal         True       Hyperconverged  True         AHV
 xx.xx.xx.11
xx.xx.xx.2      xx.xx.xx.2           xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx1
 AcropolisNormal         True       Hyperconverged  True         AHV
 xx.xx.xx.12
xx.xx.xx.3      xx.xx.xx.3           xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx1
 AcropolisNormal         True       Hyperconverged  True         AHV
 xx.xx.xx.13
xx.xx.xx.4      xx.xx.xx.4           xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx1
 EnteredMaintenanceMode  True       Hyperconverged  False        AHV
 xx.xx.xx.14
```

c. Log on to the new host with `root` privileges and run the following command.

```
root@ahv# systemctl stop ahv-host-agent
```

After a few minutes, verify that the `Connected` status of the new node is False using the aCLI host.list command.

d. Log on to the new host with `root` privileges and run the following command.

```
root@ahv# systemctl start ahv-host-agent
```

After a few minutes, verify that the `Connected` status of the new node is True using the aCLI host.list command.

Run this procedure on each new node.

15. Verify that no unresolved error exists.

a. Run NCC checks and resolve any errors.

b. In Prism Element web console of the cluster, click the **Settings** in the main menu and then select **Network Configuration** > **Virtual Switch**, and verify none of the virtual switches show a red warning icon.

If you see a red icon for any virtual switch, go to the **Alerts** page and check the alerts. The following alerts are not issued or are automatically resolved.

- Default Virtual Switch Error: This alert is not resolved automatically. Resolve it manually if you have verified that the virtual switch is healthy.
- Inconsistent Virtual Switch State Detected: This alert is resolved in the previous steps.
- Failed to configure host for Atlas networking: This alert is resolved in the previous steps.
- VPC east-west traffic configuration error: This alert is resolved in the previous steps.

Resolve all alerts. If you do not see any red icons for the virtual switches, go to the next step.

16. After the cluster health is validated as good, re-enable ADS using aCLI.

a. Get the ADS status.

```
nutanix@cvm$ acli
acli> ads.get
```

b. Enable ADS.

```
acli> ads.update enable=true
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2068

17. Remove the new nodes from maintenance mode using aCLI.

    Log on to any Controller VM in the cluster, enter `acli>` mode and run the aCLI command as follows:

    ```
    acli> host.exit_maintenance_mode <host IP address>
    ```

    Replace <host IP address> with the Controller VM IP address of the new node.

    Run this command for each new node.

What to do next

Run network connectivity validations for guest VMs in the cluster, using test VMs. Create a test VM with appropriate IP address in the guest VM network and run ping tests from the test VM to the default gateway of the guest VM network and the IP addresses of the other guest VMs in the network. You need one test VM per guest VM network for this test.

Node Maintenance

This section provides information about node maintenance in a Nutanix cluster.

Node Maintenance Mode

You are required to gracefully place a node into the maintenance mode or non-operational state for reasons such as making changes to the network configuration of a node, performing manual firmware upgrades or replacements, performing CVM maintenance or any other maintenance operations.

Entering and Exiting Maintenance Mode

You can only place one node at a time in maintenance mode for each cluster. When a host is in maintenance mode, the CVM is placed in maintenance mode as part of the node maintenance operation and any associated replication factor 1 enabled VMs are powered-off. The cluster marks the host as unschedulable so that no new VM instances are created on it. When a node is placed in the maintenance mode from the Prism Element web console, an attempt is made to evacuate VMs from the host. If the evacuation attempt fails, the host remains in the *entering maintenance mode* state, where it is marked unschedulable, waiting for user remediation.

When a host is placed in the maintenance mode, the non-migratable VMs (for example, pinned or replication factor 1 enabled VMs which have affinity towards a specific node) are powered-off while live migratable or high availability (HA) VMs are moved from the original host to other hosts in the cluster. After exiting the maintenance mode, all non-migratable guest VMs are powered on again and the live migrated VMs are automatically restored on the original host.

> **Note:** VMs with CPU passthrough or PCI passthrough, pinned VMs (with host affinity policies), and replication factor 1 enabled VMs are not migrated to other hosts in the cluster when a node undergoes maintenance. Click **View these VMs** link to view the list of VMs that cannot be live-migrated.

For information on how to place a node under maintenance, see Putting a Node into Maintenance Mode using Web Console on page 220.

You can also place an AHV host under maintenance mode or exit an AHV host from maintenance mode through the CLI.

> **Note:** Using the CLI method to place an AHV host under maintenance only places the hypervisor under maintenance mode. The CVM is up running in this method. To place the entire node under maintenance, Nutanix recommends using the UI method (through Prism Element web console or Prism Central).

- For information on how to use the CLI method to place an AHV host in maintenance mode, see Putting a Node into Maintenance Mode using CLI in the *AHV Administration Guide*.
- For information on how to use the CLI method to exit a node from the maintenance mode, see Exiting a Node from the Maintenance Mode using CLI in the *AHV Administration Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2069

Exiting a Node from Maintenance Mode

For information on how to remove a node from the maintenance mode, see Exiting a Node from the Maintenance Mode using Web Console on page 221.

Viewing a Node under Maintenance Mode

For information on how to view the node under maintenance mode, see Viewing a Node that is in Maintenance Mode on page 223.

UVM Status When Node under Maintenance Mode

For information on how to view the status of UVMs when a node is undergoing maintenance operations, see Guest VM Status when Node is in Maintenance Mode on page 223.

Best Practices and Recommendations

Nutanix strongly recommends using the **Enter Maintenance Mode** option on the Prism Element web console to place a node under maintenance.

Known Issues and Limitations

- With a minimum AOS release of 6.1.2, 6.5.1 or 6.6, you can only place one node at a time in maintenance mode for each cluster.
- Entering or exiting a node under maintenance from the CLI is not equivalent to entering or exiting the node under maintenance from the Prism Element web console. For example, placing a node under maintenance from the CLI places the AHV host and CVM under maintenance while the CVM continues to remain powered on.

  Warning: You must exit the node from maintenance mode using the same method that you have used to put the node into maintenance mode. For example, if you put the node into maintenance mode using CLI, you must use CLI to exit the node from maintenance mode. Similarly, if you put the node into maintenance mode using web console, you must use the web console to exit the node from maintenance mode.

  If you put the node in maintenance mode using CLI and attempt to exit it using web console or if you put the node in maintenance mode using web console and attempt to exit it using CLI, the maintenance workflow breaks, and activities such as node upgrade and coming up of the CVM service after exiting maintenance mode get impacted.

Putting a Node into Maintenance Mode using Web Console

Before you begin

Check the cluster status and resiliency before putting a node under maintenance. You can also verify the status of the UVMs. For more information, see Guest VM Status when Node is in Maintenance Mode on page 223.

About this task

As the node enter the maintenance mode, the following high-level tasks are performed internally.

- The AHV host initiates entering the maintenance mode.
- The HA VMs are live migrated.
- The pinned and replication factor 1 enabled VMs are powered-off.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2070

- The AHV host completes entering the maintenance mode.

  > **Note:** At this stage, the AHV host is not shut down. For information on how to shut down the AHV host, see Shutting Down a Node in a Cluster (AHV). You can list all the hosts in the cluster by running nutanix@cvm$ acli host.list command, and note the value of *Hypervisor IP* for the node you want to shut down.

- The CVM enters the maintenance mode.
- The CVM is shut down.

Perform the following steps to put the node into maintenance mode.

Procedure

1. Login to the Prism Element web console.
2. On the home page, select **Hardware** from the drop-down menu.
3. Go to the **Table** > **Host** view.
4. Select the node which you intend to put under maintenance.
5. Click the **Enter Maintenance Mode** option.
   The **Host Maintenance** window appears with a prompt to power-off all VMs that cannot be live migrated.

   > **Note:** VMs with CPU passthrough, PCI passthrough, pinned VMs (with host affinity policies), and replication factor 1 are not migrated to other hosts in the cluster when a node undergoes maintenance. Click **View these VMs** link to view the list of VMs that cannot be live-migrated.

6. Select the **Power-off VMs that can not migrate** checkbox to enable the **Enter Maintenance Mode** button.
7. Click the **Enter Maintenance Mode** button.

   - A revolving icon appears as a tool tip beside the selected node and also in the Host Details view. This indicates that the host is entering the maintenance mode.
   - The revolving icon disappears and the **Exit Maintenance Mode** option is enabled after the node completely enters the maintenance mode.
   - You can also monitor the progress of the node maintenance operation through the newly created Host enter maintenance and Enter maintenance mode tasks which appear in the task tray.

     > **Note:** In case of a node maintenance failure, certain rolled-back operations are performed. For example, the CVM is rebooted. But the live migrated are not restored to the original host.

What to do next

Once the maintenance activity is complete, you can perform any of the following.

- View the nodes under maintenance. For more information, see Viewing a Node that is in Maintenance Mode on page 223.
- View the status of the UVMs. For more information, see Guest VM Status when Node is in Maintenance Mode on page 223.
- Remove the node from the maintenance mode. For more information, see Exiting a Node from the Maintenance Mode using Web Console on page 221.

Exiting a Node from the Maintenance Mode using Web Console

After you perform any maintenance activity, exit the node from the maintenance mode.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2071

About this task

> **Warning:** You must exit the node from maintenance mode using the same method that you have used to put the node into maintenance mode. For example, if you put the node into maintenance mode using CLI, you must use CLI to exit the node from maintenance mode. Similarly, if you put the node into maintenance mode using web console, you must use the web console to exit the node from maintenance mode.
>
> If you put the node in maintenance mode using CLI and attempt to exit it using web console or if you put the node in maintenance mode using web console and attempt to exit it using CLI, the maintenance workflow breaks, and activities such as node upgrade and coming up of the CVM service after exiting maintenance mode get impacted.

As the node exits the maintenance mode, the following high-level tasks are performed internally.

- The CVM is powered on.
- The CVM is taken out of maintenance.
- The host is taken out of maintenance.

> **Note:** The AHV host is shut down during Putting a Node into Maintenance Mode using Web Console on page 220 and it is required to power on the AHV host. For information on how to power on the AHV host, see Starting a Node in a Cluster (AHV).

After the host exits the maintenance mode, the replication factor 1 enabled VMs continue to be powered on and the VMs migrate to restore host locality.

For more information, see Guest VM Status when Node is in Maintenance Mode on page 223 to view the status of the UVMs.

Perform the following steps to remove the node into maintenance mode.

Procedure

1. On the Prism Element web console home page, select **Hardware** from the drop-down menu.
2. Go to the **Table** > **Host** view.
3. Select the node which you intend to remove from the maintenance mode.
4. Click the **Exit Maintenance Mode** option.
   The **Host Maintenance** window appears.
5. Click the **Exit Maintenance Mode** button.
   - A revolving icon appears as a tool tip beside the selected node and also in the Host Details view. This indicates that the host is exiting the maintenance mode.
   - The revolving icon disappears and the **Enter Maintenance Mode** option is enabled after the node completely exits the maintenance mode.
   - You can also monitor the progress of the exit node maintenance operation through the newly created Host exit maintenance and Exit maintenance mode tasks which appear in the task tray.

What to do next

Once a node exits the maintenance mode, you can perform any of the following.

- View the status of node under maintenance. For more information, see Viewing a Node that is in Maintenance Mode on page 223.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2072

- View the status of the UVMs. For more information, see Guest VM Status when Node is in Maintenance Mode on page 223.

Viewing a Node that is in Maintenance Mode

About this task

> **Note:** This procedure is the same for AHV and ESXi nodes.

Perform the following steps to view a node under maintenance.

Procedure

1. Login to the Prism Element web console.
2. On the home page, select **Hardware** from the drop-down menu.
3. Go to the **Table** > **Host** view.
4. Observe the icon along with a tool tip that appears beside the node which is under maintenance. You can also view this icon in the host details view.
5. Alternatively, view the node under maintenance from the **Hardware** > **Diagram** view.

What to do next

You can:

- View the status of the guest VMs. For more information, see Guest VM Status when Node is in Maintenance Mode on page 223.
- Remove the node from the maintenance mode. For more information, see Exiting a Node from the Maintenance Mode using Web Console on page 221Exiting a Node from the Maintenance Mode (vSphere).

Guest VM Status when Node is in Maintenance Mode

The following scenarios demonstrate the behavior of three guest VM types - high availability (HA) VMs, pinned VMs, and replication factor 1 enabled VMs, when a node enters and exits a maintenance operation. The HA VMs are live VMs that can migrate across nodes if the host server goes down or reboots. The pinned VMs have the host affinity set to a specific node. The replication factor 1 enabled VMs have affinity towards a specific node or a Controller VM (CVM). To view the status of the guest VMs, go to **VM** > **Table**.

> **Note:** The following scenarios are the same for AHV and ESXi nodes.

Scenario 1: Guest VMs before Node Entering Maintenance Mode

All the guest VMs are powered-on and reside on the same host.

Scenario 2: Guest VMs during Node Maintenance Mode

As the node enter the maintenance mode, the following high-level tasks are performed internally.

1. The host initiates entering the maintenance mode.
2. The HA VMs are live migrated.
3. The pinned and replication factor 1 enabled VMs are powered-off.
4. The AHV host completes entering the maintenance mode.
5. The CVM enters the maintenance mode.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2073

6. The CVM is shut down.

Scenario 3: Guest VMs after Node Exiting Maintenance Mode

As the node exits the maintenance mode, the following high-level tasks are performed internally.

1. The CVM is powered on.
2. The CVM is taken out of maintenance.
3. The host is taken out of maintenance.

After the host exits the maintenance mode, the replication factor 1 enabled VMs continue to be powered on and the VMs migrate to restore host locality.

Repair Host Boot Disk and SSD Repair

Use the **Repair Host Boot Disk** function to perform graceful and non-graceful repair operations for the hypervisor and CVM when their boot disks stop working.

You can use the **Repair Host Boot Disk** functionality to repair the boot disk on CO, SO, and HCI nodes, only if the nodes are deployed with the following cluster setup:

- Optimized Database Solution:
  - AHV CO with AHV SO
  - ESXI CO with AHV SO

  For more information, see Optimized Database Solution.
- AHV SO with AHV or ESXi HCI
- AHV CO with AHV HCI
- ESXI CO with ESXI HCI

Use the **SSD Repair** function to perform the repair operations on the single SSD SO node platforms.

From Prism Element, you can perform the **Repair Host Boot Disk** and **SSD Repair** operations. For more information, see AOS ANY - Starting Host Boot Disk Repair (Proactive or Graceful Replacement) (nutanix.com) and AOS ANY - Repairing a Drive (Single SSD Platforms) (nutanix.com)

Limitations of Repair Host Boot Disk

The following limitations apply to the **Repair Host Boot Disk** function:

- The **Repair Host Boot Disk** function is not supported for the CO nodes hosted with Hyper-V
- The **Repair Host Boot Disk** function is not supported for the CO nodes hosted on non-NX platforms
- The **Repair Host Boot Disk** function is not supported for the HyperV HCI with AHV SO mixed hypervisor case
- The **Repair Host Boot Disk** function is not supported by the hypervisor for ungraceful host boot disk repairs when CO nodes are hosted on platforms with dual M.2 boot disks without a Redundant Array of Independent Disks (RAID) configuration.

Limitations of SSD Repair Function

The **SSD Repair** function is not supported for the HyperV HCI and AHV SO mixed hypervisor case.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2074

Starting Host Boot Disk Repair

This procedure describes how to proactively install a hypervisor on a boot device that has not completely failed (for example, a SATA DOM, or an M.2 device). A master node helps clone the boot device image onto the target node. This procedure works for all hypervisors. This procedure can clone and restore a complete image before the boot device fails. If this procedure fails, perform the *ungraceful* procedure for a boot device that has completely failed. For some platforms, a single procedure serves for both proactive and failed M.2 drives.

> **Caution:**
>
> Verify that it is safe to remove the node from the cluster before you start this procedure. You must follow the hypervisor boot drive replacement procedure for your specific platform. The documents are on the Nutanix support portal under Hardware Replacement Documentation in one of following categories.
>
> - For Hypervisor Boot Drive Replacement, see https://portal.nutanix.com/page/documents/list?type=hardware&filterKey=Component&filterVal=Hypervisor%20Boot%20Drive
> - For SATA DOM, see https://portal.nutanix.com/page/documents/list?type=hardware&filterKey=Component&filterVal=SATA%20DOM
> - For M.2, see https://portal.nutanix.com/page/documents/list?type=hardware&filterKey=Component&filterVal=M2
>
> Do not attempt to begin hypervisor boot drive repair without the appropriate document. For additional assistance, contact Nutanix support.

For information about replacing NVMe drives, see the NVMe replacement procedures for your platform.

Modifying a Cluster

Hardware components (nodes and disks) can be removed from a cluster or reconfigured in other ways when the conditions warrant it.

Before you begin

If the Data-at-Rest Encryption is enabled then before removing a drive or node from a cluster, test the certificates again by clicking **Test all nodes** and ensure that testing is successful and the status is **Verified**. For a detailed procedure, see Data-at-Rest Encryption in the *Security Guide*. In case of an SED drive or node, if the drive or node is not removed as recommended then the drive or node is locked.

About this task

To reconfigure one or more hardware components in a cluster, do the following:

Procedure

- Log on to the Prism Element web console.
- In the Hardware dashboard (see Hardware Dashboard on page 187), click the **Diagram** or **Table** tab.

  The following actions can be performed from either the **Diagram** or **Table** view.

Adding a Disk

You can add a disk to a node in Nutanix or non-Nutanix environments.

About this task

- The process of adding a disk is the same for all platforms (both Nutanix and third-party platforms), assuming that the platform is running Nutanix AOS.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2075

- The process of adding an NVME disk differs for each platform. For more information about adding an NVME disk, see Completing NVMe Drive Replacement (Software Serviceability).
- The types of disks you can add depends on your platform configuration. For supported disk configurations, see the System Specifications for your platform.
  - **Hybrid**: A mixture of SSDs and HDDs. Hybrid configurations fill all available disk slots, so you can add a disk only if there is a disk missing.
  - **All-flash**: All-flash nodes have both fully populated and partially populated configurations. You can add new drives to the empty slots. All-flash nodes can accept only SSDs.
  - **SSD with NVMe**: A mixture of SSDs and NVMe drives. Only certain drive slots can contain NVMe disks. Refer to the system specifications for your platform for disk configurations.
  - **HDD with NVMe**: A mixture of HDDs and NVMe drives. Only certain drive slots can contain NVMe disks. Refer to the system specifications for your platform for disk configurations.
  - **All NVMe**: All NVMe nodes have both fully populated and partially populated configurations. You can add new drives to the empty slots. All NVMe nodes can accept only NVMe drives.
- Nutanix allows mixing of disks with different capacities in the same node. However, the node treats higher-capacity disks as if they had the same capacity as the lower-capacity disks. Nutanix provides the ability to mix disk capacities for cases where you need to replace a disk, but only higher-capacity disks are available. To increase the overall storage capacity of the node, replace all disks with higher-capacity disks.
- When adding multiple disks to a node, allow at least one minute between adding each disk.

Procedure

1. Insert the disk in an empty slot of the node.
2. Log on to the web console, go to **Hardware** > **Diagram**, and select the added disk to view the details.

Figure 37: Adding a drive (multi-node block)

3. If the disk is red and shows a label of **Unmounted Disk**, select the disk and click **Repartition and Add** under the **Diagram** tab.

   This message and the button appear only if the replacement disk contains data. Their purpose is to protect you from unintentionally using a disk with data on it.

   Caution: This action removes all the data on the disk. Do not repartition the disk until you have confirmed that the disk contains no essential data.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2076

4. Go to **Hardware** > **Disk**, and verify that the disk has been added to the original storage pool.
   If the cluster has only one storage pool, the disk is automatically added to the storage pool.
5. If the cluster has multiple storage pools and the drive is not automatically added to the storage pool, add it to the desired storage pool:
   a. In the web console, select **Storage** from the drop down menu, select the **Table** tab, and then select the **Storage Pool** tab.
   b. Select the target storage pool and then click **Update**.
      The Update Storage Pool window appears.
   c. In the **Capacity** field, select the **Use unallocated capacity box** to add the available unallocated capacity to this storage pool then click **Save**.
   d. Go to **Hardware** > **Diagram**, select the drive, and confirm that it is in the correct storage pool.

Removing a Disk

You may need to remove a disk for various reasons such as during the replacement of a failed disk.

About this task

Removing a disk takes time because the data on that disk must be migrated to other disks before it is removed from a node. Monitor the progress on the disk removal through the dashboard messages.

To remove a disk, do the following.

Procedure

1. Log on to the Prism Element web console.
2. Select the disk you want to remove in one of the following ways:
   » Select the target disk in the diagram (**Diagram** view).
   » Click the **Disk** tab and select that disk in the table (**Table** view).
3. Click the **Remove Disk** link on the right of the **Summary** line.
   A dialog box appears to verify the action.
4. Click the **OK** button in the confirmation dialog box.

> **Caution:** Do not physically remove a disk until that disk status indicator turns red in the diagram. The status message that appears on completion of the steps may indicate that the data migration is complete, but the disk is not ready for removal until that the disk status indicator turns red in the diagram.

Removing a Node from a Cluster

You may need to remove a node for various reasons such as:

- Replacement of a failed node
- Node is either unreachable or powered off
- Deprecate old nodes for cluster expansion

You can remove a node using the Prism Element web console or nCLI.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2077

Prerequisites for Removing a Node

Consider the following before you remove a node:

- The Prism Element web console displays a warning message that you need to reclaim the license after you have removed the node. For information about reclaiming or rebalancing your cluster licenses, see License Manager Guide.
- Removing a node (host) takes some time because data on that node must be migrated to other nodes before it can be removed from the cluster. You can monitor progress through the dashboard messages. Removing a node implicitly removes all the disks in that node.
- (Hyper-V only) Initiating a removal of a node running Hyper-V fails if the node is running as a part of a Hyper-V failover cluster and the following message appears.

  ```
  Node node id is a part of a Hyper-V failover cluster failover cluster name. Please
   drain all the roles, remove the node from the failover cluster and then mark the
   node for removal.
  ```

  If this message is displayed in either nCLI or in web interface, as a cluster administrator, you must use the management tools provided by Microsoft such as *Failover Cluster Manager* to drain all the highly-available roles off the node. Then remove the node from the failover cluster followed by removing the node from the AOS cluster.
- (ESXi only) Before removing the node, ensure that there are no guest VMs running on the respective ESXi host. Note that CVM should be running on the node to initiate the node removal.
- (ESXi only) Ensure that the vSphere Distributed Switch (VDS) does not have any references to the host in the Port mirroring and VM templates. Ensure that there are no remaining VMs, VMkernels, or VM NICs associated with the VDS on the host you intend to remove.
- (ESXi only) Temporarily disable DRS on the cluster before the node removal. The DRS must be re-enabled after the node is removed. Update the HA configuration to exclude the node you want to remove.
- (ESXi only) As a cluster administrator, you must use the management tools provided by VMware to first migrate all the guest VMs off the node/host, then remove the node from the AOS cluster of ESXi hosts. After that disconnect and remove the node (host) from the vCenter server.

  Caution: Ensure that you migrate the guest VMs before removing a host or node. Verify that the target cluster has enough available compute capacity before actually migrating the VMs. Removing a node or host without first migrating the guest VMs may result in loss of service.

  1. Migrate the guest VMs that need to be migrated.
  2. Click **Remove Host** from Prism.
  3. After successful removal from the AOS cluster, put the host in maintenance mode.

     Caution: When you put the host in maintenance mode, the maintenance mode process powers down or migrates all the VMs that are running on the host.

     For more information, see Node Maintenance in *vSphere Administration Guide for Acropolis*.
  4. Remove the host from the vCenter server.

Removing a Single Node

About this task

Review the prerequisites for removing a node listed in Prerequisites for Removing a Node.

To remove a single node (host) from the cluster, do the following.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2078

Procedure

1. Log on to the Prism Element web console.
2. Select the node you want to remove in one of the following ways:
   - » In the **Diagram** page, select the target node (host).
   - » In the **Table** page, click the **Host** tab and select the node (host).
3. Click the **Remove Host** link on the right of the **Summary** line.

   > **Note:** The **Remove Host** link on the right of the **Summary** line does not appear for the removal of a host from a three-node cluster.

   A dialog box appears to verify the action.
4. Click the **OK** button in the confirmation dialog box.

   If the node that you are trying to remove is unreachable or powered off, a notification is triggered in the Prism UI alerting you that the storage utilization for this node could not be calculated and also suggesting the possible impact of removing this node. If you still want to go ahead, you can use the force option to forcefully mark this node for removal.

   > **Caution:** Do not shut down the CVM or put the CVM into maintenance mode while the node removal is in progress.

What to do next

- If you remove the last node with older generation hardware from a cluster and the remaining nodes have newer generation hardware, you may choose to power cycle the guest VMs to enable the VMs discover a new CPU set compatible with the newer generation hardware. For example, if you remove the last node with a G4 Haswell CPU from a cluster where all of the other nodes are newer G5 nodes with Broadwell CPUs, then VMs can discover a CPU set compatible with the newer G5 processors only when you trigger a power cycle. Note that a power cycle is not required for normal functionalities of the cluster, but the guest VMs continue to see the CPU set compatible with the older processors until you trigger a power cycle.
- After a node is removed, it goes into a state without any configuration. You can add such a node back into the cluster through the Expanding a Cluster on page 201 workflow.

  > **Caution:** After adding the removed node back into the cluster, the same cluster ID is applied to both clusters in the following circumstances:
  >
  > - When the removed node is the first node (lowest IP address in the cluster)
  > - When you reuse the removed node in another cluster
  > - When the removed node again becomes the first node (lowest IP address) in the new cluster
  >
  > To prevent this occurrence, reimage the node (using Foundation) before adding it to the new cluster.
  >
  > For information about how to image a node, see Prepare Bare-Metal Nodes for Imaging in the *Field Installation Guide*.

Remove Multiple Nodes

AOS allows you to remove multiple nodes from a cluster. The multinode removal process is sequential, that means you can request only one node at a time. However, you can mark other nodes for removal one after the other while data is being evicted in background from other nodes that are marked for removal.

Here is the multinode removal process overview:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2079

- User requests to remove multiple nodes (serially one after the other) from the Prism Element web console or nCLI.
- System runs prechecks on each node to allow node removal request. The node must pass all the checks to be successfully accepted for node removal.

  For more information, see Prechecks to Allow Multiple Node Removal on page 230.
- System removes nodes serially from metadata ring of Cassandra.
- System rebuilds the data in parallel in the background for all the nodes that are marked for removal.

Prechecks to Allow Multiple Node Removal

When you mark multiple nodes for removal, system runs the prechecks before accepting the node for removal. Below are some of the prechecks:

- The cluster upgrade process is not in progress.
- The minimum number of nodes required by Cassandra and Zookeeper are available and are in healthy (kNormal status) state.
- No other nodes are pending to be added to the cluster.
- The cluster continues to meet the maximum replication factor requirements after removal of the node.
- The cluster has enough usable storage capacity to rebuild the data from the removed node.

The system does not allow multinode removal if a node fails any of the prechecks.

Limitations for Multinode Removal

The following limitations are applicable for the multinode removal process:

- System allows a maximum of four nodes to be removed simultaneously from a cluster.
- For clusters with EC (erasure coding), the system computes the longest strip size possible on the cluster based on the EC param and desired fault tolerance of the container. The system does not allow multinode removal if there are not enough viable entities of the desired fault domain (node/ rack/ru) to accommodate the largest EC strip possible on this cluster.
- In the nCLI, the multinode removal is not allowed if you skip the space usage check.

  ```
  ncli> host rm-start skip-space-check=true
  ```

Removing Multiple Nodes

About this task

> **Note:** This feature is supported on a cluster with a minimum of four hosts (nodes).

Review the prerequisites for removing a node listed in the Prerequisites for Removing a Node on page 228 topic.

To remove multiple nodes from the cluster, do the following:

Procedure

1. Log on to the Prism Element web console.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2080

2. Select the node you want to remove by performing one of the following:

   » In the **Diagram** page, select the target node (host).

   » In the **Table** page, click the **Host** tab and select the node (host).

3. Click the **Remove Host** link on the right of the **Summary** line.

   > **Note:** The **Remove Host** link on the right of the **Summary** line does not appear for the removal of a host from a three-node cluster.

   A dialog box appears to verify the action.

4. Click **Remove** in the confirmation dialog box.

   You can monitor the node removal progress in the **Tasks** menu.

   > **Caution:** Do not shut down the CVM or put the CVM into maintenance mode while the node removal is in progress.

5. To remove multiple nodes, repeat Step 1 through Step 3 for each node.

   The Tasks menu shows the progress of the node removal. The first node that was selected to be removed has two subtasks running:

   - Transferring metadata to replacement replicas
   - Extent store replication

   The subsequent nodes have one subtask running in parallel.

   You can also monitor the data rebuild progress in the **Cluster Resiliency / Fault Tolerance Status** widget that appears in the Prism Element web console dashboard.

What to do next

- If you remove the last node with older generation hardware from a cluster and the remaining nodes have newer generation hardware, you may choose to power cycle the guest VMs to enable the VMs discover a new CPU set compatible with the newer generation hardware. For example, if you remove the last node with a G4 Haswell CPU from a cluster where all of the other nodes are newer G5 nodes with Broadwell CPUs, then VMs can discover a CPU set compatible with the newer G5 processors only when you trigger a power cycle. Note that a power cycle is not required for normal functionalities of the cluster, but the guest VMs continue to see the CPU set compatible with the older processors until you trigger a power cycle.
- After a node is removed, it goes into a state without any configuration. You can add such a node back into the cluster through the Expanding a Cluster on page 201 workflow.

  > **Caution:** After adding the removed node back into the cluster, the same cluster ID is applied to both clusters in the following circumstances:
  >
  > - When the removed node is the first node (lowest IP address in the cluster)
  > - When you reuse the removed node in another cluster
  > - When the removed node again becomes the first node (lowest IP address) in the new cluster
  >
  > To prevent this occurrence, reimage the node (using Foundation) before adding it to the new cluster.
  >
  > For information about how to image a node, see Prepare Bare-Metal Nodes for Imaging in the *Field Installation Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2081

Adding a Node

You can need to add a node or host into the metadata store in events such as the aftermath of the replacement of a failed metadata disk.

About this task

Each node includes a disk used for metadata storage, and AOS maintains a metadata store across these disks to ensure uninterrupted resiliency should a metadata disk fail. After such a failure, that node is taken out of the metadata store group and the cluster continues to operate seamlessly without it. Normally, the node is brought back into the metadata store automatically after the failed metadata disk is replaced. However, under certain (rare) circumstances this might not happen. If the node is ready but was not added back automatically, you need to add the node back into the metadata store manually.

When the node is not added back automatically, the following alert message is displayed:

Node ready to be added to metadata store

To add a host into the metadata store, do the following.

Procedure

1. Log on to the Prism Element web console.
2. Select the node you want to add in one of the following ways:
   - » Select the target node (host) in the diagram (**Diagram** view).
   - » Click the **Host** tab and select that disk in the table (**Table** view).
3. Click the **Enable Metadata Store** link on the right of the **Summary** line.
   The **Enable Metadata Store** link appears only when the node is not added back automatically and the alert message is displayed

Compute-Only and Storage-Only Nodes Management

This section provides information about the key features, deployment specifications, and deployment methods for compute-only and storage-only nodes in the HCI setup.

Compute-Only Nodes

The Nutanix cluster uses the resources (CPUs and memory) of a compute-only (CO) node exclusively for computing purposes. A CO node allows you to seamlessly and efficiently expand the computing capacity (CPU and memory) of your cluster. CO nodes do not have a Controller VM (CVM) and local storage.

Characteristics of Compute-Only Nodes

CO nodes enable you to achieve more control and value from restrictive licenses. There is no Controller VM (CVM) running on the CO node (VMs use CVMs running on the HCI nodes to access disks). When a CO node is part of a Nutanix Hyperconverged Infrastructure (HCI) cluster, then the licensed cores of the CO nodes are used only for the application VMs.

Applications or databases that are licensed on a per CPU core basis, require the entire node to be licensed, including the cores on which the CVM runs. With CO nodes, you get a much higher ROI on the purchase of your database licenses (such as Oracle and Microsoft SQL Server). Since there is no CVM running on a compute-only node and therefore, no consumption of compute resources for CVM.

CO nodes do not have local storage, and they support the following two types of nodes for storage operation:

- AHV SO (Optimized Database Solution) nodes. For more information, see Optimized Database Solution on page 245

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2082

- HCI nodes. For more information, see Deployment Specifications and Considerations for Compute-Only and Storage-Only Nodes on page 234

For information on how to deploy a CO node, see Deployment of Compute-Only Nodes on page 243.

Storage-Only Nodes

A storage-only node allows you to seamlessly expand the storage capacity in your cluster. A storage-only node always runs the AHV hypervisor. If you add a storage-only node to any cluster (regardless of the hypervisor), the hypervisor on the storage-only node is always AHV. Therefore, if you want to scale up only the storage capacity in your cluster, you do not need to purchase additional hypervisor licenses.

Foundation allocates the maximum resources to Controller VM (CVM) of the SO node as follows:

- CVM vCPU = Number of physical host CPUs minus 2, limited to a maximum of 22 vCPUs.

  Note: This is applicable till Foundation version 5.3.x. From Foundation version 5.4 onwards, the capping of maximum 22 vCPUs is not applicable.

- CVM memory = Available RAM minus 16 GiB, limited to a maximum of 256 GiB.

  Note:

  - This is applicable from Foundation version 5.3 and above. In the earlier Foundation versions, the memory allocation happens without capping to 256 GiB.
  - A capping of maximum 256 GiB is applied, and Foundation allocates the maximum possible vRAM to CVM. For example, if the available RAM is 512 GiB, the system allocates a maximum of 256 GiB and never considers the 512-16 = 496 GiB value. However, if you change the system allocated vRAM, the vRAM gets overridden with the supplied value.

Note: Minimum Foundation version of 5.3 supports these limits with NUMA pinnings or alignments. Earlier Foundation versions with a minimum version of 5.0 support these limits but not NUMA pinnings or alignments.

Characteristics of Storage-Only Nodes

The following characteristics apply to the storage-only nodes:

- A storage-only node includes an AHV hypervisor, a Controller VM (CVM), and memory and CPU resources enough to run only the CVM.
- A storage-only node always runs the AHV hypervisor. Therefore, if you add a storage-only node to an ESXi or Hyper-V cluster, the hypervisor on the storage-only node is always AHV.
- For hardware model support for storage-only node, see Supported Hardware Platforms on page 237.
- A storage-only node is supported on ESXi, Hyper-V, and AHV clusters. However, you cannot run guest VMs on the storage-only nodes.
- If you have storage-only AHV nodes in clusters with compute-only nodes being ESXI or Hyper-V, deployment of default virtual switch vs0 fails. In such cases, the Prism Element, Prism Central or CLI workflows for virtual switch management are unavailable to manage the bridges and bonds. Use the manage_ovs command options to manage the bridges and bonds.

Note: A storage-only node is not the same as a storage-heavy node. A storage-heavy node is a regular Nutanix hyperconverged node, but with a greater storage capacity. A storage-heavy node can run any hypervisor (AHV, ESXi, or Hyper-V) and can run guest VMs.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2083

AHV SO nodes do not perform the compute operation, and they support the following two types of nodes for compute operation:

- AHV or ESXi CO nodes (Optimized Database Solution)
- AHV or ESXi HCI nodes

For more information, see Supported Deployment Configurations on page 234.

For information on how to deploy a storage-only node, see Deployment of Storage-only Nodes on page 245.

Deployment Specifications and Considerations for Compute-Only and Storage-Only Nodes

This section provides information about specifications, requirements, and best practices for compute-only nodes and storage-only nodes deployment in the Hyperconverged Infrastructure (HCI) setup.

Supported Deployment Configurations

This section provides information about the supported deployment configurations with compute-only (CO) nodes and storage-only (SO) nodes.

AHV Compute-only node with AHV HCI Nodes

You can deploy AHV CO nodes that use AHV hyperconverged (HCI) nodes for storage in a cluster.

AHV Storage-only node with AHV or ESXi HCI Nodes

You can deploy AHV SO nodes for storage in the cluster with AHV hyperconverged (HCI) nodes.

Optimized Database Solution

The CO and SO nodes can also be deployed in an optimized database solution setup. For more information, see Optimized Database Solution on page 245.

Operation Specifications

This section provides information about the operational attributes for the supported deployment configurations of compute-only (CO) and storage-only (SO) nodes in the Hyperconverged Infrastructure (HCI) setup.

Table 47: Operation Mechanism - Supported Deployment Configurations

Component / Operation Type	Deployment Configuration	
	AHV CO with AHV HCI	AHV SO with AHV or ESXi HCI
Storage source for vDisk/Volumes associated with guest VMs on the compute-only (CO) node	HCI nodes in the cluster	SO nodes in the cluster
Controller VM (CVM) and local storage	No CVM and local storage on CO nodes	No CVM and local storage on HCI nodes
VMs Management (CRUD operations, ADS, and HA)	Using Prism Element web console	
Hypervisor operation for CO node	Runs on the local storage media of the CO node	Runs on the local storage media of the HCI node
Network segmentation support	Not supported	

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2084

Component / Operation Type	Deployment Configuration	
	AHV CO with AHV HCI	AHV SO with AHV or ESXi HCI
Hypervisor and firmware upgrade	Using Life Cycle Manager (LCM). For more information, see the *LCM Updates* topic in the Life Cycle Manager Guide.	

Cluster Requirements

This section provides information about the minimum cluster requirements for compute-only (CO) and storage-only (SO) nodes in the Hyperconverged Infrastructure (HCI) setup.

Table 48: Minimum Cluster Requirements for Compute-Only Nodes and Storage-Only Nodes

Cluster Attributes	AHV CO with AHV HCI	AHV SO with AHV or ESXi HCI
AOS Version	AOS 5.11 or later for HCI nodes	AOS 5.11 or later for SO nodes
AHV Version	Compatible AHV version based on AOS release.	Compatible AHV version based on AOS release.
Number of nodes	Minimum 3 HCI nodes and minimum 2 CO nodes	Minimum 3 SO nodes and minimum 2 HCI nodes
Nodes Ratio	Nutanix recommends the following nodes ratio: 2 CO : 1 HCI, if CVM is allocated with 16 logical cores.	Nutanix recommends the following nodes ratio: 1 HCI : 2 SO
Storage node Specification	All the HCI nodes in the cluster must be All-flash nodes.	All the SO nodes in the cluster must be All-flash nodes.
CPU and memory assignment	The number of vCPUs assigned to Controller VMs on the HCI nodes must be greater than or equal to the total number of available cores on all the AHV CO nodes in the cluster. The Controller VM requires a minimum of 12 vCPUs. For more information about how Foundation allocates memory and vCPUs to your platform model, see Controller VM (CVM) Field Specifications in the *Acropolis Advanced Administration Guide*.	The number of vCPUs assigned to Controller VMs on the SO nodes must be greater than or equal to the total number of available cores on all the AHV HCI nodes in the cluster. The Controller VM requires a minimum of 12 vCPUs. For more information about how Foundation allocates memory and vCPUs to your platform model, see Controller VM (CVM) Field Specifications in the *Acropolis Advanced Administration Guide*.
Network Speed	Use dual 25 GbE on AHV CO nodes and quad 25 GbE on AHV HCI nodes.	Use dual 25 GbE on AHV HCI nodes and quad 25 GbE on AHV SO nodes.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2085

Cluster Attributes	AHV CO with AHV HCI	AHV SO with AHV or ESXi HCI
Hypervisor specification	• For HCI node: AHV only • For CO node: AHV AHV CO node must run the same AHV version as the AHV HCI nodes in the cluster. When you add an AHV CO node to the cluster, AOS checks if the AHV version of the node matches with the AHV version of the existing AHV nodes in the cluster. If there is a mismatch, the node addition fails. For general requirements about adding a node to a Nutanix cluster, see Expanding a Cluster.	• For HCI node: AHV or ESXi • For SO node: AHV AHV HCI node must run the same AHV version as the AHV SO nodes in the cluster. When you add an AHV HCI node to the cluster, AOS checks if the AHV version of the node matches with the AHV version of the existing AHV nodes in the cluster. If there is a mismatch, the node addition fails. For general requirements about adding a node to a Nutanix cluster, see Expanding a Cluster.
NIC Bandwidth	Total amount of NIC bandwidth allocated to all the HCI nodes must be twice the amount of the total NIC bandwidth allocated to all the CO nodes in the cluster.	Total amount of NIC bandwidth allocated to all the SO nodes must be twice the amount of the total NIC bandwidth allocated to all the HCI nodes in the cluster.
CPU Memory	See Controller VM (CVM) Specifications in the *Acropolis Advanced Administration Guide.*	
Drives	See HCI Node Field Requirements in the *Acropolis Advanced Administration Guide.*	
Socket	For CO node: Single or Dual socket For HCI node: Dual socket except ROBO setup	For SO node:Single socket For HCI node: Dual socket except ROBO setup
Host interface	For CO node: iSCSI (boot and data drives) For HCI node: iSCSI	For SO node: • iSCSI, if mixed with AHV HCI • NFS, if mixed with ESXi HCI For HCI node: • NFS for ESXi HCI node • iSCSI for AHV HCI node

Licensing Requirements

This section provides information about the licensing requirements that apply to compute-only (CO) and storage-only (SO) nodes deployment at your site in the Hyperconverged Infrastructure (HCI) setup.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2086

Table 49: Licensing Requirements

Deployment Configuration	Licensing
AHV CO with AHV HCI AHV SO with AHV or ESXi HCI	Uses NCI licenses on a per-core basis. For more information about NCI licences, see NCI section in Nutanix Cloud Platform Software Options.

Configuration and Operation Limits

This section provides information about the configuration and operation limits that apply to compute-only and storage-only nodes deployment in the Hyperconverged Infrastructure (HCI) setup.

Table 50: Configuration and Operation Limits - CO and SO Nodes Deployment

Cluster Attributes	Deployment Configuration	
	AHV CO with AHV HCI	**AHV SO with AHV or ESXi HCI**
Number of VMs	See Nutanix Configuration Maximums	
Number of Nodes	Up to 32	
Addition of HCI Node	Supported	
Rolling Restart	Supported	
RDMA	Not supported	
Host boot disk replacement for CO nodes	Not supported	
Virtual Switch configuration	Supported	
Network segmentation for disaster recovery	Not supported	
Automatic discovery of CO nodes as part of *Expand cluster* workflow (see Expanding a Cluster)	Not supported Initiate the manual host discovery workflow to add compute-only node when you use the Expanding a Cluster workflow.	Not supported Initiate the manual host discovery workflow to add HCI node when you use the Expanding a Cluster workflow.
Cluster Conversion	Not supported	

Supported Hardware Platforms

This section provides information about the supported hardware platforms for compute-only (CO) and storage-only (SO) nodes deployment at your site in the Hyperconverged Infrastructure (HCI) setup.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2087

Table 51: Supported Hardware Platforms

Deployment Configuration	Supported Hardware Platforms
AHV CO with AHV HCI	• For HCI node: Any NX G8 or G9 model or Dell XC750/ XC650 • For CO node: NX8170-G8, NX1175S-G8, NX-8170-G9, NX-1175S-G9, NX-8155-G9, NX-8150-G9, NX-9151-G9, and Dell XC750/ XC650
AHV SO with AHV or ESXi HCI	• For HCI node: Any NX and OEM model • For SO node: Any NX and OEM model For more information on qualified models, see Hardware Platforms Spec Sheets. **Note:** The NX-8155A-G9 can only be included if all other nodes in the cluster are also hosted on NX-8155A-G9 platform.

Networking Configuration for Compute Nodes

This section provides information about how to perform the networking configurations for compute nodes based on the deployment configuration at your site in the Hyperconverged Infrastructure (HCI) setup.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2088

Table 52: Networking Configurations for Compute-Only Nodes

Deployment Configuration	Method to perform networking configurations
AHV CO with AHV HCI AHV SO with AHV HCI	Use the manage_ovs commands and add the `--host` flag to the `manage_ovs` commands. **Note:** If the deployment of default virtual switch vs0 fails, the Prism Element, Prism Central or CLI workflows for virtual switch management are unavailable to manage the bridges and bonds. Use the `manage_ovs` command options to manage the bridges and bonds. For example, to create or modify the bridges or uplink bonds or uplink load balancing, run the following command: `nutanix@cvm$ manage_ovs --host IP_address_of_compute_node --bridge_name bridge_name create_single_bridge` Replace: • *`IP_address_of_compute_node`* with the IP address of the CO node in AHV CO with AHV HCI deployment configuration or IP address of the HCI node in AHV SO with AHV HCI deployment configuration. • *`bridge_name`* with the name of bridge you want to create. **Note:** Run the `manage_ovs` commands for an AHV CO node from any Controller VM running on an AHV HCI node. Perform the networking tasks for each AHV CO node in the cluster separately. For more information about networking configuration of the AHV hosts, see Host Network Management.
AHV SO with ESXi HCI	Perform the networking tasks for each ESXi HCI node in the cluster individually. For more information on vSphere network configuration, see vSphere Networking in the *vSphere Administration Guide for Acropolis*.

Best Practices for Storage-Only Nodes

Consider the following best practice recommendations if you plan to include storage-only nodes in your cluster.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2089

- Nutanix recommends that your cluster has sufficient capacity to handle any storage-only node failure.

  Nutanix recommends also that your cluster has sufficient capacity to handle the rolling-upgrade operations performed on storage-only nodes during which the nodes need to be restarted.

  > **Important:**
  >
  > To achieve optimal cluster resiliency, deploy storage-only nodes in a replication factor plus one configuration. For example, if the replication factor of your cluster is two, deploy at least three storage-only nodes. If the replication factor of your cluster is three, deploy at least four storage-only nodes.
  >
  > The replication factor configuration is especially important if you plan to configure your storage-only nodes with higher storage capacity than the regular hyper-converged nodes.
  >
  > For example, in a cluster of four HCI nodes, each with 4 TB capacity (total 16 TB), you are adding high capacity storage-only nodes of 30 TB capacity, add replication factor plus one number of nodes.

  Since the fault tolerance value is applicable to the cluster as a whole, this value determines the usage until fault tolerance is reached and the cluster can still rebuild the data.

  For example, you have configured Resiliency Factor 3 with four storage heavy nodes (say, node_1, node_2, node_3, and node_4). Assume that the capacities of the remaining smaller nodes do not add up to same amount of storage as the capacity of a single storage heavy node. In such a case, to accommodate the failure of two storage heavy nodes AOS needs to be able to place all of their data on the remaining two storage heavy nodes in a node fault tolerant system. If extent group egroup_1 resides on node_1, node_2, and node_3 then, in an event of failure of node_1 and node_2, egroup_1 may be placed on node_4 or one of the smaller nodes that has enough space. Therefore, consider the Fault Tolerance capacity that you get based on the static configuration and ensure that the usage is maintained below Fault Tolerance value. This ensures that data can be rebuilt in a fault tolerant manner even in the event of Fault Tolerance number of simultaneous failures.

  The following table provides details of the number of storage-only nodes for cluster fault tolerance with replication factor and fault tolerance settings.

Configured Cluster Fault Tolerance	Resulting Cassandra/ Zookeeper replication factor	Recommended Compute Cluster Settings	Configured Replication Factor (for containers with user data)	Permitted Storage-only Nodes (Replication Factor + 1 minimum number of nodes to add)	Possible Fault Tolerance Level for different components(for the node failure domain)
1N/1D	3	N+1	2	3	1 - when a cluster is healthy (can tolerate single node failure) 0 - when a cluster is not healthy (cannot tolerate node failure)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2090

Configured Cluster Fault Tolerance	Resulting Cassandra/ Zookeeper replication factor	Recommended Compute Cluster Settings	Configured Replication Factor (for containers with user data)	Permitted Storage-only Nodes (Replication Factor + 1 minimum number of nodes to add)	Possible Fault Tolerance Level for different components(for the node failure domain)
2N/2D	5	N+2	2	3	2 - when a cluster is healthy (can tolerate a simultaneous failure of two nodes) 1 - when a cluster is not healthy (still can tolerate single node failure) 0 - when a cluster is not healthy (cannot tolerate node failure)
			3	4	2 - when a cluster is healthy (can tolerate a simultaneous failure of two nodes) 1 - when a cluster is not healthy (still can tolerate single node failure) 0 - when a cluster is not healthy (cannot tolerate node failure)

- **Recommended Compute Cluster Settings** refers to the number of compute (HCI or CO) nodes in the cluster for a given Fault Tolerance. **Permitted Storage-only Nodes** refers to the number of SO nodes required for the given number of Compute nodes. For example, for the minimum fault tolerance level of 1 in the first row of the table above, the **Recommended Compute Cluster Settings** number is N+1, and the **Permitted Storage-only Nodes** number is 3.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2091

- Nutanix recommends that the SSD capacity of the node is at least 10% of the HDD capacity of the node. For example, if your cluster has 20 TB HDD capacity, the SSD capacity of the node is at least 2 TB.

  This recommendation does not apply to all-flash clusters.
- Nutanix recommends that you configure all CVMs in the cluster with the same resources.
- Nutanix recommends that a cluster with all storage-only nodes, has at least 3 nodes.

  Nutanix recommends that you deploy a minimum 3 SO nodes to ensure a healthy and active cluster and 2 CO nodes to maintain high availability in case of upgrade or any other maintenance activities on the CO node

The following table shows the supported and unsupported configurations for a cluster with storage-only nodes.

Configuration	Supported	Description
A four-node cluster with 4 TB capacity on each node. `One large capacity storage-only node of 30 TB capacity.`	X	If the only storage-only node in the cluster fails, the cluster does not have the sufficient capacity of 30 TB. **Resolution**: Add the minimum number of storage-only nodes equal to the replication factor of your cluster.
A four-node cluster with 4 TB capacity on each node. `One large capacity storage-only node of 14 TB capacity.`	X	Four nodes of 4 TB = 16 TB capacity, that is 8 TB for each replication copy. If the 14 TB storage node fails, the remaining four nodes cannot accommodate 14 TB of replication data because 14 TB is greater than the 8 TB needed for second replication copy. **Resolution**: The number of storage-only nodes that you add must be equal to the replication factor of the cluster.
A four-node cluster with 4 TB capacity on each node. Two large capacity storage-only nodes of 30 TB capacity each.	#	If one storage-only node fails, the other can handle the required capacity.
A four-node cluster with 4 TB capacity on each node. One same-capacity storage-only node as the rest of the cluster.	#	The cluster is able to handle the failure of any node in the cluster, because all nodes in the cluster are of the same capacity.
Nutanix cluster with 2 TB SSD capacity and 20 TB HDD capacity.	#	The total SSD capacity is minimum 10% of the total HDD capacity.
Nutanix cluster with 2 TB SSD capacity and 40 TB HDD capacity.	X	The total SSD capacity is not minimum 10% of the total HDD capacity.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2092

Configuration	Supported	Description

= Supported configuration

X = Unsupported configuration

Deployment of Compute-Only Nodes

This section provides information about how to deploy the compute-only (CO) nodes in a AHV cluster.

The CO node can be deployed in the following ways:

New Node as CO Node

To add a new node as a CO node to the cluster, you must:

- Image the node as CO by using Foundation. For more information on how to image a node as a CO node, see the Field Installation Guide.
- Add that node to the cluster by using the Prism Element web console. For more information, see Adding an AHV Compute-Only Node to an AHV Cluster on page 244 and Adding an ESXi Compute-Only Node to an AHV Cluster on page 251.

Existing HCI Node as CO Node

To add an existing HCI node, that is already a part of the cluster, as a CO node to the cluster, you must:

- Remove that node from the cluster. For more information about how to remove a node, see Modifying a Cluster on page 225.
- Image that node as CO by using Foundation.
- Add that node back to the cluster. For more information, see Adding an AHV Compute-Only Node to an AHV Cluster on page 244 and Adding an ESXi Compute-Only Node to an AHV Cluster on page 251.

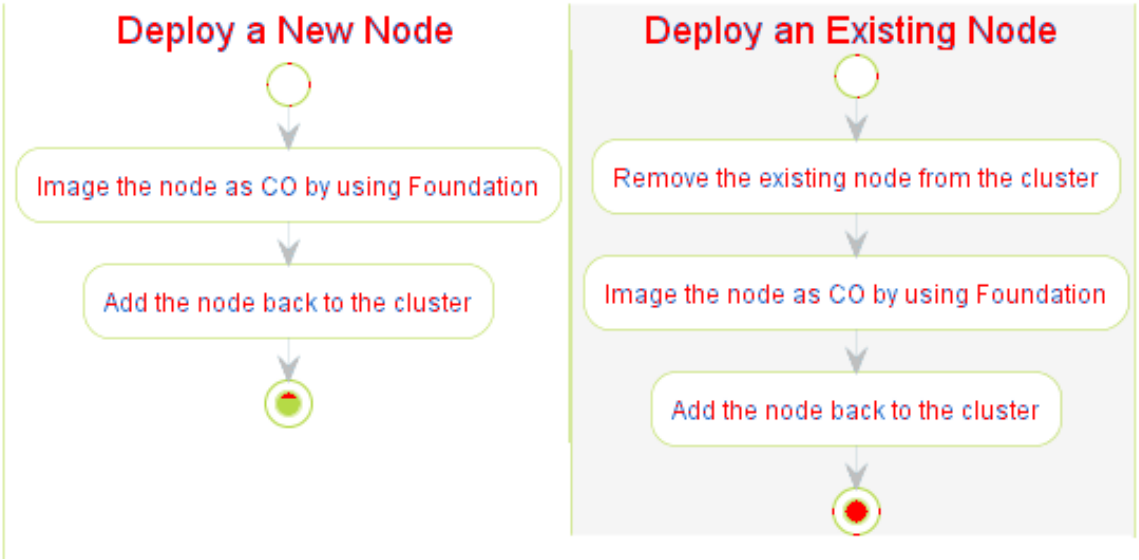


Figure 38:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2093

Adding an AHV Compute-Only Node to an AHV Cluster

About this task

Perform the following procedure to add a compute-only (CO) node to an AHV cluster.

Before you begin

Ensure that you check the Deployment Specifications and Considerations for Compute-Only and Storage-Only Nodes on page 234 before you add a compute-only node to an AHV cluster:

Procedure

To add a CO node to an AHV cluster, perform the following steps:

1. Log on to the Prism Element web console.
2. Do one of the following:
   - » Click the gear icon in the main menu and select **Expand Cluster** on the **Settings** page.
   - » Go to the hardware dashboard and click **Expand Cluster**.

   The system displays the **Expand Cluster** window:
3. Select **Expand Cluster** to expand the cluster with CO node.

   > **Note:** To expand a cluster with CO node, do not select **Prepare Now and Expand Later.** This option is used to only prepare the nodes and expand the cluster at a later point in time. For CO nodes, node preparation is not supported.
   >
   > The system displays the error Compute only nodes cannot be prepared in the **Configure Host** tab, if you proceed with **Prepare Now and Expand Later** option:

4. In the **Select Host** tab, scroll down and, under **Manual Host Discovery**, click **Discover Hosts Manually**.
5. Click **Add Host**.
6. Under **Host or CVM IP**, type the IP address of the AHV host and click **Save**.

   > **Note:** The CO node does not have a Controller VM and you must therefore provide the IP address of the AHV host.

7. Click **Discover and Add Hosts**.
   Prism Element discovers the CO node and the CO node appears in the list of nodes in the **Select Host** tab.
8. Select a CO node to view the node details, and click **Next**.
   The system displays the **Choose Node Type** tab.
9. Click **Next** in the **Choose Node Type** tab.
   The system prompts you to skip host networking.
10. Click **Skip Host Networking**.
    The system prompts you to run checks and expand the cluster with the selected CO node.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2094

11. Click either of the following options in the **Configure Host** tab:

    - **Run Checks** - Used to only run pre-checks required for cluster expansion. Once all pre-checks are successful, you can click the **Expand Cluster** to add the CO node to the cluster.
    - **Expand Cluster** - Used to run both; pre-checks required for cluster expansion and expand cluster operation together.

    The add-node process begins, and Prism Element performs a set of checks before the node is added to the cluster. Once all checks are completed and the node is added successfully, the system displays the completion states for the tasks as 100%.

    Note:

    - You can check the progress of the operation in the **Tasks** menu of the Prism Element web console. The operation takes approximately five to seven minutes to complete.
    - If you have not disabled the virtual switch as specified in Prerequisites, the system displays the multiple errors during cluster expansion.

    Check the progress of the operation in the **Tasks** menu of the Prism Element web console. The operation takes approximately five to seven minutes to complete.

12. Check the **Hardware Diagram** view to verify if the CO node is added to the cluster.

    You can identity a node as a CO node if the Prism Element web console displays **N/A** in the **CVM IP** field.

Deployment of Storage-only Nodes

You can image storage-only nodes when you are creating a cluster by using Foundation. You can also expand your existing cluster to add a storage-only node.

- For more information about imaging storage-only nodes when creating a cluster, see the Field Installation Guide.
- For instructions on adding storage-only nodes to an existing cluster, see Expanding a Cluster on page 201.

Optimized Database Solution

This section provides information about how to deploy the compute-only (CO) nodes and storage-only (SO) nodes in an optimized database solution setup

The optimized database solution provides a compartmentalized infrastructure for running databases. The compartmentalization separates the database instances and their storage, enables predictable performance, independent scalability, and isolated manageability for the database instances and their storage. It also provides dedicated resources within the Nutanix Cloud Infrastructure (NCI) cluster.

The optimized database solution uses the CO nodes and SO nodes features of NCI and Nutanix Database Service (NDB) in the following way:

- CO nodes are hosted with AHV or ESXi and no CVM
- SO nodes are hosted with AHV and CVM

In an optimized database solution cluster, the database instances are deployed on the guest VMs that are scheduled only on the CO nodes and not on the SO nodes. A different set of SO nodes serves the storage for the database instances in the cluster. NDB automates the provisioning of the storage on the SO nodes and maps them to the database instances on the CO nodes.

To preserve compartmentalization, the optimized database solution implements a fencing mechanism that prevents the guest VMs (including the guest VMs that host the database instances in the cluster) from being scheduled (automatically or manually) on SO nodes at any time. This fencing mechanism disables all the SO nodes in the cluster

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2095

to host any guest VM at the time of the cluster creation. So, the Database instances can run only on CO nodes and never on SO nodes.

The database software licensing on CO nodes and SO nodes is based on the end user licensing agreement of the database software vendor.

The optimized database solution can be deployed in the following two methods based on the hypervisor used on the CO nodes:

- AHV CO node with AHV SO node.
- ESXi CO node with AHV SO node.

> **Note:** Starting with AOS 6.8, ESXi CO nodes support ESXi 8.0 and later versions.

> **Note:** Nutanix does not support the following deployments:
>
> - A combination of AHV CO and ESXi CO nodes within a cluster.
> - ESXi SO nodes, or a combination of ESXi CO nodes and AHV HCI nodes.

An ESXi compute-only (CO) node allows you to seamlessly and efficiently expand the computing capacity (CPU and memory) of your AHV cluster. The Nutanix cluster uses the resources (CPUs and memory) of an ESXi CO node exclusively for computing purposes.

You can use a supported server or re-image an existing hyperconverged (HCI) node as an ESXi CO node.

To use a node as CO, image the node as CO by using Foundation and then add that node to the cluster by using the Prism Element web console. For more information on how to image a node as a CO node, see the Field Installation Guide.

> **Note:** If you want an existing HCI node that is already a part of the cluster to work as a CO node, remove that node from the cluster, image that node as a CO node by using Foundation, and add that node back to the cluster. For more information on how to remove a node, see Modifying a Cluster.

Operation Specifications for Optimized Database Solution

This section describes the operation specifications of compute-only (CO) and storage-only (SO) nodes in the optimized database solution setup.

Table 53: Operation Specifications - Optimized Database Solution

Component / Operation Type	Optimized Database Solution	
	AHV CO with AHV SO	ESXi CO with AHV SO
Storage source for vDisk/Volumes associated with guest VMs on the compute-only (CO) node	SO nodes in the cluster	
Controller VM (CVM) and local storage	No CVM and local storage on CO nodes	
VMs Management (CRUD operations, ADS, and HA) for CO node	Using Prism Element web console	
Hypervisor operation for CO node	Runs on the local storage media of the CO node	

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2096

Component / Operation Type	Optimized Database Solution	
	AHV CO with AHV SO	ESXi CO with AHV SO
Network segmentation support for CO node	Only for Controller VM backplane network and volume networks.	
Hypervisor and firmware upgrade for CO node	Using Life Cycle Manager (LCM). For more information, see the *LCM Updates* topic in the Life Cycle Manager Guide.	

Cluster Requirements for Optimized Database Solution

his section provides information about the minimum cluster requirements for compute-only (CO) and storage-only (SO) nodes in optimized database solution setup.

Table 54: Minimum Cluster Requirements for Compute-Only Nodes and Storage-Only Nodes in Optimized Database Solution

Cluster Attributes	Optimized Database Solution	
	AHV CO with AHV SO	ESXi CO with AHV SO
AOS Version for SO nodes	AOS 6.7 or later	AOS 6.6.2 or later
AHV Version for SO nodes	20230302.204 or later	Compatible AHV version based on AOS release
Number of nodes	Minimum 3 SO Nodes and minimum 2 CO nodes	
Nodes Ratio	Nutanix recommends the following nodes ratio: • Even nodes - 1 CO : 1 SO • Odd Nodes - Recommended difference between CO and SO nodes is 1. However, you can deploy different combination of CO and SO nodes, provided the combinations comply with minimum 5 nodes and maximum 32 nodes in a cluster and meet your workload requirements. **Note:** Use minimum 3 SO nodes to ensure a healthy and active cluster and minimum 2 CO nodes to maintain high availability in case of upgrade or any other maintenance activities on the CO node	
Storage node Specification	All the SO nodes in the cluster must be NVMe nodes.	
CPU and memory assignment	No balancing required for the vCPU assignment between the CO and SO nodes as all the CPUs and memory are allocated to the SO node.	No balancing required for the vCPU assignment between the CO and SO nodes as all the CPUs and memory are allocated to the SO node.
Network Speed	Use dual 25 GbE or above on CO and AHV SO nodes.	Use dual 25 GbE or above on CO and AHV SO nodes.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2097

Cluster Attributes	Optimized Database Solution	
	AHV CO with AHV SO	**ESXi CO with AHV SO**
Hypervisor specification	• For SO node: AHV only • For CO node: AHV AHV CO node must run the same AHV version as the AHV SO nodes in the cluster. When you add an AHV CO node to the cluster, AOS checks if the AHV version of the node matches with the AHV version of the existing AHV nodes in the cluster. If there is a mismatch, the node addition fails. For general requirements about adding a node to a Nutanix cluster, see Expanding a Cluster.	• For SO node: AHV only • For CO node: ESXi ESXi version of the ESXi compute-only nodes must be the same across the cluster. Nutanix supports the minimum ESXi version of 7.0 for ESXi CO node deployments in a Nutanix SO node cluster. When you add an ESXi CO node to the cluster, AOS checks if the ESXi version of the node matches with the ESXi version of the existing CO nodes in the cluster. If there is a mismatch, the node addition fails. For general requirements about adding a node to a Nutanix cluster, see Expanding a Cluster.
NIC Bandwidth	Uniform NIC bandwidth between CO and SO nodes.Uniform NIC bandwidth between CO and SO nodes.	
CPU	For SO node: • Minimum 24 cores (12 cores per socket) • Minimum 2.5 GHz clock speed **Note:** • 1: 1 mapping between Cores and vCPU for CVM • CVM picks all the cores minus 2 given to the SO node For CO node: • Single socket: Minimum 8 cores per node/socket • Dual socket: Minimum16 cores per node (8 cores per socket) • Minimum 2.5 GHz clock speed **Note:** See the NDB Control Plane Configuration and Scalability section of *Nutanix Database Service Administration Guide* to review the additional CPUs that may be used by NDB Agent VMs running on the Compute Only Nodes.	
Memory	For SO node: Minimum 128 GB For CO node: Based on customer requirements	

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2098

Cluster Attributes	Optimized Database Solution	
	AHV CO with AHV SO	ESXi CO with AHV SO
Drives	For SO node: Minimum 8 drives, minimum 3.84 TB each Drives (NVMe only) For CO node: Minimum 2 SSD or NVMe drives, with minimum 1.92 TB each **Note:** There is a factory limitation of shipping with minimum 2 drives.	
Socket	For SO node: Dual socket For CO node: Single or dual socket	
Host interface	For SO node: iSCSI For CO node: iSCSI (boot and data drives)	For SO node: NFS, iSCSI For CO node: NFS (boot drive), iSCSI (data drives)

Licensing Requirements for Optimized Database Solution

This section provides information about the licensing requirements that apply to compute-only (CO) and storage-only (SO) nodes deployment in optimized database solution setup.

Table 55: Licensing Requirements for Optimized Database Solution

Deployment Configuration		Licensing
Optimized Database Solution	AHV CO with AHV SO ESXi CO with AHV SO	Uses a combination of NCI Ultimate or NCI Pro licenses for AHV storage-only nodes and NDB Platform licenses for AHV compute-only nodes. Both NCI and NDB platforms are licensed on a per-core basis. NCI Ultimate on storage-only AHV nodes is the preferred licensing model to get the most functional Optimized DB Solution. When you use the NCI Pro license on the storage-only AHV nodes, the entire cluster functions at the Pro level feature set, and the NDB disaster recovery feature and other advanced functionalities are not available. For more information about NCI Ultimate and NDB feature set licenses, see https://www.nutanix.com/products/cloud-platform/software-options. **Note:** The database instances can run only on CO nodes and not on SO nodes. The database software licensing on CO nodes and SO nodes is based on the end user licensing agreement of the database software vendor.

Configuration and Operation Limits for Optimized Database Solution

This section provides information about the configuration and operation limits that apply to compute-only and storage-only nodes deployment in optimized database solution setup.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2099

Table 56: Configuration Limits - CO and SO Nodes Deployment

Cluster Attributes	Optimized Database Solution	
	AHV CO with AHV SO	ESXi CO with AHV SO
Number of VMs	Up to 500	Up to 500
Number of Nodes	Up to 32	Up to 32
Addition of HCI Node	Not supported	Not supported
Rolling Restart	Supported	Supported
RDMA	Not supported	Not supported
Host boot disk replacement for CO nodes	Not supported	Not supported
Virtual Switch configuration	Supported	Supported
Network segmentation for disaster recovery	Supported on SO node	Not supported
Automatic discovery of CO nodes as part of *Expand cluster* workflow (see Expanding a Cluster)	Not supported Initiate the manual host discovery workflow to add compute-only node when you use the Expanding a Cluster workflow.	Not supported Initiate the manual host discovery workflow to add compute-only node when you use the Expanding a Cluster workflow.
Cluster Conversion	Not supported	Not supported

Supported Hardware Platforms for Optimized Database Solution

This section provides information about the supported hardware platforms for compute-only (CO) and storage-only (SO) nodes deployment in optimized database solution setup.

Table 57: Supported Hardware Platforms - Optimized Database Solution

Optimized Database Solution	Supported Hardware Platforms
AHV CO with AHV SO ESXi CO with AHV SO	• For SO node: NX8170-G8, NX-8170-G9, NX-8155-G9, NX-8150-G9, Dell XC650-10N, Dell XC750-16N, Dell XC660-12N, and Dell XC760-24N • For CO node: NX8170-G8, NX1175S-G8, NX-8170-G9, NX-1175S-G9, NX-8155-G9, NX-8150-G9, NX-9151-G9, Dell XC650-10N, Dell XC750-16N, Dell XC660-12N, and Dell XC760-24N **Note:** In case of any queries regarding the supported hardware models, contact Nutanix Support.

Networking Configurations for Compute-Only Nodes in Optimized Database Solution

This section provides information about how to perform the networking configurations for compute-only nodes based on the deployment configuration in optimized database solution setup.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2100

Table 58: Networking Configurations for Compute-Only Nodes in Optimized Database Solution

Optimized Database Solution	Method to perform networking configurations
AHV CO with AHV SO	Use the manage_ovs commands and add the `--host` flag to the `manage_ovs` commands. **Note:** If the deployment of default virtual switch vs0 fails for AHV CO node with AHV SO node, the Prism Element, Prism Central or CLI workflows for virtual switch management are unavailable to manage the bridges and bonds. Use the `manage_ovs` command options to manage the bridges and bonds. For example, to create or modify the bridges or uplink bonds or uplink load balancing, run the following command: `nutanix@cvm$ manage_ovs --host IP_address_of_co_node --bridge_name bridge_name create_single_bridge` Replace `IP_address_of_co_node` with the IP address of the CO node and `bridge_name` with the name of bridge you want to create. **Note:** Run the `manage_ovs` commands for an AHV CO node from any Controller VM running on an AHV SO node. Perform the networking tasks for each AHV CO node in the cluster separately. For more information about networking configuration of the AHV hosts, see Host Network Management.
ESXi CO with AHV SO	Perform the networking tasks for each ESXi CO node in the cluster individually. For more information on vSphere network configuration, see vSphere Networking in the *vSphere Administration Guide for Acropolis*.

Deployment of Compute-Only and Storage-Only nodes in Optimized Database Solution

This section describes how to deploy the compute-only nodes and storage-only nodes in the optimized database solution setup.

For information on how to deploy AHV compute-only node in optimized database solution, see Adding an AHV Compute-Only Node to an AHV Cluster on page 244.

For information on how to deploy ESXi compute-only node in optimized database solution, see Adding an ESXi Compute-Only Node to an AHV Cluster on page 251.

For information on how to deploy storage-only nodes in optimized database solution, see Deployment of Storage-only Nodes on page 245.

Adding an ESXi Compute-Only Node to an AHV Cluster

About this task

Perform the following procedure to add an ESXi compute-only node to a Nutanix cluster.

Before you begin

Check the Deployment Specifications and Considerations for Compute-Only and Storage-Only Nodes on page 234.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2101

Procedure

1. Log on to the Prism Element web console.
2. Do one of the following:
   - » Click the gear icon in the main menu and select **Expand Cluster** in the **Settings** page.
   - » Go to the hardware dashboard and click **Expand Cluster**.
3. In the **Select Host** screen, scroll down and, under **Manual Host Discovery**, click **Discover Hosts Manually**.
4. Click **Add Host**.
5. Under **Host or CVM IP**, type the IP address of the ESXi CO node and click **Save**.
   This node does not have a Controller VM and you must therefore provide the IP address of the ESXI CO node.
6. Click **Discover and Add Hosts**.
   Prism Element discovers this node and the node appears in the list of nodes in the **Select Host** screen.
7. Select the node to display the details of the compute-only node.
8. Click **Next**.
9. In the **Configure Host** screen, click **Expand Cluster**.
   The add node process begins and Prism Element performs a set of checks before the node is added to the cluster.
   Check the progress of the operation in the **Tasks** menu of the Prism Element web console. The operation takes approximately five to seven minutes to complete.
10. Check the **Hardware Diagram** view to verify if the node is added to the cluster.
    You can identity a node as a CO node if the Prism Element web console does not display the IP address for the Controller VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2102

NUTANIX VOLUMES

Nutanix Volumes acts as one or more targets for client Windows or Linux operating systems running on a bare metal server or as guest VMs using iSCSI initiators. You can use any storage available in any new or existing Nutanix cluster for Volumes.

For more information, see the Nutanix Volumes Guide. For best practice information, Nutanix provides the Nutanix Volumes Solutions Documentation.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2103

FILE SERVER MANAGEMENT

Nutanix Files (Files) lets you share files across user work stations in a centralized and protected location to eliminate the requirement for a third-party file server. The **File Server** dashboard displays dynamically updated information about the file servers and shares/exports in a cluster. To view the **File Server** dashboard, select **File Server** from the pull-down list on the left of the main menu. For more information, see the Nutanix Files Guide.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2104

DATA PROTECTION

Nutanix offers data protection solutions for virtual datacenters. Nutanix provides data protection functions at the VM, file, and volume group level, so VMs and data remain safe in a crash-consistent environment.

> **Note:** For more information about the data protection solutions available from Nutanix, see Nutanix DR Solutions Workflow in the *Data Protection and Recovery with Prism Element* Guide.

- Nutanix supports several types of protection strategies including one-to-one or one-to-many replication. For more information, see Protection Strategies in the *Data Protection and Recovery with Prism Element* Guide.
- You can configure asynchronous disaster recovery. For more information, see Data Protection with Asynchronous Replication (One-hour or Greater RPO) in the *Data Protection and Recovery with Prism Element* Guide.
  - The Cloud Connect feature gives you the option to asynchronously back up data on the Amazon Web Service (AWS) cloud. For more information, see Asynchronous Replication With Cloud Connect (On-Premises To Cloud) in the *Data Protection and Recovery with Prism Element* Guide.
- You can also configure synchronous disaster recovery. There are two options:
  - For environments that support metro availability, you can configure a metro availability protection domain. For more information, see Metro Availability (ESXi and Hyper-V 2016) in the *Data Protection and Recovery with Prism Element* Guide.
  - For other environments, you can configure synchronous replication. For more information, see Synchronous Replication (ESXi and Hyper-V 2012) in the *Data Protection and Recovery with Prism Element* Guide.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2105

HEALTH MONITORING

Nutanix provides a range of status checks to monitor the health of a cluster.

- Summary health status information for VMs, hosts, and disks appears on the home dashboard. For more information, see Home Dashboard on page 63.
- In depth health status information for VMs, hosts, and disks is available through the Health dashboard. For more information, see Health Dashboard on page 256.
- You can customize the frequency of the scheduled health checks and how frequently to run them. For more information, see Configuring Health Checks on page 259.
- You can run NCC health checks directly from the Prism. For more information, see Running Checks by Using Prism Element Web Console on page 261.
- You can collect logs for all the nodes and components. For more information, see Collecting Logs by Using Prism Element Web Console on page 261.
- For a description of each available health check. For more information, see Alerts/Health checks.

> **Note:** If the Cluster Health service status is DOWN for more than 15 minutes, an alert email is sent by the AOS cluster to configured addresses and Nutanix support (if selected). In this case, no alert is generated in the Prism Element web console. The email is sent once per 24 hours. You can run the NCC check cluster_services_down_check to see the service status.

Health Dashboard

The Health dashboard displays dynamically updated health information about VMs, hosts, and disks in the cluster. To view the Health dashboard, select **Health** from the pull-down list on the left of the main menu.

Menu Options

The Health dashboard does not include menu options other than those available from the main menu.

> **Note:** When you first visit the Health dashboard, a tutorial opens that takes you through a guided tour of the health analysis features. Read the message and then click the **Next** button in the text box to continue the tutorial (or click the **X** in the upper right to close the text box and end the tutorial.) You can view this tutorial at any time by selecting the **Health Tutorial** option in the user menu. For more information, see Main Menu on page 58.

Screen Details

The Health dashboard is divided into three columns:

- The left column displays tabs for each entity type (VMs, hosts, disks, storage pools, storage containers, cluster services, and [when configured] protection domains and remote sites). Each tab displays the entity total for the cluster (such as the total number of disks) and the number in each health state. Clicking a tab expands the displayed information (see following section).
- The middle column displays more detailed information about whatever is selected in the left column.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2106

- The right column displays summary of all the health checks. You also have an option to view individual checks from the **Checks** button (success, warning, failure, or disabled).
  - The **Summary** tab provides summarized view of all the health checks according to check status and check type.
  - The **Checks** tab provides information about individual checks. Hovering the cursor over an entry displays more information about that health check. You can filter the checks by clicking appropriate field type and clicking **Apply**. The checks are categorized as follows.

    Filter by Status

    Passed, Failed, Warning, Error, Off, or All

    Filter by Type

    Scheduled, Not Scheduled, Event Triggered, or All

    Filter by Entity Type

    VM, Host, Disk, Storage Pool, Storage Container, Cluster Service, or All

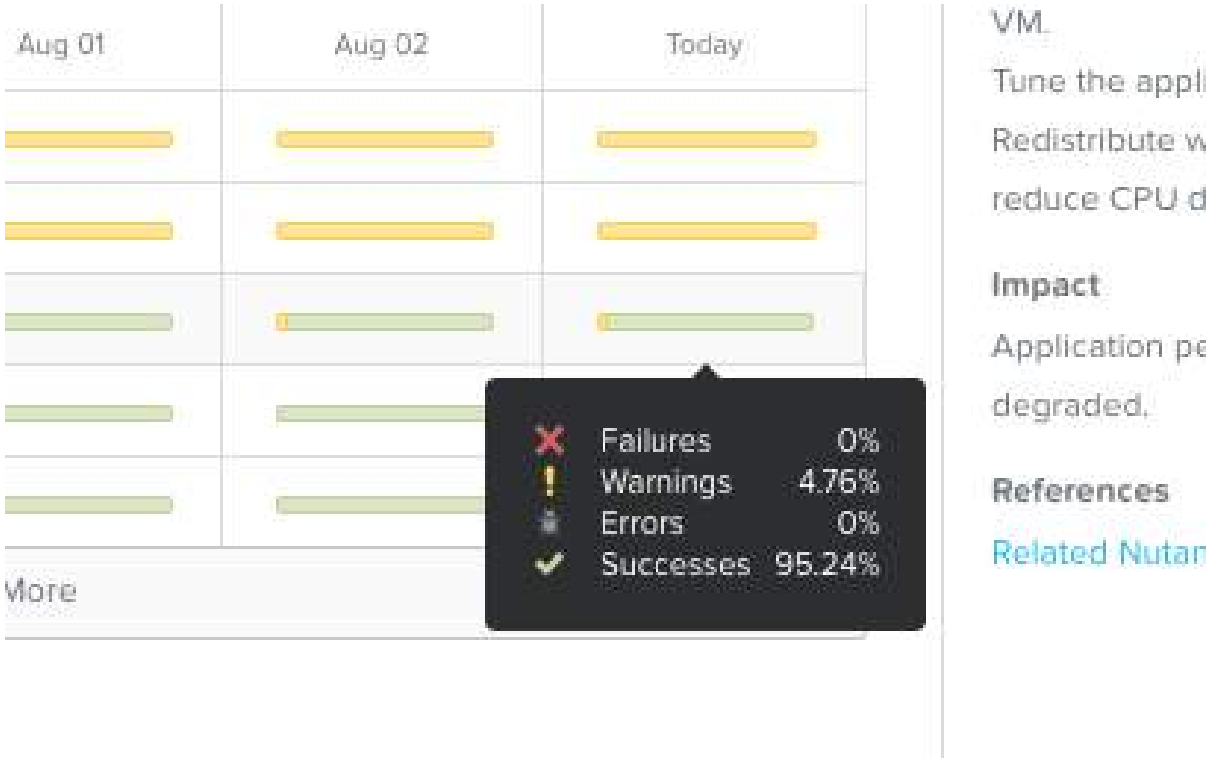


Figure 39: Hover Information

For example, if you want to see only the failed checks, filter the checks by selecting the **Failed** option. If you click on the specific check, the middle column will provide the detailed history of when the checks failed and what is the percentage of the check failure. If you click the bar, a detailed graph of the pass and fail history is

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2107

displayed (as shown below). Hovering the mouse along the graph line displays information about that point in time.

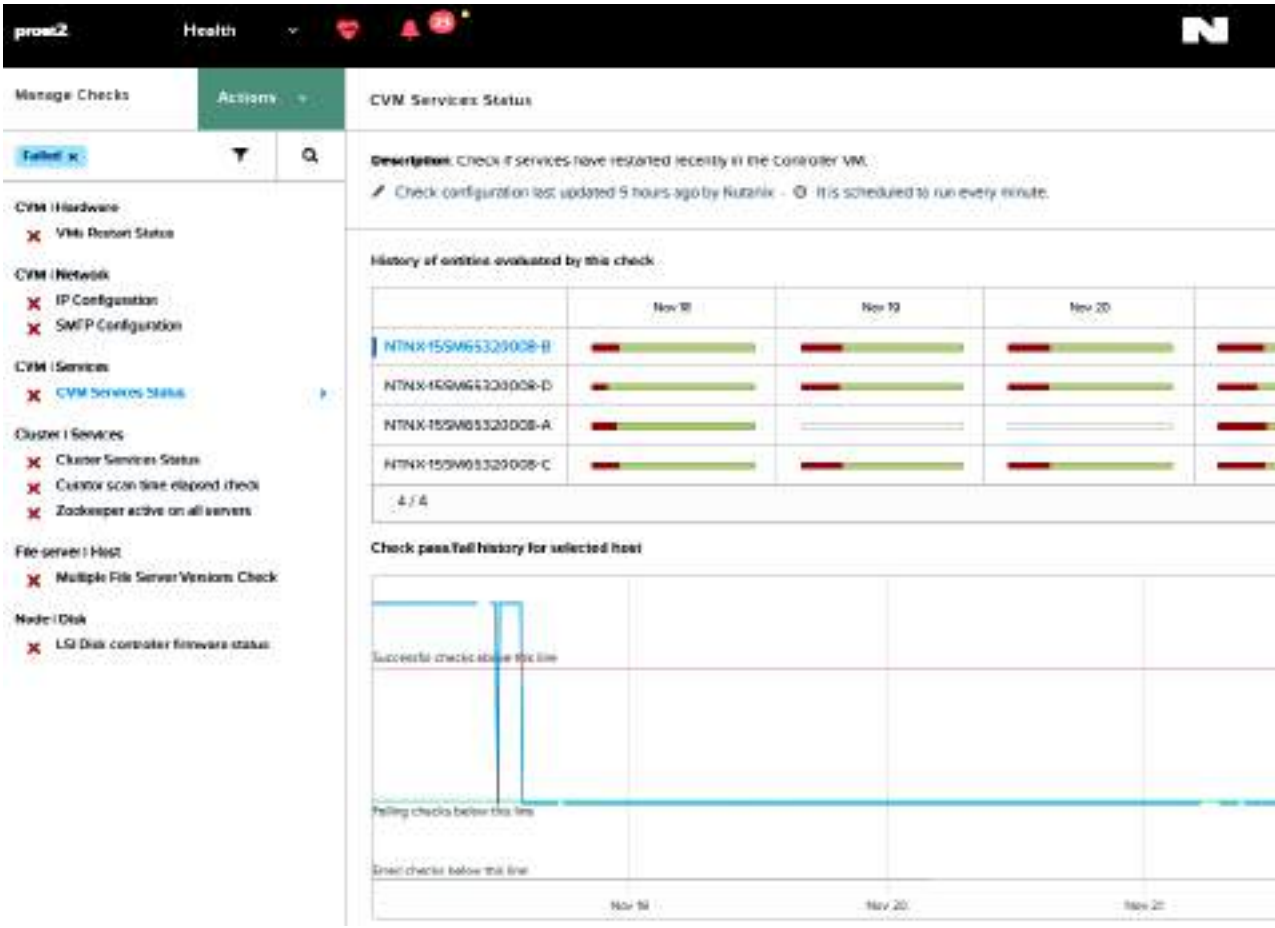


Figure 40: Filter Categorization

> **Note:** For the checks with status as error, follow the similar process as described above to get detailed information about the errors.

You can also search for specific checks by clicking the health search icon and then entering a string in the search box.

- The **Actions** tab provides you with an option to manage checks, run checks, and collect logs.

Focus and Filtering Options

The Health dashboard allows you to display entity health information through various views. Clicking a left column tab expands that tab to display grouping categories for that entity type (VMs, hosts, or disks). The middle section also expands with additional detail. The **Checks** tab of the right column displays the health checks that are relevant for that entity type.

Clicking on a grouping category displays detailed information about that grouping:

- The left column expands to display a set of grouping and filter options. The selected grouping is highlighted. You can select a different grouping by clicking on that grouping. Each grouping entry lists how many categories are in that grouping, and the middle section displays information about those categories. In the following example, the disks storage tier is selected, and there are two categories (SSD and HDD) in that grouping. By default, all entities

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2108

(in this example, all disks) are included in the category information. You can narrow the included list by clicking one or more of the filters.

- The middle column displays a field for each category in the selected grouping. Each field provides details about that category. You can see additional information by hovering the cursor over a specific entry. There is a drop-down select list for filtering (same as the grouping filters) and a drop-down sort by list for ordering the information.
- The right column continues to display the health checks that are relevant for that entity type.

The middle column provides two viewing options: a diagram view and a table view. The table view provides more detailed information in tabular form. You can sort the entries by clicking a column header.

The middle column also includes watch list information at the top (*Currently watching `xx` entities* or *Currently watching `x` / `xx` total `entity_type`*). The Health dashboard is dynamically adjusted to reflect information about the entities in the current watch list. In this example, all disks are currently selected for the watch list (*Currently watching 18 / 18 total disks*), so the status information (middle column) and relevant health checks (right column) reflect the 18 disks. When you change the watch list to a subset of the current entity type (such as a single disk) or a different entity type (such as hosts), the status information and relevant health checks are customized accordingly for the new watch list.

Configuring Health Checks

A set of health checks are run regularly that provide a range of clusters health indicators. You can specify which checks to run and configure the schedulable checks and other parameters for each health check.

About this task

The cluster health checks cover a range of entities including AOS, hypervisor, and hardware components. A set of checks are enabled by default, but you can run, disable, or reconfigure any of the checks at any time. To reconfigure one or more health checks, do the following:

Procedure

1. Log on to the Prism Element web console.
2. In the Health dashboard, click **Actions** > **Manage Checks** .
   The Health dashboard redisplays with information about the health checks. If you clicked on a specific health check, that check is highlighted. Either you are prompted to select a health check (first time) or the previously selected health check is highlighted.
3. Select a check.
   a. The left column lists the health checks with the selected check highlighted. Click any of the entries to select and highlight that health check.
   b. The middle column describes what this health check does, and it provides the run schedule and history across affected entities (hosts, disks, or VMs).
   c. The right column describes what failing this health check means (cause, resolution, and impact).
4. To run a particular check, click **Run Check**.
5. To turn off (or turn on) a health check, click the **Turn Check Off** (or **Turn Check On**) link at the top of the middle column and then click the **Yes** button in the dialog box.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2109

6. To change the alert policy for those health checks that have a configurable policy, click Alert Policy at the top of the middle column, change one or more of the parameter values in the drop-down window, and then click **Save**.

   a. Depending on the alert condition (**Info**, **Critical**, and so on), unselect the condition to disable these alert condition messages.

      All the alerts are enabled by default (box checked). In most cases this field includes just a single box with the word Critical, Warning, or Info indicating the severity level. Checking the box means this event will trigger an alert of that severity. Unchecking the box means an alert will not be issued when the event occurs. In some cases, such as in the example figure about disk space usage, the event can trigger two alerts, a warning alert when one threshold is reached (in this example 90%) and a critical alert when a second threshold is reached (95%). In these cases you can specify whether the alert should be triggered (check/uncheck the box) and at what threshold (enter a percentage in the box).

   b. **Auto Resolve These Alerts**: Uncheck (or check) the box to disable (or re-enable) automatic alert resolution.

      Automatic alert resolution is enabled for all alert types (where applicable) by default. When this is enabled, the system will automatically resolve alerts under certain conditions such as when the system recognizes that the error has been resolved or when the initiating event has not reoccurred for 48 hours. (Automatic resolution is not allowed for some alert types, and this is noted in the policy window for those types.)

7. To change a parameter setting for those health checks that have configurable parameters, click the **Parameters** link at the top of the middle column, change one or more of the parameter values in the drop-down window, and then click the **Update** button.

   This link appears only when the health check includes configurable parameters. The configurable parameters are specific to that health check. For example, the *CPU Utilization* health check includes parameters to specify the host average CPU utilization threshold percentage and host peak CPU utilization threshold percentage.

8. To change the schedule for running a health check, select an interval from the **Schedule** drop-down list for the schedulable checks at the top of the middle column.

   Each check has a default interval, which varies from as short as once a minute to as long as once a day depending on the health check. The default intervals are optimal in most cases, and changing the interval is not recommended (unless requested to do so by Nutanix customer support).

Configuring NCC Frequency

Perform the following procedure to configure NCC to run automatically after the specified period of time from Prism.

Procedure

1. Log on to the Prism Element web console.
2. In the Health dashboard, from the **Actions** drop-down menu select **Set NCC Frequency**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2110

3. Select the configuration schedule.

   » **Every 4 hours**: Select this option to run the NCC checks at four hours interval.

   » **Every Day**: Select this option to run the NCC checks on a daily basis.

   Select the time of the day when you want to run the checks from **Start Time** field.

   » **Every Week**: Select this option to run the NCC checks on a weekly basis.

   Select the day and time of the week when you want to run the checks from the **On** and **Start Time** fields. For example, if you select Sunday and Monday from the **On** field and select 3:00 p.m. from the **Start Time** field, every Sunday and Monday at 3 p.m. the NCC checks are run automatically.

   The Email address that you have configured by using alert emails is also displayed. A report will be sent as an email to all the recipients. For more information on how to configure alert emails, see Configuring Alert Emails in *Prism Element Alerts and Events Reference Guide*.

4. Click **Save**.

Running Checks by Using Prism Element Web Console

You can now run the NCC checks from the **Health** dashboard of the Prism Element web console. You can select to run all the checks at once, the checks that have failed or displayed some warning, or even specific checks of your choice.

About this task

> **Note:** If you are running checks by using Prism Element web console, you will not be able to collect the logs at the same time.

Procedure

1. In the Health dashboard, from the **Actions** drop-down menu select **Run NCC Checks**.
2. Select the checks that you want to run for the cluster.

   a. **All checks**: Select this option to run all the checks at once.

   b. **Only Failed and Warning Checks**: Select this option to run only the checks that were failed or gave warning during the health check runs.

   c. **Specific Checks**: Select this option and type the check or checks name in the text box that appears that you want to run.

   This field gets auto-populated once you start typing the name of the check. All the checks that you have selected for this run are listed in the **Added Checks** box.

3. Select the **Send the cluster check report in the email** option to receive the report after the cluster check.

   To receive the email configuration ensure that you have configured email configuration for alerts. For more information, see Configuring Alert Emails in *Prism Element Alerts and Events Reference Guide*.

   The status of the run (succeeded or aborted) is available in the **Tasks** dashboard. By default, all the event triggered checks are passed. Also, the **Summary** page of the **Health** dashboard will be updated with the status according to health check runs.

Collecting Logs by Using Prism Element Web Console

You can collect logs for Controller VMs, file server, hardware, alerts, hypervisor, and for the system. After the task finishes, the log bundle is available for download purpose from the **Tasks** dashboard.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2111

About this task

Log bundle includes logs and configuration information from one or more Controller VMs, configuration information for hypervisors, and information about alerts and so on. To collect the logs and download the log bundle, perform the following procedure.

> **Note:**
>
> - While this method works, the preferred method for collecting logs is through a CLI tool called logbay. For more information about logbay, see the Nutanix Cluster Check (NCC) Guide.
> - The timestamps for all Nutanix service logs are moved to UTC (in ISO 8601:2020-01-01 T00:00:00Z) from Prism version 5.18.
> - All operating system logs will not be moved to UTC, hence Nutanix recommends that you set the server local time to UTC.

Procedure

1. Log on to the Prism Element web console.
2. In the **Health** dashboard, from the **Actions** drop-down menu, select **Collect Logs**.
3. In **Node Selection**, click **+ Select Nodes**. Select the nodes for which you want to collect the logs and click **Done**.
4. Click **Next**.
5. In **Log Settings**, select one of the following:
   - » **All**. Select this option if you want to collect the logs for all the tags.
   - » **Specific (by tags)**. Select this option, click **+ Select Tags** if you want to collect the logs only for the selected tags and then click **Done**.
6. In **Output Preferences**, do the following in the indicated fields.
   - 1. **Select Duration**. Select the duration for which you want to collect the logs. You can collect the logs either in hours or days. Click the drop-down list to select the required option.
     2. **Cluster Date**. Select the date from which you want to start the log collection operation. Click the drop-down list to select either **Before** or **After** to collect logs before or after a selected date.
     3. **Cluster Time**. Select the time from when you want to start the log collection operation.
     4. **Select Destination for the collected logs**. Click the drop-down list to select the server where you want the logs to be collected.
        - **Download Locally**
        - **Nutanix Support FTP**. If you select this option, enter the case number in the **Case Number** field.
        - **Nutanix Support SFTP**. If you select this option, enter the case number in the **Case Number** field.
        - **Custom Server**. Enter server name, port, username, password, and archive path if you select this option.
     5. **Anonymize Output**. Select this checkbox if you want to mask all the sensitive information like the IP addresses.
7. To start the operation, click **Collect**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2112

8. After the operation completes, you can download the log bundle for the last two runs and (as needed) add it to a support case as follows:

   a. Go to the **Task** dashboard, find the log bundle task entry, and click the **Succeeded** link for that task (in the Status column) to download the log bundle. For more information, see View Task Status on page 89.

      > **Note:** If a pop-up blocker in your browser stops the download, turn off the pop-up blocker and try again.

   b. Log in the support portal, click on the target case in the **360 View** widget on the dashboard (or click the **Create a New Case** button to create a new case), and upload the log bundle to the case (click the **Choose Files** button in the **Attach Files** section to select the file to upload).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2113

VIRTUAL MACHINE MANAGEMENT

Each node in a cluster includes local storage (flash and hard disk), a Controller VM, a hypervisor, and any number of host VMs running on that hypervisor.

- The web console allows you to monitor status of the VMs across the cluster. For more information, see VM Dashboard on page 264.
- In Acropolis managed clusters, the web console also allows you to do the following:
  - Create VMs. For more information, see Creating a VM (AHV) on page 274.
  - Manage VMs. For more information, see Managing a VM (AHV) on page 279.
  - Enable VM high availability. For more information, see Enabling High Availability for the Cluster on page 305.
  - Configure network connections. For more information, see Network Configuration for VM Interfaces on page 167.
- You can create and manage VMs directly from Prism Element when the hypervisor is ESXi.
  - Create VMs. For more information, see Creating a VM (ESXi) on page 289.
  - Manage VMs. For more information, see Managing a VM (ESXi) on page 291.

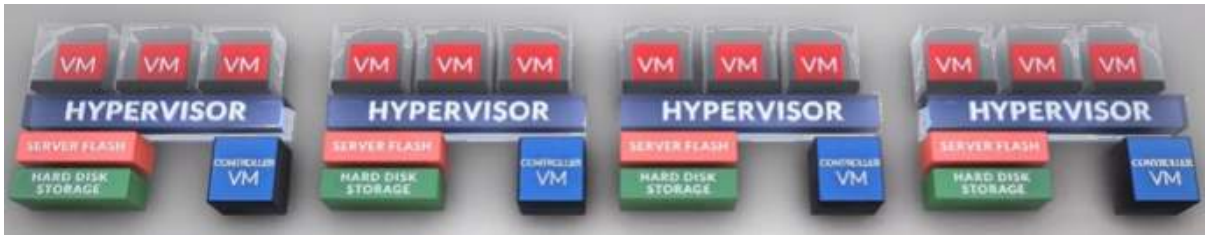


Figure 41: Node Architecture

VM Dashboard

The virtual machine (VM) dashboard displays dynamically updated information about virtual machines in the cluster. To view the VM dashboard, select **VM** from the pull-down list on the left of the main menu.

Menu Options

In addition to the main menu, the VM screen includes a menu bar with the following options:

- *View selector*. Click the **Overview** button on the left to display the VM dashboard. For more information, see VM Overview View on page 265. Click the **Table** button to display VM information in a tabular form. For more information, see VM Table View on page 266.
- *Action buttons*. Click the **Create VM** button on the right to create a virtual machine. For more information, see Creating a VM (AHV) on page 274. Click the **Network Config** button to configure a network connection. For more information, see Network Configuration for VM Interfaces on page 167.

> **Note:** The action buttons appear only in Acropolis managed clusters.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2114

- *CVM filter*. In the Table view, the Controller VMs are not listed by default. To include them in the table list, check the **Include Controller VMs** box.
- *Page selector*. In the Table view, VMs are listed 10 per page. When there are more than 10 VMs, left and right paging arrows appear on the right, along with the total VM count and the VM numbers for the current page.
- *Export VM information*. In the Table view, you can export the table containing the list of VMs and their information to a file in either CSV or JSON format by clicking the gear icon on the right and selecting either **Export CSV** or **Export JSON** from the drop-down menu. (The browser must allow a dialog box for export to work.) Chrome, Internet Explorer, and Firefox download the data into a file; Safari opens the data in the current window.
- *Search box*. In the Table view, you can search for entries in the table by entering a search string in the box.

VM Overview View

The VM Overview view displays VM-specific performance and usage statistics on the left plus the most recent VM-specific alert and event messages on the right.

The following table describes each field in the VM Overview view. Several fields include a slide bar on the right to view additional information in that field. The displayed information is dynamically updated to remain current.

> **Note:** For information about how the statistics are derived, see Understanding Displayed Statistics on page 70.

Table 59: VM Overview View Fields

Name	Description
Hypervisor Summary	Displays the name and version number of the hypervisor.
VM Summary	Displays the total number of VMs in the cluster broken down by on, off, and suspended states.
CPU	Displays the total number of provisioned virtual CPUs and the total amount of reserved CPU capacity in GHz for the VMs.
Memory	Displays the total amount of provisioned and reserved memory in GBs for the VMs.
Top User VMs by Controller IOPS	Displays I/O operations per VM for the 10 most active VMs.
Top User VMs by Controller IO Latency	Displays I/O bandwidth used per VM for the 10 most active VMs. The value is displayed in an appropriate metric (MBps, KBps, and so on) depending on traffic volume.
Top User VMs by Memory Usage	Displays the percentage of reserved memory capacity used per VM for the 10 most active VMs.
Top User VMs by CPU Usage	Displays the percentage of reserved CPU capacity used per VM for the 10 most active VMs.
VM Critical Alerts	Displays the five most recent unresolved VM-specific critical alert messages. Click a message to open the Alert screen at that message. You can also open the Alert screen by clicking the *view all alerts* button at the bottom of the list. For more information, see Alerts Dashboard in *Prism Element Alerts and Events Reference Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2115

Name	Description
VM Warning Alerts	Displays the five most recent unresolved VM-specific warning alert messages. Click a message to open the Alert screen at that message. You can also open the Alert screen by clicking the *view all alerts* button at the bottom of the list.
VM Events	Displays the ten most recent VM-specific event messages. Click a message to open the Event screen at that message. You can also open the Event screen by clicking the *view all events* button at the bottom of the list.

VM Table View

The VM Table view displays information about each VM in a tabular form. The displayed information is dynamically updated to remain current. In Acropolis managed clusters, you can both monitor and manage VMs through the VM Table view.

Table View Fields

The VM Table view is divided into two sections:

- The top section is a table. Each row represents a single VM and includes basic information about that VM. Click a column header to order the rows by that column value (alphabetically or numerically as appropriate).
- The bottom **Summary** section provides additional information. It includes a summary or details column on the left and a set of tabs on the right. The details column and tab content varies depending on what has been selected.

The following table describes each field in the table portion of the view. The details portion and tab contents are described in the subsequent sections.

> **Note:** For information about how the statistics are derived, see Understanding Displayed Statistics on page 70. VirtIO must be installed in a VM for AHV to display correct VM memory statistics. For more information about VirtIO drivers, see Nutanix VirtIO for Windows in *AHV Administration Guide*.

Table 60: VM Table View: Table Fields

Parameter	Description	Values
VM Name	Displays the name given to the VM.	(VM name)
ID	Displays the UUID of the VM.	(VM UUID)
Host	Displays the name of the host.	(Host name)
IP Addresses	Displays the IP address assigned to the VM.	(IP address)
Cores	Displays the number of CPU cores being used by the VM.	(number)
Memory Capacity	Displays the total amount of memory available to the VM.	xxx [MB | GB]
Storage	Displays the used capacity (utilised capacity of the VM disk(s)) in relation to the total capacity (the total storage capacity of all the disks provisioned to the VM). For example, 1.9 GiB/ 5 GiB.	xxx / xxx [MiB | GiB]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2116

Parameter	Description	Values
CPU Usage	Displays the percentage of allocated CPU capacity currently being used by the VM.	0 - 100%
Memory Usage	Displays the percentage of allocated memory capacity currently being used by the VM.	0 -100%
[Controller] Read IOPS	Displays read I/O operations per second (IOPS) for the VM. **Note:** In this and the following three fields, the column name includes the word *Controller* if the information comes from the Controller VM instead of the hypervisor. For ESXi, the information comes from the hypervisor; for Hyper-V and AHV, the information comes from the Controller VM.	(number)
[Controller] Write IOPS	Displays write I/O operations per second for the VM.	(number)
[Controller] IO Bandwidth	Displays I/O bandwidth used per second by the VM.	xxx [MBps|KBps]
[Controller] Avg IO Latency	Displays the average I/O latency of the VM.	xxx [ms]
Backup and Recovery Capable	Indicates (Yes or No) whether the VM can be protected (create backup snapshots) and recovered if needed. When the value is No, click the question mark icon for an explanation.	[Yes|No]
Flash Mode	Displays whether flash mode feature is enabled or not for the VM.	[Yes|No]

VM Detail Information

When a VM is selected in the table, information about that VM appears in the lower part of the screen.

- **Summary:** ***vm_name*** appears below the table and **VM Details** fields appear in the lower left column. The following table describes the fields in this column.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2117

- For VMs in Acropolis managed clusters, action links appear on the right of the **Summary:** ***vm_name*** line. For more information about these actions, see Managing a VM (AHV) on page 279.
  - Click **Manage NGT** to enable and mount Nutanix guest tools for this VM.
  - Click the **Launch Console** link to open a console window for this VM.
  - Click the **Power on** (or **Power Off Actions**) link to start (or shut down) this VM.
  - Click the **Take Snapshot** link to create a backup snapshot on demand.
  - Click the **Migrate** link to migrate the VM onto a different host.
  - Click the **Pause** (or **Resume**) link to pause (or resume) this VM.

    Note: VM pause and resume feature is not supported on AHV.
  - Click the **Clone** link to clone a copy of the VM.
  - Click the **Update** link to update the VM configuration.
  - Click the **Delete** link to delete the VM. (A VM must be powered off before it can be deleted.)

    Note: If the VM is a Prism Central VM, all Actions except **Launch Console**, **Take Snapshot**, and **Migrate** are disabled as a protective measure.
- A set of tabs appear to the right of the details section that display information about the selected VM. The set of tabs varies depending on whether the VM is an Acropolis managed VM or not. The following sections describe each tab.
  - Standard VM tabs: **VM Performance**, **Virtual Disks**, **VM NICs**, **VM Alerts**, **VM Events**, **I/O Metrics**, and **Console**.
  - Acropolis managed VM tabs: **VM Performance**, **Virtual Disks**, **VM NICs**, **VM Snapshots**, **VM Tasks**, **I/O Metrics**, and **Console**.

Table 61: VM Detail Fields

Parameter	Description	Values
Name	Displays the name given the VM.	(VM name)
Host	Displays the host name on which this VM is running.	(IP address)
Host IP	Displays the host IP address for this VM.	(IP address)
Guest OS	Displays the operating system running on this VM, such as Windows 7 or Ubuntu Linux. (This information is not available when running AHV.)	(operating system name)
Memory	Displays the amount of memory available to this VM.	xxx [MB|GB]
Reserved Memory	Displays the amount of memory reserved for this VM (by the hypervisor).	xxx [MB|GB]
Assigned Memory (Hyper-V only)	Displays the amount of dynamic memory currently assigned to the VM by the hypervisor.	xxx [MB|GB]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2118

Parameter	Description	Values
Cores	Displays the number of CPU cores being used by this VM.	(number)
Reserved CPU	Displays the amount of CPU power reserved for this VM (by the hypervisor).	xxx [GHz]
Disk Capacity	Displays the total disk capacity available to this VM.	xxx [GB|TB]
Network Adapters	Displays the number of network adapters available to this VM.	(# of adapter ports)
IP Addresses	Displays the IP address assigned to the VM.	(IP address)
Storage Container	Displays the name of the storage container in which the VM resides.	(storage container name)
Virtual Disks	Displays the number of virtual disks in the VM.	(number)
NGT Enabled	Displays whether NGT is enabled or not for the VM.	[Yes|No]
NGT Mounted	Displays whether NGT is mounted or not for the VM.	[Yes|No]
GPU Configuration	(AHV only) Comma-separated list of GPUs configured for the VM. GPU information includes the model name and a count in parentheses if multiple GPUs of the same type are configured for the VM. If the firmware on the GPU is in compute mode, the string `compute` is appended to the model name. The field is hidden if no GPUs are configured or if the hypervisor is not AHV.	(list of GPUs)
GPUs in Use	(AHV only) Number of GPUs in use by a VM. The field is hidden if no GPUs are configured or if the hypervisor is not AHV.	(number)
VMware Guest Tools Mounted	Displays whether VMware guest tools are mounted or not on the VM	[Yes|No]
VMware Guest Tools Running Status	Displays whether VMware guest tools are running or not on the VM.	[Yes|No]

Cluster Summary Information

When a VM is not selected in the table (or when the word **Summary** is clicked), summary information across all VMs in the cluster appears in the lower part of the screen.

- The **VM Summary** fields appear in the lower left column. The following table describes the fields in this column.
- Three tabs appear that display cluster-wide information (see following sections for details about each tab): **Performance Summary**, **All VM Alerts**, **All VM Events**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2119

Table 62: VM Summary Fields

Parameter	Description	Values
Total VMs	Displays the total number of VMs in the cluster.	(number)
VM State	Displays the number of powered on, powered off, and suspended VMs in the cluster.	[number] powered on, powered off, suspended
Total Provisioned vCPU	Displays the total number of provisioned virtual CPUs in the cluster.	(number)
Total Reserved CPU	Displays the total amount of CPU power reserved for the VMs (by the hypervisor).	xxx [GHz]
Total Provisioned Memory	Displays the total amount of memory provisioned for all VMs.	xxx [GB]
Total Reserved Memory	Displays the total amount of memory reserved for all VMs (by the hypervisor).	xxx [GB]

VM Performance Tab

The VM Performance tab displays graphs of performance metrics. The tab label varies depending on what is selected in the table:

- **Performance Summary** (no VM selected). Displays resource performance statistics (CPU, memory, and I/O) across all VMs in the cluster.
- **VM Performance** (VM selected). Displays resource performance statistics (CPU, memory, and I/O) for the selected VM.

The graphs are rolling time interval performance monitors that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in depth analysis, you can add a monitor to the analysis page by clicking the blue link in the upper right of the graph. For more information, see Analysis Dashboard on page 334. The Performance tab includes the following graphs:

- **[Cluster-wide] CPU Usage**: Displays the percentage of CPU capacity currently being used (0 - 100%) across all VMs or for the selected VM.
- **[Cluster-wide] Memory Usage**: Displays the percentage of memory capacity currently being used (0 - 100%) across all VMs or for the selected VM. (This field does not appear when the hypervisor is Hyper-V.)
- **[Cluster-wide] {Hypervisor|Controller} IOPS**: Displays I/O operations per second (IOPS) across all VMs or for the selected VM.

  > **Note:** In this and the following two fields, the field name is either *Controller* or *Hypervisor* to indicate where the information comes from. For ESXi, the information comes from the hypervisor; for Hyper-V and AHV, the information comes from the Controller VM.

- **[Cluster-wide] {Hypervisor|Controller} I/O Bandwidth**: Displays I/O bandwidth used per second (MBps or KBps) across all VMs or for the selected VM.
- **[Cluster-wide] {Hypervisor|Controller} Avg I/O Latency**: Displays the average I/O latency (in milliseconds) across all VMs or for the selected VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2120

Virtual Disks Tab

The Virtual Disks tab displays information in tabular form about the virtual disks in a selected VM. (This tab appears only when a VM is selected.) Each line represents a virtual disk, and the following information is displayed for each disk organized under *Default* and *Additional Stats* subtabs.

Default Tab:

> **Note:** Clicking on a virtual disk (line) displays subtabs for total, read, and write IOPS, I/O bandwidth, and I/O latency performance graphs for the virtual disk (see the *Performance Tab* section for more information about the graphs).

- **Virtual Disk**. Displays the virtual disk identification number.
- **Total Capacity**. Displays the total capacity of the virtual disk (in GiBs).
- **Physical Usage**. Displays the used space of the virtual disks (in GiBs).
- **Read IOPS**. Displays the read IOPS for the virtual disk.
- **Read BW**. Displays the bandwidth used by the virtual disk for read operations.
- **Read Latency**. Displays the average I/O latency for read requests to this virtual disk.
- **Write IOPS**. Displays the write IOPS for the virtual disk.
- **Write BW**. Displays the bandwidth used by the virtual disk for write operations.
- **Write Latency**. Displays the average I/O latency for write requests to this virtual disk.
- **Flash Mode**. Displays whether flash mode is enabled for the virtual disk or not.

Additional Stats Tab:

- **Total IOPS**. Displays the total (both read and write) I/O operations per second (IOPS) for the virtual disk.
- **Random IO**. Displays the percentage of I/O that is random (not sequential).
- **Read Source Cache**. Displays the amount of cache data accessed for read requests.
- **Read Source SSD**. Displays the amount of SSD data accessed for read requests.
- **Read Source HDD**. Displays the amount of HDD data accessed for read requests.
- **Read Working Size Set**. Displays the amount of data actively being read by applications in the VM that are using this virtual disk.
- **Write Working Size Set**. Displays the amount of data actively being written by applications in the VM that are using this virtual disk.
- **Union Working Size Set**. Displays the total amount of data used by the VM for either reads or writes.

VM NICs Tab

The VM NICs tab displays information in tabular form about the virtual NICs in a selected VM. (This tab appears only when a VM is selected.) Each line represents a virtual NIC, and the following information is displayed for each NIC:

- **Virtual NIC**. Displays the virtual NIC identification number.
- **Adapter Type**. Displays the adaptor type defined for the virtual NIC.
- **MAC Address**. Displays the virtual NIC MAC address
- **IPv4 Addresses**. Displays the virtual NIC IPv4 address(es).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2121

- **IPv6 Addresses**. Displays the virtual NIC IPv6 address(es).
- **Received Packets**. Displays the number of packets received by the virtual NIC.
- **Transmitted Packets**. Displays the number of packets transmitted by the virtual NIC.
- **Dropped Rx Packets**. Displays the number of received packets dropped by the virtual NIC.
- **Dropped Tx Packets**. Displays the number of transmitted packets dropped by the virtual NIC.

When you click a virtual NIC entry, three more tabs appear below the list of virtual NICs. Clicking the **Virtual NICs Stats** tab displays the following statistics for that virtual NIC:

- **Total Packets Received**. Displays a monitor of the total packets received (in KB or MB) over time. Place the cursor anywhere on the line to see the value for that point in time. (This applies to all the monitors on this tab.)
- **Total Packets Transmitted**. Displays a monitor of the transmitted data rate.
- **Dropped Packets Received**. Displays a monitor of received packets that were dropped.
- **Dropped Packets Transmitted**. Displays a monitor of transmitted packets that were dropped.
- **Error Packets Received**. Displays a monitor for error packets received.

Clicking the **Host NICs Stats** tab displays the following statistics for each host NIC (one per line) that is used by the selected virtual NIC to send the traffic:

- **Host NIC**. Displays the host NIC name.
- **Speed (in KBps)**. Displays the host NIC transmission speed.
- **MAC Address**. Displays the host NIC MAC address.
- **Received Packets**. Displays the number of packets received by the host NIC.
- **Transmitted Packets**. Displays the number of packets transmitted by the host NIC.
- **Dropped Rx Packets**. Displays the number of received packets dropped by the host NIC.
- **Dropped Tx Packets**. Displays the number of transmitted packets dropped by the host NIC.
- **Rx Packet Errors**. Displays the number of error packets received by the host NIC.
- **Tx Packet Errors**. Displays the number of error packets transmitted by the host NIC.

Clicking the **Physical Switch Interface Stats** tab displays the following statistics for each physical switch interface (one per line) used by the selected virtual NIC to send the traffic:

- **Physical Switch Interface**. Displays the switch interface name.
- **Switch ID**. Displays the switch interface ID value.
- **Index**. Displays the switch interface index number.
- **MTU (in Bytes)**. Displays the size in bytes of the largest protocol data unit (maximum transmission unit) that the layer can pass onwards.
- **MAC Address**. Displays the interface MAC address.
- **Unicast Rx Pkts**. Displays the number of unicast packets received.
- **Unicast Tx Pkts**. Displays the number of unicast packets transmitted.
- **Error Rx Pkts**. Displays the number of received packets with an error.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2122

- **Error Tx Pkts**. Displays the number of transmitted packets with an error.
- **Discard Rx Pkts**. Displays the number of received packets that were discarded.
- **Discard Tx Pkts**. Displays the number of transmitted packets that were discarded.

VM Alerts Tab

The VM Alerts tab displays the unresolved alert messages about all VMs or the selected VM in the same form as the Alerts page. For more information, see Alerts Summary View. Click the **Unresolved X** button in the filter field to also display resolved alerts.

VM Events Tab

The VM Events tab displays the unacknowledged event messages about all VMs or the selected VM in the same form as the Events page. For more information, see Events Summary View. Click the **Include Acknowledged** button to also display acknowledged events.

VM Snapshots Tab (Acropolis only)

The VM Snapshots tab displays information in tabular form about backup snapshots of the VM. (This tab appears only when a VM is selected.) Each line represents a snapshot, and the following information is displayed for each snapshot:

- **Create Time**. Displays the time the backup snapshot was created (completed).
- **Name**. Displays a name for the backup if one was created.
- **Actions**. Displays four action links:
  - Click the **Details** link to open a window that displays the VM configuration plus a creation time stamp field.
  - Click the **Clone** link to clone a VM from the snapshot.
  - Click the **Restore** link to restore the VM from the snapshot. This restores the VM back to the state of the selected snapshot.
  - Click the **Delete** link to delete the snapshot.

VM Tasks Tab (Acropolis only)

The VM Tasks (selected VM) or All VM Tasks (cluster-wide) tab displays a log in tabular form of the running and completed tasks for the selected VM or across the cluster. Each line represents a task, and the following information is displayed for each task:

- **Operation**. Describes the type of task.
- **Entities**. Lists the affected VM and node.
- **Percent Complete**. Displays the run status (0-100%) of the task.
- **Progress Status**. Displays the completion status of the task (succeeded, in progress, failed).
- **Create Time**. Displays when the task began.
- **Duration**. Displays how long the task took to complete.

I/O Metrics

The I/O Metrics tab displays information about different I/O metrics for the VM (latency and performance distribution).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2123

- Average I/O latency for the VM. Displays a graph of average I/O latency (in milliseconds) for reads and writes over a period of time. If you hover the cursor over the graph, the read and write latency at that particular time is displayed.
- Performance distribution. Displays a bar chart for the performance distribution of read and write size (in bytes) and read and write latency (in milliseconds). This widget also provides information on the read source (HDD, SSD, or DRAM), random vs sequential read and writes in a pie chart format. This information changes according to the time that you select in the **Avg I/O Latency** widget.

Console Tab

The Console tab displays a live console window. (This tab appears only when a VM is selected.) In addition to entering commands in the console window, you can invoke several options from this tab:

- Click the language (left-most) button and select the desired language from the pull-down list to set the language key mapping for the console keyboard.
- Click the **Send CtrlAltDel** button to send a Ctrl+Alt+Delete key signal. This is the same as pressing Ctrl+Alt +Delete from the console keyboard.
- Click the **Take Screenshot** button to take a screen shot of the console display that you can save for future reference.
- Click the **New Window** button to open a new console window. This is the same as clicking the **Launch Console** link on the Summary line.

VM Management

You can create and manage VMs directly from *Prism Element* when the hypervisor is either AHV or ESXi. The following topics provide more information on creating and managing VM configuration on AHV and ESXi.

- AHV
  - To create a VM, see Creating a VM (AHV) on page 274.
  - To manage guest tools, launch console, power actions, take snapshot, migrate, power operations, clone, update, or delete operations, see Managing a VM (AHV) on page 279.
- ESXi
  - To create a VM, see Creating a VM (ESXi) on page 289.
  - To manage guest tools, launch VM console, power actions, clone, update, or delete operations, see Managing a VM (ESXi) on page 291.

Creating a VM (AHV)

In AHV clusters, you can create a new virtual machine (VM) through the Prism Element web console.

About this task

> **Note:** Use Prism Central to create a VM with the memory overcommit feature enabled. Prism Element web console does not allow you to enable memory overcommit while creating a VM. If you create a VM using the Prism Element web console and want to enable memory overcommit for it, update the VM using Prism Central and enable memory overcommit in the **Update VM** page in Prism Central. For more information, see Updating a VM through Prism Central information in *Prism Central Infrastructure Guide*.

When creating a VM, you can configure all of its components, such as number of vCPUs and memory, but you cannot attach a volume group to the VM. Attaching a volume group is possible only when you are modifying a VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2124

To create a VM, do the following:

Procedure

1. Log in to Prism Element web console.
2. In the VM dashboard, click the **Create VM** button.

   > **Note:** This option does not appear in clusters that do not support this feature.

   The **Create VM** dialog box appears.
3. Do the following in the indicated fields:
   a. **Name**: Enter a name for the VM.
   b. **Description** (optional): Enter a description for the VM.
   c. **Timezone**: Select the timezone that you want the VM to use. If you are creating a Linux VM, select **(UTC) UTC**.

      > **Note:**
      >
      > The RTC of Linux VMs must be in UTC, so select the UTC timezone if you are creating a Linux VM.
      >
      > Windows VMs preserve the RTC in the local timezone, so set up the Windows VM with the hardware clock pointing to the desired timezone.

   d. **Use this VM as an agent VM**: Select this option to make this VM as an agent VM.

      You can use this option for the VMs that must be powered on before the rest of the VMs (for example, to provide network functions before the rest of the VMs are powered on the host) and must be powered off after the rest of the VMs are powered off (for example, during maintenance mode operations). Agent VMs are never migrated to any other host in the cluster. If an HA event occurs or the host is put in maintenance mode, agent VMs are powered off and are powered on the same host once that host comes back to a normal state.

      If an agent VM is powered off, you can manually start that agent VM on another host and the agent VM now permanently resides on the new host. The agent VM is never migrated back to the original host. Note that you cannot migrate an agent VM to another host while the agent VM is powered on.

   e. **vCPU(s)**: Enter the number of virtual CPUs to allocate to this VM.
   f. **Number of Cores per vCPU**: Enter the number of cores assigned to each virtual CPU.
   g. **Memory**: Enter the amount of memory (in GiB) to allocate to this VM.
4. (For GPU-enabled AHV clusters only) To configure GPU access, click **Add GPU** in the **Graphics** section, and then do the following in the **Add GPU** dialog box:

   For more information, see GPU and vGPU Support in the *AHV Administration Guide*.

   a. To configure GPU pass-through, in **GPU Mode**, click **Passthrough**, select the GPU that you want to allocate, and then click **Add**.

      If you want to allocate additional GPUs to the VM, repeat the procedure as many times as you need to. Make sure that all the allocated pass-through GPUs are on the same host. If all specified GPUs of the type that you

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2125

want to allocate are in use, you can proceed to allocate the GPU to the VM, but you cannot power on the VM until a VM that is using the specified GPU type is powered off.

For more information, see GPU and vGPU Support in the *AHV Administration Guide*.

b. To configure virtual GPU (vGPU) access, in **GPU Mode**, click **virtual GPU**, select a GRID license, and then select a virtual GPU (vGPU) profile from the list.

> **Note:** This option is available only if you have installed the GRID host driver on the GPU hosts in the cluster.
>
> For more information about the NVIDIA GRID host driver installation instructions, see the NVIDIA Grid Host Driver for Nutanix AHV Installation Guide.

You can assign multiple virtual GPU (vGPU) to a VM. A vGPU is assigned to the VM only if a vGPU is available when the VM is starting up.

Before you add multiple vGPUs to the VM, see Multiple Virtual GPU Support and Restrictions for Multiple vGPU Support in the *AHV Administration Guide*.

> **Note:** Multiple vGPUs are supported on the same VM only if you select the highest vGPU profile type.

After you add the first vGPU, to add multiple vGPUs, see Adding Multiple vGPUs to the Same VM in the *AHV Administration Guide*.

5. Select one of the following firmware to boot the VM.

» **Legacy BIOS**: Select legacy BIOS to boot the VM with legacy BIOS firmware.

» **UEFI**: Select UEFI to boot the VM with UEFI firmware. UEFI firmware supports larger hard drives, faster boot time, and provides more security features. For more information about UEFI firmware, see UEFI Support for VM in the *AHV Administration Guide*.

If you select UEFI, you can enable the following features:

- **Secure Boot**: Select this option to enable UEFI secure boot policies for your guest VMs. For more information about Secure Boot, see Secure Boot Support for VMs in the *AHV Administration Guide*.
- **Windows Defender Credential Guard**: Select this option to enable the Windows Defender Credential Guard feature of Microsoft Windows operating systems that allows you to securely isolate user credentials from the rest of the operating system. Follow the detailed instructions described in Windows Defender Credential Guard Support in AHV in the *AHV Administration Guide* to enable this feature.

> **Note:** For information on how to add the virtual TPM, see Securing AHV VMs with Virtual Trusted Platform Module.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2126

6. To attach a disk to the VM, click the **Add New Disk** button.

   The **Add Disk** dialog box appears. Do the following in the indicated fields:

   a. **Type**: Select the type of storage device, **DISK** or **CD-ROM**, from the drop-down list.

      The following fields and options vary depending on whether you choose **DISK** or **CD-ROM**.

   b. **Operation**: Specify the device contents from the drop-down list.

      - Select **Clone from ADSF file** to copy any file from the cluster that can be used as an image onto the disk.
      - Select **Empty CD-ROM** to create a blank CD-ROM device. (This option appears only when **CD-ROM** is selected in the previous field.) A CD-ROM device is needed when you intend to provide a system image from CD-ROM.
      - Select **Allocate on Storage Container** to allocate space without specifying an image. (This option appears only when **DISK** is selected in the previous field.) Selecting this option means you are allocating space only. You have to provide a system image later from a CD-ROM or other source.
      - Select **Clone from Image Service** to copy an image that you have imported by using image service feature onto the disk. For more information about the Image Service feature, see Configuring Images and Image Management in the *Prism Self Service Administration Guide*.

   c. **Bus Type**: Select the bus type from the dropdown list.

      The options displayed in the **Bus Type** dropdown list varies based on the storage device **Type** selected in Step a.

      - For device **Disk**, select from **SCSI**, **SATA**, **PCI**, or **IDE** bus type.
      - For device **CD-ROM**, you can select either **IDE** or **SATA** bus type.

      Note:

      - SCSI bus is the preferred bus type and it is used in most cases. Ensure you have installed the VirtIO drivers in the guest OS. For more information about VirtIO drivers, see Nutanix VirtIO for Windows in *AHV Administration Guide*.
      - For AHV 5.16 and later, you cannot use an IDE device if **Secured Boot** is enabled for **UEFI Mode** boot configuration.

      Caution: Use SATA, PCI, IDE for compatibility purpose when the guest OS does not have VirtIO drivers to support SCSI devices. This may have performance implications. For more information about VirtIO drivers, see Nutanix VirtIO for Windows in *AHV Administration Guide*.

   d. **ADSF Path**: Enter the path to the desired system image.

      This field appears only when **Clone from ADSF file** is selected. It specifies the image to copy. Enter the path name as `/storage_container_name/iso_name.iso`. For example to clone an image from myos.iso in a storage container named crt1, enter /crt1/myos.iso. When a user types the storage container

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2127

name (/*storage_container_name*/), a list appears of the ISO files in that storage container (assuming one or more ISO files had previously been copied to that storage container).

e. **Image**: Select the image that you have created by using the image service feature.
   This field appears only when **Clone from Image Service** is selected. It specifies the image to copy.

f. **Storage Container**: Select the storage container to use from the drop-down list.
   This field appears only when **Allocate on Storage Container** is selected. The list includes all storage containers created for this cluster.

g. **Logical Size (GiB)**: Enter the disk size in GiB.

h. **Index**: Displays **Next Available** by default.

i. When all the field entries are correct, click the **Add** button to attach the disk to the VM and return to the **Create VM** dialog box.

j. Repeat this step to attach additional devices to the VM.

7. To create a network interface for the VM, click the **Add New NIC** button.
   Prism console displays the **Create NIC** dialog box.

   Note: To create or update a Traffic Mirroring destination type VM or vNIC, use command line interface. For more information, see Traffic Mirroring on AHV Hosts in the *AHV Administration Guide*.

   Do the following in the indicated fields:

   a. **Subnet Name**: Select the target virtual LAN from the drop-down list.
      The list includes all defined networks.

      Note: Selecting IPAM enabled subnet from the drop-down list displays the **Private IP Assignment** information that provides information about the number of free IP addresses available in the subnet and in the IP pool.

   b. **Network Connection State**: Select the state for the network that you want it to operate in after VM creation. The options are *Connected* or *Disconnected*.

   c. **Private IP Assignment**: This is a read-only field and displays the following:

      - **Network Address/Prefix**: The network IP address and prefix.
      - **Free IPs (Subnet)**: The number of free IP addresses in the subnet.
      - **Free IPs (Pool)**: The number of free IP addresses available in the IP pools for the subnet.

   d. **Assignment Type**: This is for IPAM enabled network. Select **Assign with DHCP** to assign IP address automatically to the VM using DHCP. For more information, see IP Address Management in the *AHV Administration Guide*.

   e. When all the field entries are correct, click the **Add** button to create a network interface for the VM and return to the **Create VM** dialog box.

   f. Repeat this step to create additional network interfaces for the VM.

      Note:

      - Nutanix does not recommend configuring multiple clusters to use the same broadcast domain (the same VLAN network), but if you do, configure MAC address prefixes for each cluster to avoid

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2128

duplicate MAC addresses. For information on configuring or removing pre-defined prefix of MAC addresses for each cluster, see MAC Address Prefix on page 164

- Nutanix AHV clusters use the MAC address prefix OUI `50:6B:8D` by default.

8. To configure affinity policy for this VM, click **Set Affinity**.
   The **Set VM Host Affinity** dialog box appears.
   a. Select the host or hosts on which you want configure the affinity for this VM.
   b. Click **Save**.
      The selected host or hosts are listed. This configuration is permanent. The VM will not be moved from this host or hosts even in case of HA event and will take effect once the VM starts.
9. To customize the VM by using Cloud-init (for Linux VMs) or Sysprep (for Windows VMs), select the **Custom Script** check box.
   Fields required for configuring Cloud-init and Sysprep, such as options for specifying a configuration script or answer file and text boxes for specifying paths to required files, appear below the check box.
10. To specify a user data file (Linux VMs) or answer file (Windows VMs) for unattended provisioning, do one of the following:
    » If you uploaded the file to a storage container on the cluster, click **ADSF path**, and then enter the path to the file.
      Enter the ADSF prefix (adsf:///) followed by the absolute path to the file. For example, if the user data is in /home/my_dir/cloud.cfg, enter adsf:///home/my_dir/cloud.cfg. Note the use of three slashes.
    » If the file is available on your local computer, click **Upload a file**, click **Choose File**, and then upload the file.
    » If you want to create or paste the contents of the file, click **Type or paste script**, and then use the text box that is provided.
11. To copy one or more files to a location on the VM (Linux VMs) or to a location in the ISO file (Windows VMs) during initialization, do the following:
    a. In **Source File ADSF Path**, enter the absolute path to the file.
    b. In **Destination Path in VM**, enter the absolute path to the target directory and the file name.
      For example, if the source file entry is /home/my_dir/myfile.txt then the entry for the **Destination Path in VM** should be /<directory_name>/copy_destination> i.e. /mnt/myfile.txt.
    c. To add another file or directory, click the button beside the destination path field. In the new row that appears, specify the source and target details.
12. When all the field entries are correct, click the **Save** button to create the VM and close the **Create VM** dialog box.
    The new VM appears in the VM table view.

Managing a VM (AHV)

You can use the web console to manage virtual machines (VMs) in AHV managed clusters.

About this task

Note: Use Prism Central to update a VM if you want to enable memory overcommit for it. Prism Element web console does not allow you to enable memory overcommit while updating a VM. You can enable memory overcommit in

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2129

the **Update VM** page in Prism Central. For more information, see Updating a VM through Prism Central information in *Prism Central Infrastructure Guide*.

After creating a VM, you can use the web console to start or shut down the VM, launch a console window, update the VM configuration, take a snapshot, attach a volume group, migrate the VM, clone the VM, or delete the VM.

> **Note:** Your available options depend on the VM status, type, and permissions. Unavailable options are grayed out.

To accomplish one or more of these tasks, do the following:

Procedure

1. Log in to Prism Element web console.
2. In the VM dashboard, click the **Table** view.
3. Select the target VM in the table (top section of screen).

   The Summary line (middle of screen) displays the VM name with a set of relevant action links on the right. You can also right-click on a VM to select a relevant action.

   The possible actions are **Manage Guest Tools**, **Launch Console**, **Power on** (or **Power off**), **Take Snapshot**, **Migrate**, **Clone**, **Update**, and **Delete**.

   > **Note:** VM pause and resume feature is not supported on AHV.

   The following steps describe how to perform each action.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2130

4. To manage guest tools as follows, click **Manage Guest Tools**.

   You can also enable NGT applications (self-service restore, Volume Snapshot Service and application-consistent snapshots) also as part of manage guest tools.

   a. Select the **Enable Nutanix Guest Tools** checkbox to enable NGT on the selected VM.

   b. Select the **Mount Nutanix Guest Tools** checkbox to mount NGT on the selected VM.

      Ensure that VM must have at least one empty IDE CD-ROM slot to attach the ISO.

      The VM is registered with the NGT service. NGT is enabled and mounted on the selected virtual machine. A CD with volume label NUTANIX_TOOLS gets attached to the VM.

   c. To enable self-service restore feature for Windows VMs, select the **Self Service Restore (SSR)** checkbox.

      The Self-Service Restore feature is enabled on the VM. The guest VM administrator can restore the desired file or files from the VM. For more information about self-service restore feature, see Self-Service Restore in the *Data Protection and Recovery with Prism Element* guide.

   d. After you select the **Enable Nutanix Guest Tools** checkbox the VSS snapshot feature is enabled by default.

      After this feature is enabled, Nutanix native in-guest VmQuiesced Snapshot Service (VSS) agent takes snapshots for VMs that support VSS.

      > **Note:** The AHV VM snapshots are not application consistent. The AHV snapshots are taken from the **VM** entity menu by selecting a VM and clicking **Take Snapshot**.
      >
      > The application consistent snapshots feature is available with Protection Domain based snapshots and Recovery Points in Prism Central. For more information, see Conditions for Application-consistent Snapshots in the *Data Protection and Recovery with Prism Element* guide.

   e. Click **Submit**.

      The VM is registered with the NGT service. NGT is enabled and mounted on the selected virtual machine. A CD with volume label NUTANIX_TOOLS gets attached to the VM.

      > **Note:**
      >
      > - If you clone a VM, by default NGT is not enabled on the cloned VM. If the cloned VM is powered off, enable NGT from the UI and power on the VM. If cloned VM is powered on, enable NGT from the UI and restart the nutanix guest agent service.
      > - You can enable NGT on multiple VMs simultaneously. For more information, see Enabling NGT and Mounting the NGT Installer Simultaneously on Multiple Cloned VMs.

      If you eject the CD, you can mount the CD back again by logging into the Controller VM and running the following nCLI command.

      ```
      nutanix@cvm$ ncli ngt mount vm-id=virtual_machine_id
      ```

      For example, to mount the NGT on the VM with VM_ID=00051a34-066f-72ed-0000-000000005400::38dc7bf2-a345-4e52-9af6-c1601e759987, type the following command.

      ```
      nutanix@cvm$ ncli ngt mount vm-id=00051a34-066f-72ed-0000-000000005400::38dc7bf2-
      a345-4e52-9af6-
      c1601e759987
      ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2131

5. To launch a console window, click the **Launch Console** action link.

   This opens a Virtual Network Computing (VNC) client and displays the console in a new tab or window. This option is available only when the VM is powered on. The console window includes the following menu options (top right):

   - Clicking the **Mount ISO** button displays a window that allows you to mount an ISO image to the VM. To mount an image, select the desired image and CD-ROM drive from the drop-down lists and then click the **Mount** button.

     > **Note:** For information on how to select CD-ROM as the storage device when you intent to provide a system image from CD-ROM, see *Add New Disk* in Creating a VM (AHV) on page 274.

   - Clicking the **Unmount ISO** button unmounts the ISO from the console.
   - Clicking the **C-A-D** icon button sends a **CtrlAltDel** command to the VM.
   - Clicking the camera icon button takes a screenshot of the console window.
   - Clicking the power icon button allows you to power on/off the VM. These are the same options that you can access from the **Power On Actions** or **Power Off Actions** action link below the VM table (see next step).

6. To start or shut down the VM, click the **Power on** (or **Power off**) action link.

   Power on begins immediately. If you want to power off the VMs, you are prompted to select one of the following options:

   - **Power Off**: Hypervisor performs a hard power off action on the VM.
   - **Power Cycle**: Hypervisor performs a hard restart action on the VM.
   - **Reset**: Hypervisor performs an ACPI reset action through the BIOS on the VM.
   - **Guest Shutdown**: Operating system of the VM performs a graceful shutdown.
   - **Guest Reboot**: Operating system of the VM performs a graceful restart.

   Select the option you want and click **Submit**.

   > **Note:** If you perform power operations such as Guest Reboot or Guest Shutdown by using the Prism Element web console or API on Windows VMs, these operations might silently fail without any error messages if at that time a screen saver is running in the Windows VM. Perform the same power operations again immediately, so that they succeed.

7. To make a snapshot of the VM, click the **Take Snapshot** action link.

   For more information, see Virtual Machine Snapshots on page 285.

8. To migrate the VM to another host, click the **Migrate** action link.

   This displays the **Migrate VM** dialog box. Select the target host from the drop-down list (or select the **System will automatically select a host** option to let the system choose the host) and then click the **Migrate** button to start the migration.

   > **Note:** Nutanix recommends to live migrate VMs when they are under light load. If they are migrated while heavily utilized, migration may fail because of limited bandwidth.

9. To clone the VM, click the **Clone** action link.

   This displays the **Clone VM** dialog box, which includes the same fields as the **Create VM** dialog box. A cloned VM inherits the most the configurations (except the name) of the source VM. Enter a name for the clone and

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2132

then click the **Save** button to create the clone. You can optionally override some of the configurations before clicking the **Save** button. For example, you can override the number of vCPUs, memory size, boot priority, NICs, or the guest customization.

> **Note:**
>
> - You can clone up to 250 VMs at a time.
> - You cannot override the secure boot setting while cloning a VM, unless the source VM already had secure boot setting enabled.

10. To modify the VM configuration, click the **Update** action link.

    The **Update VM** dialog box appears, which includes the same fields as the **Create VM** dialog box. Modify the configuration as needed, and then save the configuration. In addition to modifying the configuration, you can attach a volume group to the VM and enable flash mode on the VM. If you attach a volume group to a VM that is part of a protection domain, the VM is not protected automatically. Add the VM to the same Consistency Group manually.

    (For GPU-enabled AHV clusters only) You can add pass-through GPUs if a VM is already using GPU pass-through. You can also change the GPU configuration from pass-through to vGPU or vGPU to pass-through, change the vGPU profile, add more vGPUs, and change the specified vGPU license. However, you need to power off the VM before you perform these operations.

    - Before you add multiple vGPUs to the VM, see Multiple Virtual GPU Support and Restrictions for Multiple vGPU Support in the *AHV Administration Guide*.
    - Multiple vGPUs are supported on the same VM only if you select the highest vGPU profile type.
    - For more information on vGPU profile selection, see:
      - *Virtual GPU Types for Supported GPUs* in the *NVIDIA Virtual GPU Software User Guide* in the NVIDIA's *Virtual GPU Software Documentation* web-page, and
      - GPU and vGPU Support in the *AHV Administration Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2133

- After you add the first vGPU, to add multiple vGPUs, see Adding Multiple vGPUs to the Same VM in the *AHV Administration Guide*.

You can add new network adapters or NICs using the **Add New NIC** option. For more information, see Step 7 in Creating a VM (AHV) on page 274.

You can also modify the network used by an existing NIC. Before you modify the NIC network observe the limitations in Limitation for vNIC Hot-Unplugging in the *AHV Administration Guide*.

> **Note:**
>
> - To create or update a Traffic Mirroring destination type VM or vNIC, use command line interface. For more information, see Traffic Mirroring on AHV Hosts in the *AHV Administration Guide*.
> - If you delete a vDisk attached to a VM and snapshots associated with this VM exist, space associated with that vDisk is not reclaimed unless you also delete the VM snapshots.

To increase the memory allocation and the number of vCPUs on your VMs while the VMs are powered on (hot-pluggable), do the following:

a. In the **vCPUs** field, you can increase the number of vCPUs on your VMs while the VMs are powered on.

b. In the **Number of Cores Per vCPU** field, you can change the number of cores per vCPU only if the VMs are powered off.

> **Note:** This is not a hot-pluggable feature.

c. In the **Memory** field, you can increase the memory allocation on your VMs while the VMs are powered on.

For more information about hot-pluggable vCPUs and memory, see Virtual Machine Memory and CPU Hot-Plug Configurations.

To attach a volume group to the VM, do the following:

a. In the **Volume Groups** section, click **Add volume group**, and then do one of the following:

   » From the **Available Volume Groups** list, select the volume group that you want to attach to the VM.

   » Click **Create new volume group**, and then, in the **Create Volume Group** dialog box, create a volume group. After you create a volume group, select it from the **Available Volume Groups** list.

   Repeat these steps until you have added all the volume groups that you want to attach to the VM.

b. Click **Add**.

11. To enable flash mode on the VM, click the **Enable Flash Mode** check box.

» After you enable this feature on the VM, the status is updated in the VM table view. To view the status of individual virtual disks (disks that are flashed to the SSD), click the update disk icon in the **Disks** pane in the **Update VM** window.

» You can disable the flash mode feature for individual virtual disks. To update the flash mode for individual virtual disks, click the update disk icon in the **Disks** pane and deselect the **Enable Flash Mode** check box.

12. To delete the VM, click the **Delete** action link. A window prompt appears; click the **OK** button to delete the VM.
The deleted VM disappears from the list of VMs in the table.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2134

Virtual Machine Snapshots

You can generate snapshots of virtual machines or VMs. You can generate snapshots of VMs manually or automatically. Some of the purposes that VM snapshots serve are as follows:

- Disaster recovery
- Testing - as a safe restoration point in case something went wrong during testing.
- Migrate VMs
- Create multiple instances of a VM.

Snapshot is a point-in-time state of entities such as VM and Volume Groups, and used for restoration and replication of data. You can generate snapshots and store them locally or remotely. Snapshots are mechanism to capture the delta changes that has occurred over time. Snapshots are primarily used for data protection and disaster recovery. Snapshots are not autonomous like backup, in the sense that they depend on the underlying VM infrastructure and other snapshots to restore the VM. Snapshots consume less resources compared to a full autonomous backup. Typically, a VM snapshot captures the following:

- The state including the power state (for example, powered-on, powered-off, suspended) of the VMs.
- The data includes all the files that make up the VM. This data also includes the data from disks, configurations, and devices, such as virtual network interface cards.

VM Snapshots and Snapshots for Disaster Recovery

The **VM** Dashboard only allows you to generate VM snapshots manually. You cannot select VMs and schedule snapshots of the VMs using the VM dashboard. The snapshots generated manually have very limited utility.

> **Note:** These snapshots (stored locally) cannot be replicated to other sites.

You can schedule and generate snapshots as a part of the disaster recovery process using Nutanix DR solutions. AOS generates snapshots when you protect a VM with a protection domain using the **Data Protection** dashboard in Prism Element web console. For more information, see Snapshots in the *Data Protection and Recovery with Prism Element Guide*. Similarly, AOS generates recovery points (snapshots are called recovery points in Prism Central) when you protect a VM with a protection policy. For more information about protection policies, see Protection Policies View in *Nutanix Disaster Recovery Guide*.

For example, in the **Data Protection** dashboard in Prism Element web console, you can create schedules to generate snapshots using various RPO schemes such as asynchronous replication with frequency intervals of 60 minutes or more, or NearSync replication with frequency intervals of as less as 20 seconds up to 15 minutes. These schemes create snapshots in addition to the ones generated by the schedules, for example, asynchronous replication schedules generate snapshots according to the configured schedule and, in addition, an extra snapshot every 6 hours. Similarly, NearSync generates snapshots according to the configured schedule and also generates one extra snapshot every hour.

Similarly, you can use the options in the Data Protection entity of Prism Central to generate recovery points using the same RPO schemes.

Creating a VM Snapshot Manually

You can create or generate a VM snapshot manually in Prism Element web console.

Procedure

1. Log in to Prism Element web console.
2. In the VM dashboard, click the **Table** view.
3. Click the VM you want to take a snapshot of.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2135

4. In the **Take Snapshot** dialog box, provide a name for the snapshot and click **Submit**.
   Ensure that the name contains only alphanumeric, dot, dash, or underscore characters.
   The snapshot is listed with the name you provided in the **VM Snapshots** tab in the **Summary** section of the **VM Table** view.

What to do next

You can **Delete** the snapshot. For more information, see Deleting a VM Snapshot Manually on page 286.

You can clone a VM by clicking the **Clone** action link for the snapshot of the VM.

You can use the VM snapshot to **Restore** the VM to the previous state captured in the snapshot.

Click **Details** to view the details of the snapshot.

Deleting a VM Snapshot Manually

You can delete a snapshot for any VM.

Procedure

1. Log in to Prism Element web console.
2. In the VM dashboard, click the **Table** view.
3. Click the VM you want to delete a snapshot of.
4. Click the **VM Snapshots** tab in the **Summary** section of the **VM Table** view.
5. Click the **Delete** action link for the snapshot that you want to delete in the list of snapshots.
6. On the confirmation box,
   - » Click **Yes** to delete the snapshot.
   - » Click **Cancel** to close the confirmation box without deleting the snapshot.

What to do next

To create a snapshot manually, see Creating a VM Snapshot Manually on page 285.

Adding Multiple vGPUs to the Same VM

About this task

You can add multiple vGPUs of the same vGPU type when you create a new VM or update an existing VM.

- For information on how to create a VM, see Creating a VM through Prism Central (AHV).
- For information on how to update an existing VM, see Updating a VM through Prism Central (AHV).

For more information on multiple vGPU support, see Multiple Virtual GPU Support.

Before you begin

Ensure that the following prerequisites are met before you add multiple vGPUs to the VM:

- Select the license for NVIDIA Virtual GPU (vGPU) software version 10.1 (440.53) or later.
- Observe the guidelines and restrictions specified in Multiple Virtual GPU Support and Restrictions for Multiple vGPU Support.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2136

Procedure

To add multiple vGPUs to the same VM, perform the following steps:

1. Click **Add GPU** in the **Resources** step of create VM workflow or update VM workflow. For more information, see Creating a VM through Prism Central (AHV) or Updating a VM through Prism Central (AHV)
2. In the **Add GPU** window, click **Add**.

   The License field is grayed out and you cannot select a different license when you add a vGPU for the same VM.

   The **VGPU Profile** is auto-selected. The system allows you to select additional vGPU of the same vGPU type as indicated by the message at the top of the **Add GPU** window.

   The newly added vGPU appears in the **Create VM** or **Update VM** window.
3. Repeat the steps for each vGPU addition to the VM.

Migrating Live a vGPU-enabled VM Within the Cluster

You can migrate a vGPU-enabled VM only to another host in the same cluster on Prism Element.

About this task

You can perform live migration of VMs enabled with virtual GPUs (vGPU-enabled VMs) only on commercially reasonable effort, if the destination node is equipped to provide enough resources to the vGPU- enabled VMs. However, if the destination node is not equipped with the enough resources, the vGPU-enabled VMs are shut down and you might experience a downtime.

In a successful migration case, the vGPUs can continue to run while the VMs that are running the vGPUs are seamlessly migrated in the background.

When you perform the LCM update, the vGPU-enabled VMs are listed as Non-HA-protected VMs. LCM also migrates the Non-HA-protected VMs on commercially reasonable effort to the destination node if the following requirements are met:

- Destination node is equipped with the required resources for the VM.
- The VM GPU drivers are compatible with the AHV host GPU drivers.

If the destination node is not equipped with the enough resources or there is any compatibility issue between the VM GPU drivers and AHV host GPU drivers, the LCM forcibly shuts down the Non-HA-protected VMs.

Before you begin

Ensure the following prerequisites are met before you live migrate the vGPU-enabled VMs:

- The VM is not powered off.
- The host affinity is not set for the VM.

  If the host affinity of the VM is set to only one host, you cannot live migrate the VM. However, based on the GPU resources required, if the host affinity is set to multiple hosts with the same or similar GPU resources, you can migrate the VM among the hosts with which the affinity is set.
- You have another host in the same cluster to migrate the VM.

For limitations applicable to live migration of vGPU-enabled VMs, see Limitations of Live Migration Support in the *AHV Administration Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2137

Table 63: Minimum Versions

Component	Supports	With Minimum Version
AOS	Live migration within the same cluster	5.18.1
AHV	Live migration within the same cluster	20190916.294
AOS	Live migration across cluster	6.1
AHV	Live migration across cluster	20201105.30142

Procedure

To migrate the vGPU-enabled VM to another host within the same cluster on Prism Element, perform the following steps:

1. Log in to Prism Element web console.
2. In the VM dashboard, click the **Table** view.
3. To migrate the VM, go to the **VM** > **Table**.
4. Select the VM you want to migrate live. Click **Migrate**.
5. In the **Migrate VM** dialog box, do the following:
   a. In the **Host** drop-down list, do one of the following:
      » Retain the `System will automatically select a host` option if you want to migrate the VM to a host selected by the system.

        The system selects a host based on the GPU resources available with the host as appropriate for the VM to be migrated live.
      » Select the host listed in the drop-down list that you want to migrate the VM to.
6. Click **Migrate**.

   Prism submits the task and displays the following message:

   ```
   Successfully submitted migrate operation.
   Task details
   ```

   Task details is a link to the **Tasks** page. Click the link to monitor the migration task on the **Tasks** page.

   When the migration is complete, the host name of the VM in the **List** view changes to the host name to which you migrated the VM.

VM Management through Prism Element (ESXi)

You can perform your core VM management operations directly from Prism without using any hypervisor management interface (for example, vCenter Server). The VM Management through Prism for ESXi feature provides an unified management interface for all of the ESXi hypervisors. For this functionality to work, you need to register vCenter Server with the Prism Element or multiple vCenter Servers with the Prism Central. For more information about registering vCenter Server to your cluster, see Registering a Cluster to vCenter Server on page 366.

By using this feature you can perform following operations directly through Prism.

- Create, clone, update, and delete VMs.
- Create and delete NICs.
- Attach and delete disks.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2138

- Power operations: Power on or off, reset, suspend, resume, guest shutdown, and guest restart.
- Open and launch VM console.
- Manage VM guest tools (mounting VMware guest tools, mounting NGT).

> **Note:**
>
> - You can perform the power operations and launching of VM console even when vCenter Server is not registered.
> - If you are creating VM through Prism, configuration changes to the VM when it is powered on is enabled by default and it depends on the guest operating system that is deployed on the VM.

Rules and Guidelines

- Ensure that all the hosts in the cluster is managed by a single vCenter Server.
- Ensure that DRS is enabled on the vCenter Server.
- Ensure that you are running ESXi and vCenter Server 5.5 or later releases.
- Ensure that you have homogeneous network configuration. For example, network should have either 1G or 10G NICs.
- Ensure that you unregister the vCenter Server from the cluster before changing the IP address of the vCenter Server. After you change the IP address of the vCenter Sever, you must register the vCenter Server again with the new IP address.
- The vCenter Server Registration page displays the registered vCenter Server. If for some reason the Host Connection field changes to **Not Connected**, it implies that the hosts are being managed by a different vCenter Server. In this case, there will be new vCenter entry with host connection status as Connected and you need to register to this vCenter Server. For more information about registering vCenter Server again, see Managing vCenter Server Registration Changes on page 367.

> **Caution:** If multiple vCenter Servers are managing the hosts, you will not be able to perform the VM management operations. Move all the hosts into one vCenter Server.

Requirements and Limitations

- SCSI, IDE, and SATA disks are supported. PCI disks are not supported.
- The E1000, E1000e, PCnet32, VMXNET, VMXNET 2, VMXNET 3 network adapter types (NICs) are supported.
- Creating a VM by using a template is not supported.
- Creating a VM by using image service is not supported.
- If a VM is deleted, all the disks that are attached to the VM gets deleted.
- Network configuration (creation of port groups or VLANs) is not supported.

Creating a VM (ESXi)

In ESXi clusters, you can create a new virtual machine (VM) through the web console.

Before you begin

- Ensure that you refer requirements and limitations. For more information, see the requirements and limitations section in VM Management through Prism Element (ESXi) before proceeding.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2139

- Register the vCenter Server with your cluster. For more information, see Registering a Cluster to vCenter Server on page 366.

About this task

When creating a VM, you can configure all of its components, such as number of vCPUs and memory, but you cannot attach a volume group to the VM.

To create a VM, do the following:

Procedure

1. Log in to Prism Element web console.
2. In the VM dashboard, click the **Create VM** button.
   The **Create VM** dialog box appears.
3. Do the following in the indicated fields:
   a. **Name**: Enter a name for the VM.
   b. **Description** (optional): Enter a description for the VM.
   c. **Guest OS**: Type and select the guest operating system.
      The guest operating system that you select affects the supported devices and number of virtual CPUs available for the virtual machine. The **Create VM** wizard does not install the guest operating system. For information on the list of supported operating systems, see VM Management through Prism Element (ESXi).
   d. **vCPU(s)**: Enter the number of virtual CPUs to allocate to this VM.
   e. **Number of Cores per vCPU**: Enter the number of cores assigned to each virtual CPU.
   f. **Memory**: Enter the amount of memory (in GiBs) to allocate to this VM.
4. To attach a disk to the VM, click the **Add New Disk** button.
   The Add Disks dialog box appears. Do the following in the indicated fields:
   a. **Type**: Select the type of storage device, **DISK** or **CD-ROM**, from the drop-down list.
      The following fields and options vary depending on whether you choose **DISK** or **CD-ROM**.
   b. **Operation**: Specify the device contents from the drop-down list.
      - Select **Clone from ADSF file** to copy any file from the cluster that can be used as an image onto the disk.
      - Select **Allocate on Storage Container** to allocate space without specifying an image. (This option appears only when **DISK** is selected in the previous field.) Selecting this option means you are allocating space only. You have to provide a system image later from a CD-ROM or other source.
   c. **Bus Type**: Select the bus type from the drop-down list. The choices are **IDE** or **SCSI**.
   d. **ADSF Path**: Enter the path to the desired system image.
      This field appears only when **Clone from ADSF file** is selected. It specifies the image to copy. Enter the path name as `/storage_container_name/vmdk_name.vmdk`. For example to clone an image from myvm-flat.vmdk in a storage container named crt1, enter /crt1/myvm-flat.vmdk. When a user types the storage

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2140

container name (/*storage_container_name*/), a list appears of the VMDK files in that storage container (assuming one or more VMDK files had previously been copied to that storage container).

> **Note:** Make sure you are copying from a flat file.

e. **Storage Container**: Select the storage container to use from the drop-down list.

This field appears only when **Allocate on Storage Container** is selected. The list includes all storage containers created for this cluster.

f. **Size**: Enter the disk size in GiBs.

g. When all the field entries are correct, click the **Add** button to attach the disk to the VM and return to the **Create VM** dialog box.

h. Repeat this step to attach more devices to the VM.

5. To create a network interface for the VM, click the **Add New NIC** button.

The Create NIC dialog box appears. Do the following in the indicated fields:

a. **VLAN Name**: Select the target virtual LAN from the drop-down list.

The list includes all defined networks. For more information, see Network Configuration for VM Interfaces.

b. **Network Adapter Type**: Select the network adapter type from the drop-down list.

For information on the list of supported adapter types, see VM Management through Prism Element (ESXi).

c. **Network UUID**: This is a read-only field that displays the network UUID.

d. **Network Address/Prefix**: This is a read-only field that displays the network IP address and prefix.

e. When all the field entries are correct, click the **Add** button to create a network interface for the VM and return to the **Create VM** dialog box.

f. Repeat this step to create more network interfaces for the VM.

6. When all the field entries are correct, click the **Save** button to create the VM and close the **Create VM** dialog box.

The new VM appears in the VM table view. For more information, see VM Table View.

Managing a VM (ESXi)

You can use the web console to manage virtual machines (VMs) in the ESXi clusters.

Before you begin

- Ensure that you refer the requirements and limitations. For more information, see the requirements and limitations section in VM Management through Prism Element (ESXi) before proceeding.
- Ensure that you have registered the vCenter Server with your cluster. For more information, see Registering a Cluster to vCenter Server on page 366.

About this task

After creating a VM, you can use the web console to manage guest tools, power operations, suspend, launch a VM console window, update the VM configuration, clone the VM, or delete the VM. To accomplish one or more of these tasks, do the following:

> **Note:** Your available options depend on the VM status, type, and permissions. Unavailable options are unavailable.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2141

Procedure

1. Log in to Prism Element web console.
2. In the VM dashboard, click the **Table** view.
3. Select the target VM in the table (top section of screen).

   The summary line (middle of screen) displays the VM name with a set of relevant action links on the right. You can also right-click on a VM to select a relevant action.

   The possible actions are **Manage Guest Tools**, **Launch Console**, **Power on** (or **Power off actions**), **Suspend** (or **Resume**), **Clone**, **Update**, and **Delete**. The following steps describe how to perform each action.
4. To manage guest tools as follows, click **Manage Guest Tools**.

   You can also enable NGT applications (self-service restore, volume snapshot service and application-consistent snapshots) as part of manage guest tools.

   a. Select the **Enable Nutanix Guest Tools** checkbox to enable NGT on the selected VM.

   b. Select the **Mount Nutanix Guest Tools** checkbox to mount NGT on the selected VM.

      Ensure that VM has at least one empty IDE CD-ROM or SATA slot to attach the ISO.

      The VM is registered with the NGT service. NGT is enabled and mounted on the selected virtual machine. A CD with volume label NUTANIX_TOOLS gets attached to the VM.

   c. To enable self-service restore feature for Windows VMs, select the **Self Service Restore (SSR)** checkbox.

      The self-service restore feature is enabled of the VM. The guest VM administrator can restore the desired file or files from the VM. For information on the self-service restore feature, see Self-Service Restore in the *Data Protection and Recovery with Prism Element* guide.

   d. After you select the **Enable Nutanix Guest Tools** checkbox the VSS and application-consistent snapshot feature is enabled by default.

      After this feature is enabled, Nutanix native in-guest VmQuiesced snapshot service (VSS) agent is used to take application-consistent snapshots for all the VMs that support VSS. This mechanism takes application-consistent snapshots without any VM stuns (temporary unresponsive VMs) and also enables third-party backup providers like Commvault and Rubrik to take application-consistent snapshots on Nutanix platform

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2142

in a hypervisor-agnostic manner. For more information, see Conditions for Application-consistent Snapshots in the *Data Protection and Recovery with Prism Element* guide.

e. To mount VMware guest tools, select the **Mount VMware Guest Tools** checkbox.

The VMware guest tools are mounted on the VM.

> **Note:** You can mount both VMware guest tools and Nutanix Guest Tools at the same time on a particular VM provided the VM has sufficient empty CD-ROM slots.

f. Click **Submit**.

The VM is registered with the NGT service. NGT is enabled and mounted on the selected virtual machine. A CD with volume label NUTANIX_TOOLS gets attached to the VM.

> **Note:**
>
> - If you clone a VM, by default NGT is not enabled on the cloned VM. If the cloned VM is powered off, enable NGT from the UI and start the VM. If cloned VM is powered on, enable NGT from the UI and restart the Nutanix guest agent service.
> - For information on how to enable NGT on multiple VMs simultaneously, see Enabling NGT and Mounting the NGT Installer on Cloned VMs.

If you eject the CD, you can mount the CD back again by logging into the Controller VM and running the following nCLI command.

```
ncli> ngt mount vm-id=virtual_machine_id
```

For example, to mount the NGT on the VM with VM_ID=00051a34-066f-72ed-0000-000000005400::38dc7bf2-a345-4e52-9af6-c1601e759987, type the following command.

```
ncli> ngt mount vm-id=00051a34-066f-72ed-0000-000000005400::38dc7bf2-
a345-4e52-9af6-
c1601e759987
```

> **Caution:** In AOS 4.6, for the powered-on Linux VMs on AHV, ensure that the NGT ISO is ejected or unmounted within the guest VM before disabling NGT by using the web console. This issue is specific for 4.6 version and does not occur from AOS 4.6.x or later releases.

> **Note:** If you have created the NGT ISO CD-ROMs prior to AOS 4.6 or later releases, the NGT functionality will not work even if you upgrade your cluster because REST APIs have been disabled. You must unmount the ISO, remount the ISO, install the NGT software again, and then upgrade to 4.6 or later version.

5. To launch a VM console window, click the **Launch Console** action link.

This opens a virtual network computing (VNC) client and displays the console in a new tab or window. This option is available only when the VM is powered on. The VM power options that you access from the **Power Off Actions** action link below the VM table can also be accessed from the VNC console window. To access the VM power options, click the **Power** button at the top-right corner of the console window.

> **Note:** A VNC client may not function properly on all browsers. Some keys are not recognized when the browser is Google Chrome. (Firefox typically works best.)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2143

6. To start (or shut down) the VM, click the **Power on** (or **Power off**) action link.

   Power on begins immediately. If you want to shut down the VMs, you are prompted to select one of the following options:

   - **Power Off**. Hypervisor performs a hard shut down action on the VM.
   - **Reset**. Hypervisor performs an ACPI reset action through the BIOS on the VM.
   - **Guest Shutdown**. Operating system of the VM performs a graceful shutdown.
   - **Guest Reboot**. Operating system of the VM performs a graceful restart.

   > **Note:** The **Guest Shutdown** and **Guest Reboot** options are available only when VMware guest tools are installed.

7. To pause (or resume) the VM, click the **Suspend** (or **Resume**) action link. This option is available only when the VM is powered on.

8. To clone the VM, click the **Clone** action link.

   This displays the **Clone VM** dialog box, which includes the same fields as the **Create VM** dialog box. A cloned VM inherits the most the configurations (except the name) of the source VM. Enter a name for the clone and then click the **Save** button to create the clone. You can optionally override some of the configurations before clicking the **Save** button. For example, you can override the number of vCPUs, memory size, boot priority, NICs, or the guest customization.

   > **Note:**
   > - You can clone up to 250 VMs at a time.
   > - In the Clone window, you cannot update the disks.

9. To modify the VM configuration, click the **Update** action link.

   The **Update VM** dialog box appears, which includes the same fields as the **Create VM** dialog box. Modify the configuration as needed, and in addition you can enable Flash Mode for the VM.

   > **Note:** If you delete a vDisk attached to a VM and snapshots associated with this VM exist, space associated with that vDisk is not reclaimed unless you also delete the VM snapshots.

   a. Select the **Enable Flash Mode** checkbox.

      » After you enable this feature on the VM, the status is updated in the VM table view. To view the status of individual virtual disks (disks that are flashed to the SSD), go the **Virtual Disks** tab in the VM table view.

      » You can disable the Flash Mode feature for individual virtual disks. To update the Flash Mode for individual virtual disks, click the update disk icon in the **Disks** pane and clear the **Enable Flash Mode** checkbox.

10. To delete the VM, click the **Delete** action link. A window prompt appears; click the **OK** button to delete the VM.
    The deleted VM disappears from the list of VMs in the table. You can also delete a VM that is already powered on.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2144

Configuring Images

In AHV clusters, you can import and configure operating system ISO and disk image files through the web console. You can also convert previously imported files to the format that AHV uses.

About this task

The image service feature allows you to build a store of imported files that you can use to create a CD-ROM from an ISO image or an operating system disk from a disk image when creating a VM. The image service supports raw, VHD, VHDX, VMDK, VDI, OVA, ISO, and QCOW2 disk formats. Port 2007 must be open, since the image service uses port 2007. For the complete list of required ports, see Port Reference.

Image create, update, and delete (CUD) behavior depends on whether a cluster (also known as Prism Element) is registered to Prism Central.

- Images created on a Prism Element reside on Prism Element and can be managed from Prism Element.
- For better centralized management, you can migrate images manually to Prism Central by using the image import feature in Prism Central. An image migrated to Prism Central in this way remains on Prism Element, but you can manage the image only from Prism Central. Migrated images cannot be updated from the Prism Element.
- In the case of a local image upload, with more than one Prism Element cluster managed by Prism Central, the image state is active on that Prism Element cluster. All other Prism Element clusters show the image as inactive. If you create a VM from that image, the image bits are copied to the other Prism Element clusters. The image then appears in an active state on all managed Prism Element clusters.

> **Note:**
>
> After you upload a disk image file, the storage size of the image file in the cluster appears higher than the actual size of the image. This is because the image service in the cluster converts the image file to raw format which is required by AHV to create a VM from an image.

To import and configure an image file, do the following:

Procedure

1. Log on to the Prism Element web console.
2. Click the gear icon in the main menu and then select **Image Configuration** in the **Settings** page.
   The **Image Configuration** window appears.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2145

3. To upload an image file to the cluster, click the **Upload Image** button.
   The **Create Image** window appears. Do the following in the indicated fields:

   a. **Name**: Enter a name for the image.

   b. **Annotation** (optional): Enter a description for the image.

   c. **Image Type** (optional): Select the image type, either **ISO** or **Disk**, from the pull-down list.

   d. **Storage Container**: Select the storage container to use from the pull-down list.
      The list includes all storage containers created for this cluster. If there are no storage containers currently, a **Create Storage Container** link appears to create a storage container.

   e. **Image Source**: Do one of the following:

      - Click the **From URL** option to import the image from the Internet. Enter the appropriate URL address in the field using the following syntax for either NFS or HTTP. (NFS and HTTP are the only supported protocols.)

        ```
        nfs://[hostname|IP_addr]/path
        http://[hostname|IP_addr]/path
        ```

        Enter either the name of the host (*hostname*) or the host IP address (*IP_addr)* and the path to the file. If you use a *hostname*, the cluster must be configured to point at a DNS server that can resolve that name. A file uploaded through NFS must have 644 permissions. For more information, see Configuring Name Servers on page 353.

        If the image files have been copied to a container on the cluster, replace *IP_addr* with CVM IP address.

        For example, enter nfs://*CVM_IP_addr*/*container_name*/*file_name*.

        Replace *CVM_IP_addr* with the CVM IP address, *container_name* with the name of the container where the image is placed, and *file_name* with the image file name.

        To identify the NFS path to the VM disks of a VM, log on to any CVM in a cluster as Nutanix user. Run the following command to find the associated disk UUID.

        ```
        nutanix@cvm$ acli vm.get <VM name> include_vmdisk_paths=1 | grep -E 'disk_list|
        vmdisk_nfs_path|vmdisk_size|vmdisk_uuid'
        ```

        To construct the NFS path, append the VM disk path returned by the command to nfs://*CVM_IP_addr*. For example, if the command returns the path ContainerA/.acropolis/vmdisk/9365b2eb-a3fd-45ee-b9e5-64b87f64a2df, then your NFS path is nfs://*CVM_IP_addr*/ContainerA/.acropolis/vmdisk/9365b2eb-a3fd-45ee-b9e5-64b87f64a2df.

        Replace *CVM_IP_addr* with the CVM IP address.

      - Click the **Upload a file** option to upload a file from your workstation. Click the **Choose File** button and then select the file to upload from the file search window.

   f. When all the fields are correct, click the **Save** button.
      The **Create Image** window closes and the **Image Configuration** window reappears with the new image appearing in the list.

4. To update the image information, click the pencil icon for that image.
   The **Update Image** window appears. Update the fields as desired and then click the **Save** button.

   > **Note:** The pencil icon is unavailable for images imported to Prism Central. Use Prism Central to manage such images.

5. To delete an image file from the store, click the X icon for that image.
   The image file is deleted and that entry disappears from the list.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2146

Virtual Machine Customization

In an Acropolis cluster, you can use Cloud-init to customize Linux VMs and the System Preparation (Sysprep) tool to customize Windows VMs.

About Cloud-Init

Cloud-init is a utility that is used to customize Linux VMs during first-boot initialization. The utility must be pre-installed in the operating system image used to create VMs. Cloud-init runs early in the boot process and configures the operating system on the basis of data that you provide (user data). You can use Cloud-init to automate tasks such as setting a host name and locale, creating users and groups, generating and adding SSH keys so that users can log in, installing packages, copying files, and bootstrapping other configuration management tools such as Chef, Puppet, and Salt. For more information about Cloud-init, see https://cloudinit.readthedocs.org/.

About Sysprep

Sysprep is a utility that prepares a Windows installation for duplication (imaging) across multiple systems. Sysprep is most often used to generalize a Windows installation. During generalization, Sysprep removes system-specific information and settings such as the security identifier (SID) and leaves installed applications untouched. You can capture an image of the generalized installation and use the image with an answer file to customize the installation of Windows on other systems. The answer file contains the information that Sysprep needs to complete an unattended installation. For more information about Sysprep and answer files, see the Microsoft Sysprep documentation.

The Customization Process in a Nutanix Cluster

You can use Cloud-init or Sysprep both when creating and when cloning VMs in a Nutanix cluster. For unattended provisioning, you can specify a user data file for Cloud-init and an answer file for Sysprep. All Cloud-init user-data formats are supported. For example, you can use the Cloud Config format, which is written in YAML, or you can provide a multi-part archive. To enable Cloud-init or Sysprep to access the script, AOS creates a temporary ISO image that includes the script and attaches the ISO image to the VM when you power on the VM.

> **Note:** The ISO image is mounted on bus IDE 3, so ensure that no other device is mounted on that bus.

You can also specify source paths to the files or directories that you want to copy to the VM, and you can specify the target directories for those files. This is particularly useful if you need to copy software that is needed at start time, such as software libraries and device drivers. For Linux VMs, AOS can copy files to the VM. For Windows VMs, AOS can copy files to the ISO image that it creates for the answer file.

After customizing a VM, you can copy the VDisk of the VM to Image Service for backup and duplication.

Customizing Linux Virtual Machines with Cloud-Init

Keep the user data file ready, either saved locally or uploaded to a storage container on the cluster. Alternatively, you can create or paste the script in the web console. If you want files copied to the VM during initialization, upload the files to a storage container on the cluster.

About this task

To customize a Linux VM by using Cloud-init, do the following:

Procedure

1. Log in to the web console by using the Nutanix credentials.
2. In the VM dashboard, do one of the following:
   - » To create a VM, click **Create VM**.
   - » To clone a VM, click the VM that you want to clone, and then click **Clone**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2147

3. In the **Create VM** or **Clone VM** dialog box, specify a name for the VM and allocate resources such as vCPUs, memory, and storage. Select the **Custom Script** check box and specify how you want to customize the VM.

   For information about creating a VM and specifying customization options, see Creating a VM (AHV) on page 274. For information about cloning a VM, see Managing a VM (AHV) on page 279.

   For information about using cloud-init custom script, see Cloud-Init Limitations and Guidelines on page 298 and Cloud-init Sample Scripts on page 298.

4. In the VM dashboard, select the VM, and then click **Power On**.
   The VM is powered on and initialized based on the directives in the user data file. To create a reference image from the VM, use Image Service. For more information about Image Service, see Configuring Images.

Cloud-Init Limitations and Guidelines

- Nutanix supports a maximum of 32 KB for the size of a VM guest customization script.
- AHV supports guest customization through cloud-init using Config Drive v2 datasource (see Cloud-init documentation). For more information, see the example cloud-init scripts for network configuration.

Cloud-init Sample Scripts

The following are a few sample cloud-init scripts that you can use to customize the VMs.

Script for setting up a static IP configuration (CentOS)

On CentOS, you can inject the static IP configuration in the cloud-init script by editing the network interface configuration file located in /etc/sysconfig/network-scripts directory with a *write_files* block as shown in the following example:

```
#cloud-config

disable_root: False
cloud_config_modules:
 -resolv_conf

# Set the hostname
hostname: host_name
fqdn: host_name.domain_name

# User Authentication
users:
   - default
   - name: linux.username
     ssh-authorized-keys:
     - public_key
     sudo: ['ALL=(ALL) NOPASSWD:ALL']

# Assign static IP address
write_files:
 - path: /etc/sysconfig/network-scripts/ifcfg-eth0
   content: |
     IPADDR=vm_ip
     NETMASK=vm_subnet_mask
     GATEWAY=vm_gateway
     BOOTPROTO=static
     ONBOOT=yes
     DEVICE=eth0

# Configure resolv.conf
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2148

```
manage_resolv_conf: true
resolv_conf:
  nameservers: ['dns1','dns2']
  domain: 'domain_name'
  options:
    attempts: 5
    timeout: 15

# Run the boot commands
runcmd:
  - [sudo, ifdown, eth0]
  - [sudo, ifup, eth0]
  - [sudo, systemctl, restart, network]
  - [sudo, systemctl, mask, cloud-init-local, cloud-init, cloud-config, cloud-final]
  - [eject]

# Enable automatic package upgrade
package_upgrade: true

# Specify power state
power_state:
  delay: "+1"
  mode: reboot
  message: Rebooting after cloud-init
  timeout: 30
  condition: True
```

Variable used in the script	Value
host_name	hostname of the VM
host_name.*domain_name*	host name of the VM and domain name joined by a dot (.)
linux.username	Linux username
public_key	Public Key
vm_ip	IP address of the VM
vm_subnet_mask	Subnet mask of the VM
vm_gateway	Default gateway of the VM
dns1	Primary DNS address
dns2	Secondary DNS address
domain_name	Domain name

Script for setting up a static IP configuration (Ubuntu)

Unlike CentOS, Ubuntu uses *netplan* for network interface configuration, so you need to edit the /etc/netplan/50-cloud-init.yaml file and then run the netplan applycommand through cloud-init script as shown in the following example:

```
#cloud-config
apt_upgrade: true
repo_update: true
repo_upgrade: all

# Set the hostname
hostname: host_name
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2149

```
# User Authentication
users:
   - default
   - name: ubuntu
     groups: sudo
     shell: /bin/bash
     lock_passwd: false
     ssh-authorized-keys:
     - public_key
     sudo: ["ALL=(ALL) NOPASSWD:ALL"]
chpasswd:
   list: |
     ubuntu:user_password
   expire: false

# Assign static IP address
write_files:
   - path: /etc/netplan/50-cloud-init.yaml
     content: |
        network: |
           version: 2
           renderer: networkd
           ethernets:
              ens3:
                addresses: [vm_ip/netmask_bit]
                gateway4: vm_gateway
                nameservers:
                  addresses: [dns1,dns2]


# Run the commands to add packages and resize the root partition
runcmd:
   - netplan apply
packages:
  - git
  - wget
  - curl
  - unzip
  - tar
  - python3
  - cloud-guest-utils
growpart:
  mode: auto
  devices: ['/']
  ignore_growroot_disabled: false


# Specify power state
power_state:
  delay: "+1"
  mode: reboot
  message: Rebooting after cloud-init
  timeout: 30
  condition: True
```

Variable used in the script	Value
host_name	hostname of the VM
public_key	Public Key
user_password	Password for the user

Variable used in the script	Value
vm_ip	IP address of the VM
netmask_bit	Netmask bit such as 24 or 32
vm_gateway	Default gateway of the VM
dns1	Primary DNS address
dns2	Secondary DNS address

Script for setting up a static IP configuration (RHEL 9)

If your Linux distribution is using *NetworkManager* (as is the case with RHEL9), you need to use several nmcli commands in the cloud-init *runcmd* block to configure the static IPV 4 on your network interface as shown in the following example:

```
#cloud-config
apt_upgrade: true
repo_update: true
repo_upgrade: all

# Set the hostname
hostname: host_name

# User Authentication
users:
   - default
   - name: rhel
     groups: sudo
     shell: /bin/bash
     lock_passwd: false
     ssh-authorized-keys:
      - public_key
     sudo: ["ALL=(ALL) NOPASSWD:ALL"]
chpasswd:
   list: |
     rhel: user_password
   expire: false

# Assign static IP address
runcmd:
   - nmcli connection migrate
   - nmcli con down "System eth0"
   - nmcli con del "System eth0"
   - nmcli con add con-name "System eth0" ifname eth0 type ethernet
 ip4 vm_ip/netmask_bit gw4 vm_gateway ipv4.dns "dns1 dns2"
   - nmcli con up "System eth0"
   - nmcli general reload
   - nmcli connection reload

# Run the commands to add packages and resize the root partition
packages:
  - git
  - wget
  - curl
  - unzip
  - tar
  - python3
  - cloud-guest-utils
growpart:
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2151

```
  mode: auto
  devices: ['/']
  ignore_growroot_disabled: false


# Specify power state
power_state:
  delay: "+1"
  mode: reboot
  message: Rebooting after cloud-init
  timeout: 30
  condition: True
```

Variable used in the script	Value
host_name	hostname of the VM
public_key	Public Key
user_password	Password for the user
vm_ip	IP address of the VM
netmask_bit	Netmask bit such as 24 or 32
vm_gateway	Default gateway of the VM
dns1	Primary DNS address
dns2	Secondary DNS address

Customization of Windows Virtual Machines with System Preparation

To customize a Windows VM by using Sysprep, you need to perform the following tasks:

1. Create a reference image by using Sysprep.
2. Create a VM from the reference image.

You can also customize a VM when performing a fresh installation of Windows with an ISO file.

If you require unattended provisioning, keep the answer file ready, either saved locally or uploaded to a storage container on the cluster. Alternatively, you can create or paste the script in the web console. If you have files that need to be copied to the temporary ISO image, upload the files to a storage container on the cluster.

Preparing a VM to Create a Reference Image

Creating a reference image requires knowledge of Sysprep. For information about how to use Sysprep, see the Sysprep documentation on the Microsoft TechNet website.

About this task

To create a reference image, do the following:

Procedure

1. Log in to the web console by using the Nutanix credentials, and then browse to the VM dashboard.
2. Select the VM that you want to clone, click **Launch Console**, and then log in to the VM with administrator credentials.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2152

3. Configure Sysprep with the system cleanup action of your choice, specify whether or not you want to generalize the installation, and then choose to shut down the VM.

   - Open the command prompt as an administrator and navigate to the sysprep folder.

     ```
     cd C:\windows\system32\sysprep
     ```

   - Generalize the installation and then shut down the VM.

     ```
     C:\Windows\system32\sysprep>sysprep /generalize /shutdown /oobe
     ```

     The VM shuts down automatically.

     Note: Make sure to shut down the VM. Restarting the VM will result in the VM losing its generalized state and in Sysprep attempting to find an answer file that has not been provided yet. For the same reasons, until you have completed this procedure, do not start the VM.

4. Create a reference image from the VM by using Image Service. For more information, see Configuring Images on page 295.

Creating a Customized Virtual Machine from a Reference Image

About this task

To use a reference image, do the following:

Procedure

1. Log in to the web console by using the Nutanix credentials, and then browse to the VM dashboard.
2. Click **Create VM**, and then, in the **Create VM** dialog box, do the following:
   a. Specify a name for the VM and allocate resources such as vCPUs, memory, and storage.
   b. Click **Add new disk**, select the **Clone from Image Service** operation, and select the Windows reference image that you copied to Image Service.
   c. Click the **Custom Script** check box and specify how you want to customize the VM.

   For more information about creating a VM, see Creating a VM (AHV) on page 274.
3. In the VM dashboard, select the VM, and then click **Power On**.
   The VM is powered on and initialized based on the directives in the answer file. To create a reference image from the VM, use Image Service. For more information about Image Service, see Configuring Images.

Customizing a Fresh Installation

You can perform a fresh installation only if you attach an empty vDisk and an installation CD-ROM to the VM. If you specify an image from Image Service or ADSF, for use as a vDisk, the VM is created from that image, and the install is no longer a fresh install.

About this task

To customize a fresh installation of Windows by using Sysprep, do the following:

Procedure

1. Log in to the web console by using the Nutanix credentials, and then browse to the VM dashboard.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2153

2. Click **Create VM**, specify the details that are required for installing Windows on the new VM, and then do the following:

   a. Specify a name for the VM and allocate resources such as vCPUs, memory, and storage.

   b. In the **Disks** area, click the edit button that is provided against the default CD-ROM entry. In the **Update Disk** dialog box, select the operation (**Clone from ADSF File** or **Clone from Image Service**), and then specify the image that you want to use. Click **Update**.

   c. Click **Add new disk**. Allocate space for a new disk on a storage container, and then click **Add**.

   d. Click the **Custom Script** check box and specify how you want to customize the VM.

   For more information about creating a VM, see Creating a VM (AHV) on page 274.

3. In the VM dashboard, select the VM, and then click **Power On**.
   The VM is powered on and initialized based on the directives in the answer file. To create a reference image from the VM, use Image Service. For more information about Image Service, see Configuring Images.

VM High Availability in Acropolis

Acropolis uses the segment-based reservation method to enable VM high availability. The host-based reservation method is deprecated, and not supported.

If you have not enabled High Availability, in case of host failure, the VMs are restarted from the failed host to any available space on the other hosts in the cluster. Once the failed host joins the cluster again, VMs are migrated back to the host. This type of VM high availability is implemented without reserving any resources. Admission control is not enforced and hence there may not be sufficient capacity available to start all the VMs.

Note:

- Nutanix does not support VMs that are running with 100% remote storage for High Availability. The VMs must have at least one local disk that is present on the cluster.
- The VM HA does not reserve the memory for the non-migratable VMs. For information on how to check the non-migratable VMs, see Checking Live Migration Status of a VM in the *Prism Central Infrastructure Guide*.

The VM HA uses the Guarantee mode with segment-based reservation method.

In segment-based reservation, the cluster is divided into segments to ensure that enough space is reserved for any host failure. Each segment corresponds to the largest VM that is guaranteed to be restarted in case the failure occurs. The other factor is the number of host failures that can be tolerated. Using these inputs, the scheduler implements admission control to always have enough resources reserved so that the VMs can be restarted upon failure of any host in the cluster.

The segment size ensures that the largest VM can be powered on in HA failover when cluster is fully loaded (if the cluster is fully used except the reserved segments). The number of segments that is reserved is such a way that for each host enough resources are reserved to ensure that any host failure in the cluster is tolerated. Multiple VMs may fit into a segment. If anything changes in the cluster, the reservation is computed again. The total resources reserved for segments can be more than the resources used by running VMs. This implementation guarantees successful failover even in the case of fragmentation of segments. The actual number of reserved resources depends on the current load of the cluster, but it is typically at 1 to 1.25 times the resource usage on the most loaded host.

If the host enters maintenance mode (in case of host upgrade), you might not be protected against further host failures. Maintenance mode uses reservations made for HA for migrating VMs from the host. Although you are not protected against host failure if you have reservation for HA, hypervisor upgrade occurs without any difficulty because from the perspective of a user it is the same as host failure except that the VMs are migrated (instead of restarted) and hence no runtime state is lost. The HA status goes through the same states as it goes when the host failure had occurred.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2154

Fault Detection for High Availability

Acropolis version 6.1 (with minimum supported AHV version 20201105.2229) onwards, the fault detection mechanism for High Availability checks for the heartbeat of the management services on the host. If any one of the services are down, then the host is marked as disconnected.

In addition to this, the fault detection mechanism also performs the following health checks for the host:

- Root file system corruption
- Read-only root file system

If any of the above-mentioned health checks are affirmative, then the host is marked as disconnected.

If the host remains in the disconnected status for 40 seconds, the VMs running on the affected host are automatically restarted (based on the resource availability) .

You can view the alerts raised for any of the above-mentioned checks in the **Activity** > **Alerts** view in Prism UI.

Enabling High Availability for the Cluster

In Acropolis managed clusters, you can enable high availability for the cluster to ensure that VMs can be migrated and restarted on another host in case of failure.

About this task

After you enable high availability for the cluster, if a host failure occurs the cluster goes through following changes.

- OK: This state implies that the cluster is protected against a host failure.
- Healing: Healing period is the time that Acropolis brings the cluster to the protected state. There are two phases to this state. The first phase occurs when the host fails. The VMs are restarted on the available host. After restarting all the VMs if there are enough resources to protect the VM, the HA status of the cluster comes back to OK state. If this does not occur, the cluster goes into critical state. The second phase occurs when the host comes back from the failure. Once the host comes back from failure, no VMs are present on the host and hence during this healing phase restore locality task occurs (VMs are migrated back). Apart from restoring the locality of the VMs, the restore locality task ensures that the cluster is back to the same state before the HA failure. Once it is finished, the HA status is back to OK state.
- Critical: If the host is down, the HA status of the cluster goes into Critical state. This happens because the cluster cannot tolerate any more host failures. You have to ensure that you bring back the host so that your cluster is protected against any further host failures.

  > **Note:** On a less loaded cluster, it is possible for HA to go directly back to OK state if enough resources is reserved to protect another host failure. The start and migrate operations on the VMs are restricted in the Critical state because Acropolis continuously tries to ensure that the HA status is back to the OK state.

Procedure

1. Log in to the Prism Element web console.
2. Click the gear icon in the main menu and then select **Manage VM High Availability** in the **Settings** page.

   > **Note:** This option does not appear in clusters that do not support this feature.

   The **Manage VM High Availability** dialog box appears.
3. Check the **Enable HA Reservation** box and then click the **Save** button to enable.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2155

Nutanix Guest Tools

Nutanix Guest Tools (NGT) is a software package that comes bundled with AOS. You can install NGT in a guest virtual machine (VM) to enable advanced VM management functionalities provided by Nutanix.

For more information about NGT and the various NGT features, see Nutanix Guest Tools Overview in the *Prism Central Guide*.

Prism Element web console does not support automatic installation of NGT. You must log in to a VM to manually install NGT in that VM. Nutanix recommends that you use Prism Central to install NGT automatically in the VMs. For more information, see Installing NGT in the *Prism Central Guide*.

To set up NGT through the Prism Element web console, you must do the following:

1. Enable NGT for a VM in the Prism Element web console.

   When you enable NGT for a VM, Prism Element prepares the VM so that you can successfully install NGT and use the NGT features in that VM.
2. Mount the NGT installer (ISO disk file) in a VM.
3. Install NGT in a VM.

Enabling NGT and Mounting the NGT Installer in a VM

By default, the NGT feature is disabled for a guest VM running in a Nutanix cluster. To install and use the NGT feature in a VM, you must first enable the NGT feature (allow the installation and usage of NGT) for the VM, then mount the NGT installer in that VM using the Prism Element web console.

Before you begin

Ensure that all the NGT requirements are met. For more information, see Nutanix Guest Tools Requirements in the *Prism Central Guide*.

About this task

When you are enabling the NGT feature and mounting the NGT installer in a VM, you must also select the NGT applications (self-service restore, volume snapshot service, and application-consistent snapshots) that you want to use in that VM.

Perform the following steps to enable the NGT feature, mount the NGT installer, and select the NGT applications that you want to use in a VM using the Prism Element web console.

> **Note:** You can install both VMware guest tools and NGT in a VM because NGT is designed to install alongside VMware guest tools.

Procedure

1. Log in to the Prism Element web console.
2. In the dropdown list of the main menu, select **VM**.
3. From the VM page, select the **Table** view.
4. Select the VM for which you want to enable NGT and click **Manage Guest Tools**.
5. In the **Manage VM Guest Tools** window, select the **Enable Nutanix Guest Tools** checkbox.

   Selecting this checkbox displays the options to mount the NGT installer, and to select the NGT applications that you want to use in the VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2156

6. Perform the following in the indicated fields:

   a. **Mount Nutanix Guest Tools**: Select this checkbox to mount the NGT installer in the selected VM.

   b. **Self Service Restore (SSR)**: Select this checkbox to enable the self-service restore feature for Windows VMs.

      For more information about the self-service restore feature, see Self-Service Restore in the *Data Protection and Recovery with Prism Element* guide.

   c. **Volume Snapshot Service / Application Consistent Snapshots (VSS)**: This checkbox is selected by default when you select the **Enable Nutanix Guest Tools** checkbox.

      This feature enables the Nutanix native in-guest Volume Snapshot Service (VSS) agent to take application-consistent snapshots for all the VMs that support VSS. For more information, see Conditions for Application-consistent Snapshots in the *Data Protection and Recovery with Prism Element* guide.

   d. Click **Submit**.

      Prism Element enables the NGT feature, mounts the NGT installer, and attaches the NGT installation media with the volume label NUTANIX_TOOLS to the selected VM.

7. To verify whether NGT is enabled and the NGT installer is mounted successfully on a guest VM, do the following from the Prism Element web console:

   a. In the dropdown list of the main menu, select **VM**.

   b. From the VM page, select the **Table** view.

   c. Select the desired VM.

   d. Under **VM DETAILS**, check the **NGT Enabled**, and **NGT Mounted** fields.

      If NGT is enabled and the NGT installer is mounted successfully, the respective fields display the status **Yes**.

      Note:

      - NGT is not enabled on a cloned VM by default. For more information, see Enabling NGT and Mounting the NGT Installer on Cloned VMs.
      - For information about troubleshooting any NGT-related issues, see KB-3741.

What to do next

Install NGT in the guest VM by following the instructions in NGT Installation.

NGT Installation

Prism Element web console does not support automatic installation of NGT. You must log in to a VM to manually install NGT in that VM.

Note: You cannot install NGT on VMs created on storage containers with replication factor 1.

Installing NGT on a Windows VM

Before you begin

Ensure that the following prerequisites are met:

- All the NGT requirements are met. For more information, see Nutanix Guest Tools Requirements in the *Prism Central Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2157

- NGT is enabled in the selected VM and the NGT installer is mounted on the selected VM. For more information, see Enabling NGT and Mounting the NGT Installer in a VM.

Procedure

1. Log in to the Windows VM.
2. Open File Explorer and click the CD drive with the NUTANIX_TOOLS label from the left navigation pane.
3. From the right pane that displays all the files and sub-folders in the drive, double-click the setup.exe file.

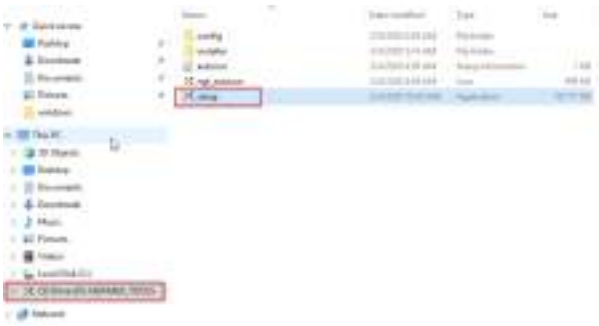


Figure 42: Start NGT Installation on Windows

> **Note:** If you mount the NGT installer while the VM is powered off, the CD drive might not display the NUTANIX_TOOLS label after you power on the VM. You must open the CD drive, and double-click the setup.exe file.

4. Accept the license agreement and follow the prompts to install NGT in the virtual machine.
   A Setup Successful message appears if NGT is successfully installed.
5. After you install NGT in a Windows VM, the Nutanix Guest Agent (NGA) service in the VM starts periodic communication with the CVM. To verify whether the NGA service is communicating with the CVM, log in to the CVM and run the following command:

   ```
   nutanix@cvm$ nutanix_guest_tools_cli list_vm_tools_entities include_vm_info=true
    vm_name=vm-name
   ```

   Replace *vm-name* with the name of the Windows VM.

   In the command output, communication_link_active = true indicates that the NGA is communicating with the CVM.

   > **Note:** For information about troubleshooting any NGT-related issues, see KB-3741.

Installing NGT on a Windows VM (Silent Install)

The NGT installer package allows you to manually install NGT on a Windows VM, in the background, without affecting normal VM operations.

Before you begin

Ensure that the following prerequisites are met:

- All the NGT requirements are met. For more information, see Nutanix Guest Tools Requirements in the *Prism Central Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2158

- NGT is enabled in the selected VM and the NGT installer is mounted on the selected VM. For more information, see Enabling NGT and Mounting the NGT Installer in a VM.

About this task

Perform the following procedure to install NGT using the NGT silent installer package.

Note:

- Add the commands mentioned in the following procedure to a custom script and run the script to install NGT on multiple Windows VMs. However, you might need to restart the VM after NGT is installed for the updated functionalities to be available in the VM.
- For information about the contents included in the NGT silent installer package, see Nutanix Guest Tools Overview in the *Prism Central Guide*.

Procedure

1. Open the command prompt and go to the drive on which the NGT installer is mounted.
2. Install NGT using the installer package by running either of the following commands:

   » `$ setup.exe /quiet ACCEPTEULA=yes /norestart`

   Use this command to ensure that VMs are not restarted after installing NGT.

   Note: This command updates the Nutanix VirtIO drivers to the latest version, but the updated functionality of the VirtIO drivers is available only after a VM restart. For more information about VirtIO drivers, see Nutanix VirtIO for Windows in *AHV Administration Guide*.

   » `$ setup.exe /quiet ACCEPTEULA=yes`

   Use this command to restart the VM and for all the updated VirtIO driver functionalities to be available in the VM. For more information about VirtIO drivers, see Nutanix VirtIO for Windows in *AHV Administration Guide*.

   By default, NGT logs are generated in **Event Viewer** and in the %TEMP% directory starting with *Nutanix_Guest_Tools_`timestamp`*. Event Viewer log files are created for all the components as part of the NGT installation.

   Note:

   - NGT installation on guest VMs running on AHV might require a VM restart if the VirtIO drivers are updated during the installation whereas NGT installation on guest VMs running on ESXi does not require a VM restart because the installed VirtIO drivers are not active until the VM moves to AHV. For more information about VirtIO drivers, see Nutanix VirtIO for Windows in *AHV Administration Guide*.
   - The NGT installer has some built-in checks (for example, if the VSS service is disabled or if KB2921916 Windows update is installed inside Windows 7/Windows Server 2008R2) that are treated as warnings during an interactive installation of NGT. However, these checks are deemed as errors during a silent installation. To ignore these errors and proceed with the silent installation, use the `IGNOREALLWARNINGS=yes` flag. For example, drive:\> setup.exe /quiet ACCEPTEULA=yes IGNOREALLWARNINGS=yes.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2159

3. (Optional) If you want the NGT logs to be generated in a location other than the %TEMP% directory, install NGT by running the following command.

```
$ setup.exe /quiet ACCEPTEULA=yes -log log_path
```

Replace *log_path* with the path where you want to create the log files.

Logs are generated in the path that you provide. Ensure that the path you provide has the necessary write permissions. Also, some events are added to the Windows Application Event Log.

> **Note:** For information on troubleshooting any NGT related issues, see KB-3741 available on the Nutanix support portal.

4. After you install NGT in a Windows VM, the Nutanix Guest Agent (NGA) service in the VM starts periodic communication with the CVM. To verify whether the NGA service is communicating with the CVM, log in to the CVM and run the following command:

```
nutanix@cvm$ nutanix_guest_tools_cli list_vm_tools_entities include_vm_info=true
 vm_name=vm-name
```

Replace *vm-name* with the name of the Windows VM.

In the command output, communication_link_active = true indicates that the NGA is communicating with the CVM.

> **Note:** For information about troubleshooting any NGT-related issues, see KB-3741.

Installing NGT on a Linux VM

Before you begin

Ensure that the following prerequisites are met:

- All the NGT requirements are met. For more information, see Nutanix Guest Tools Requirements in the *Prism Central Guide*.
- NGT is enabled in the selected VM and the NGT installer is mounted on the selected VM. For more information, see Enabling NGT and Mounting the NGT Installer in a VM.

About this task

Some Linux deployments auto-discover the CD-ROM and mount the CD-ROM appropriately. Some of the following steps might be optional for your VM.

Procedure

1. Log in to the Linux VM.
2. Run one of the following to determine the device in which the NUTANIX_TOOLS CD is inserted:
   - `$ blkid -L NUTANIX_TOOLS`
   - `$ lsblk -o NAME, LABEL`

   The second command displays a list of directories. You must look for a directory with the label NUTANIX_TOOLS.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2160

3. Create a temporary directory if a target mount point does not exist and mount the content of the CD in the temporary directory that you created by running the following command:

```
$ sudo mount /dev/device target-mount-point /mnt
```

Replace *device* with the device that you determined in Step 2, for example, sr0 or sr1, and replace *target-mount-point* with the name of the directory where the content of the CD should be mounted.

> **Note:** On some Linux distributions, it is appropriate to use /mnt or a specific directory created under /mnt.

4. Install NGT by running the following command:

```
$ sudo python target-mount-point/installer/linux/install_ngt.py --operation install
```

Replace *target-mount-point* with the name of the directory where the content of the CD is mounted.

Output similar to the following is displayed.

```
[root@localhost linux]# python install_ngt.py --operation install
Downloading packages:
Public key for nutanix-guest-agent-4.0-1.x86_64.rpm is not installed
Retrieving key from file:///tmp/cdrom/installer/linux/ngt_rpm_installer/RPM-GPG-
PUBLIC-KEY
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Pre: RPM is getting installed
Installing : nutanix-guest-agent-4.0-1.x86_64                              1/1
Post: RPM is getting installed.
Running installer utility script.
INFO: Setting up Nutanix Guest Tools - VM mobility drivers.
INFO: Successfully set up Nutanix Guest Tools - VM mobility drivers.
INFO: Creating desktop shortcuts...
Restarting ngt_guest_agent.service systemctl service...
ngt_guest_agent.service service restart done.
Restarting ngt_self_service_restore.service systemctl service...
ngt_self_service_restore.service service restart done.
  Verifying: nutanix-guest-agent-4.0-1.x86_64                              1/1
Installed:
  nutanix-guest-agent.x86_64 0:4.0-1
[root@localhost linux]#
```

5. Verify whether the Nutanix Guest Agent (NGA) service is installed in the VM by running the command based on your package management tool.

The following is an example of the command for the YUM package management tool.

```
$ sudo yum list installed | grep 'nutanix-guest-agent'
```

Output similar to the following is displayed.

```
[root@localhost linux]# sudo yum list installed | grep 'nutanix-guest-agent'
Failed to set locale, defaulting to C
nutanix-guest-agent.x86_64          4.0-1                    @nutanix-
ngt-20230524223422
[root@localhost linux]#
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2161

6. After you install NGT in a Linux VM, the Nutanix Guest Agent (NGA) service in the VM starts periodic communication with the CVM. To verify whether the NGA service is communicating with the CVM, log in to the CVM and run the following command:

```
nutanix@cvm$ nutanix_guest_tools_cli list_vm_tools_entities include_vm_info=true
 vm_name=vm-name
```

Replace *vm-name* with the name of the Linux VM.

In the command output, communication_link_active = true indicates that the NGA communicates with the CVM.

> **Note:** For information about troubleshooting any NGT-related issues, see KB-3741.

Manage Bulk Operations for NGT

You can install or upgrade NGT in bulk on multiple guest virtual machines (VMs) using third-party endpoint management tools, such as Microsoft Intune or HCL BigFix, or automation tools, such as Ansible. Using these management tools, you can also remove NGT in bulk from guest VMs.

Bulk installation of NGT is supported on guest VMs running AOS 6.7 or later versions only.

The Nutanix Support portal lists the following NGT installer files:

- EXE file for Windows OS
- TGZ file for RPM-based Linux OS
- TGZ file for DEB-based Linux OS
- Nutanix NGT GnuPG public key

Download the latest installer files to install or upgrade NGT in bulk.

> **Note:** Bulk installation of NGT using third-party endpoint management tools does not require Prism Element web console. However, you must enable and mount NGT in guest VMs using Prism Element web console after installing NGT in VMs. For more information, see Enable and Configure NGT.

Prepare the NGT installation files for Distribution

You can install NGT using the installer files available in the Nutanix Support portal in a single VM or, in bulk, on multiple VMs. When you prepare to install NGT in bulk on multiple VMs, download the installer files and make them available for use by the third-party endpoint management tool deployed at your site. The instructions in this document assume that the third-party endpoint management tool deployed at your site requires that you host the NGT installer files on a web server.

Hosting the files for Windows VMs

Before you begin

Ensure that the NGT version is compatible with the AOS version installed in your cluster.

Procedure

1. Go to the Nutanix Support portal, select **Downloads** > **NGT**, and download the *nutanix-guest-agent-<version>.exe* installer file for Windows, which matches the AOS version installed in your clusters.
2. Host this installation file directly on the web server.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2162

Hosting the files for Red Hat Package Manager (RPM) based VMs

Before you begin

Ensure that the NGT version is compatible with the AOS version installed in your cluster.

Procedure

1. Go to the Nutanix Support portal, select **Downloads** > **NGT**, and download the *nutanix-guest-agent-rpm-<version>.tar.gz* installer file for RPM-based distributions, which matches the AOS version installed in your clusters.
2. Extract the *nutanix-guest-agent-rpm-<version>.tar.gz* file, and host the *NUTANIX-NGT-GPG-KEY* file and the *ngt_repo* directory on the web server.

Hosting the files for Debian (DEB) based VMs

Before you begin

Ensure that the NGT version is compatible with the AOS version installed in your cluster.

Procedure

1. Go to the Nutanix Support portal, select **Downloads** > **NGT**, and download the *nutanix-guest-agent-deb-<version>.tar.gz* installer file for DEB-based distributions, which matches the AOS version installed in your clusters.
2. Extract the *nutanix-guest-agent-deb-<version>.tar.gz* file, and host the i386 and amd64 directories on the web server.
3. (Optional) Perform the following steps to verify the DEB installer packages against the detached signatures using the *NUTANIX-NGT-GPG-KEY* file:
   a. Run the following command to import the public key:

      ```
      $ gpg --import NUTANIX-NGT-GPG-KEY
      ```

      The following is an example.

      ```
      $ gpg --import NUTANIX-NGT-GPG-KEY
      gpg: key 42DBF8BB: public key "Nutanix, Inc. (NGT Packaging)
       <security@nutanix.com>" imported
      gpg: Total number processed: 1
      gpg:               imported: 1  (RSA: 1)
      ```

   b. Run the following command to verify the DEB installer packages against the detached signatures:

      ```
      $ gpg --verify os-arch/nutanix-guest-agent.deb.asc os-arch/nutanix-guest-
      agent_version-1_os-arch.de
      ```

      Replace *os-arch* with the architecture of the OS of guest VM, and *version* with the NGA version.

      The following is an example.

      ```
      $ gpg --verify i386/nutanix-guest-agent.deb.asc i386/nutanix-guest-
      agent_4.0-1_i386.deb
      gpg: Signature made Wed 24 May 2023 01:46:29 PM UTC using RSA key ID 42DBF8BB
      gpg: Good signature from "Nutanix, Inc. (NGT Packaging) <security@nutanix.com>"
      gpg: WARNING: This key is not certified with a trusted signature!
      gpg:          There is no indication that the signature belongs to the owner.
      Primary key fingerprint: D8B0 18BD CFEB 774C D157  F0A5 11B1 600F 42DB F8BB
      ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2163

Install NGT in Bulk on Multiple VMs

You can install NGT in bulk on multiple Windows and Linux guest VMs using the NGT installer files available in the Nutanix Support portal.

Installing NGT in Bulk on Windows VMs

Before you begin

- Ensure that the cluster meets all NGT requirements. For more information, see Nutanix Guest Tools Requirements in the *Prism Central Infrastructure Guide*.
- Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.
- Review the end user license agreement (EULA) for Nutanix Guest Tools using a manual installation because the following installation procedure requires you to accept the EULA automatically.

Procedure

1. Configure the third-party endpoint management tool deployed at your site to distribute the *nutanix-guest-agent-<version>.exe* file to the VMs where NGT is installed.

   For more information, see the tool-specific documentation.

2. Configure the third-party endpoint management tool to install NGT by running one of the following commands:

   » `C:\ngtinstaller> nutanix-guest-agent-version.exe /quiet ACCEPTEULA=yes /norestart`

   Replace `version` with the NGA version.

   Use this command to ensure that VMs do not restart after you install NGT.

   > **Note:** This command might update the Nutanix VirtIO drivers if no Nutanix VirtIO drivers are installed or if a newer version is available, but the updated functionality of the VirtIO drivers is available only after a VM restart.

   » `C:\ngtinstaller> nutanix-guest-agent-version.exe /quiet ACCEPTEULA=yes`

   Replace `version` with the NGA version.

   Use this command to automatically restart the VM and to make all the updated VirtIO driver functionalities to be available in the VM.

3. (Optional) To generate the NGT logs in a location other than the %TEMP% directory, install NGT by running the following command.

   `C:\ngtinstaller> nutanix-guest-agent-version.exe /quiet ACCEPTEULA=yes /log log_file`

   Replace `version` with the NGA version, and `log_file` with the filename to write the logs.

   Ensure that the directory containing the filename that you provide has the necessary write permissions. Also, the installation process adds some events to the Windows application event log.

What to do next

After successful installation, enable and configure NGT in guest VMs. For more information, see Enable and Configure NGT.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2164

Installing NGT in Bulk on Linux VMs

About this task

This sample procedure provides steps to install NGT on Red Hat Package Manager (RPM) based operating systems. Use this procedure as a template to install NGT on Debian-based operating systems.

Before you begin

- Ensure that the cluster meets all NGT requirements. For more information, see Nutanix Guest Tools Requirements in the *Prism Central Infrastructure Guide*.
- Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.

Procedure

1. To verify the package signatures, configure the third-party endpoint management tool deployed at your site to install the NUTANIX-NGT-GPG-KEY file on RPM-based operating systems.

   For more information, see the tool-specific documentation.

2. Configure the third-party endpoint management tool to set up the repositories.

   For more information, see the tool-specific documentation.

   For example, guest VMs running RedHat 8.x distribution might need a repository configuration in /etc/yum.repos.d/nutanix-guest-tools.repo similar to the following configuration:

   ```
   [NutanixGuestTools]
   name=Nutanix Guest Tools
   baseurl=http://local-web-server/ngt_repo
   enabled=1
   gpgcheck=1
   gpgkey=http://local-web-server/RPM-GPG-PUBLIC-KEY
   repo_gpgcheck=0
   ```

   Replace `local-web-server` with the name of the web server used to distribute the NGT installer files as described in Preparing the NGT installation files for the Distribution.

3. Configure the third-party endpoint management tool to install the Nutanix guest agent package by running the package manager-specific install command.

   For example, the yum install -y nutanix-guest-agent command installs Nutanix guest agent package using the yum package manager for RedHat-based distributions.

   ```
   [nutanix@localhost ~]$ yum install -y nutanix-guest-agent
   ```

   For information about the install command specific to the package manager at your site, see the package manager-specific documentation.

What to do next

After successful installation, enable and configure NGT in guest VMs. For more information, see Enable and Configure NGT.

Enable and Configure NGT

Use Prism Element web console to enable and configure NGT in VMs so that you can use the NGT applications such as self-service restore, volume snapshot service, and application-consistent snapshots. The initial configuration of NGT requires mounting an ISO into the CD-ROM drive of guest VMs. The NGT agent detects the ISO and performs the initial configuration, making connections to the CVM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2165

Enabling and Configuring NGT using the Prism Element Web Console

Procedure

- Mount NGT on guest VMs by performing Step 1 to Step 6 in Enabling NGT and Mounting the NGT Installer in a VM on page 306.

What to do next

The Nutanix Guest Agent (NGA) service in the VMs starts periodic communication with the CVM. To verify whether the NGA service is communicating with the CVM, log in to the CVM and run the following command:

```
nutanix@cvm$ nutanix_guest_tools_cli list_vm_tools_entities include_vm_info=true
 vm_name=vm-name
```

Replace *vm-name* with the name of one of the VMs.

Enabling and Configuring NGT using CVM (Config-only Mount)

The config-only mount method reduces the size of the NGT ISO mounted on the guest VM by not including the NGT installers. Therefore, it is less prone to scalability issues (for example, the ISO stored on disk is smaller) and might attach faster to the guest VM.

About this task

Nutanix recommends config-only mount when you enable NGT on a large number of VMs.

Procedure

1. Log in to the CVM using SSH and (admin, nutanix, or root) access.
2. Run the following command to enable NGT in the guest VM.

   ```
   nutanix@cvm$ nutanix_guest_tools_cli create_vm_tools_entity vm_uuid
    guest_tools_enabled=true
   ```

   Replace *vm_uuid* with the UUID of the VM.

   > **Note:** To enable SSR and VSS while enabling NGT, use the following command:
   >
   > ```
   > nutanix@cvm$ nutanix_guest_tools_cli create_vm_tools_entity vm_uuid
   >  guest_tools_enabled=true file_level_restore=true vss_snapshot=true
   > ```
   >
   > Replace *vm_uuid* with the UUID of the VM.

3. Run the following command to mount the NGT configuration updates in the guest VM.

   ```
   nutanix@cvm$ nutanix_guest_tools_cli mount_guest_tools vm_uuid config_only=true
   ```

   Replace *vm_uuid* with the UUID of the VM.

   Output similar to the following is displayed.

   ```
   nutanix@cvm$ nutanix_guest_tools_cli mount_guest_tools aca91d9b-8a31-47ec-a9b7-
   dfc613115748 config_only=true
   2023-05-26 06:11:51,809Z:30612(0x7f33d60d4340):ZOO_INFO@zookeeper_init@994:
    Initiating client connection, host=zk1:9876 sessionTimeout=20000
    watcher=0x7f33e59dec10 sessionId=0 sessionPasswd=<null> context=0x7ffd1271ba00
    flags=0
   2023-05-26 06:11:51,813Z:30612(0x7f33d57ff700):ZOO_INFO@zookeeper_interest@1941:
    Connecting to server 10.46.27.73:9876
   ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2166

```
2023-05-26 06:11:51,813Z:30612(0x7f33d57ff700):ZOO_INFO@zookeeper_interest@1978:
 Zookeeper handle state changed to ZOO_CONNECTING_STATE for socket [10.46.27.73:9876]
2023-05-26 06:11:51,814Z:30612(0x7f33d57ff700):ZOO_INFO@check_events@2187: initiated
 connection to server [10.46.27.73:9876]
2023-05-26 06:11:51,814Z:30612(0x7f33d57ff700):ZOO_INFO@check_events@2235: session
 establishment complete on server [10.46.27.73:9876], sessionId=0x188458c12d08959,
 negotiated timeout=20000
2023-05-26 06:11:51,919Z:30612(0x7f33d60d4340):ZOO_INFO@zookeeper_close@3108: Closing
 zookeeper sessionId=0x188458c12d08959 to [10.46.27.73:9876]

mount_result : kNoError
task_uuid : d5f7eb25-9e3d-4c7d-ade9-5d25e1e737d5
nutanix@cvm$
```

What to do next

The Nutanix Guest Agent (NGA) service in the VMs starts periodic communication with the CVM. To verify whether the NGA service is communicating with the CVM, log in to the CVM and run the following command:

```
nutanix@cvm$ nutanix_guest_tools_cli list_vm_tools_entities include_vm_info=true
 vm_name=vm-name
```

Replace *vm-name* with the name of one of the VMs.

Upgrade NGT in Bulk on Multiple VMs

You can upgrade NGT in bulk on multiple Windows and Linux guest VMs using the NGT installer file available in the Nutanix Support portal.

Upgrading NGT in Bulk on Windows VMs

Before you begin

- Ensure that the NGT version is compatible with the AOS version installed in your cluster. For more information, see the NGT section in the *Compatibility and Interoperability Matrix*.
- Ensure that the cluster meets all NGT requirements. For more information, see Nutanix Guest Tools Requirements in the *Prism Central Infrastructure Guide*.
- Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.

Procedure

- Perform Step 1 to Step 3 in Installing NGT in Bulk on Windows VMs.

  The installer detects that an existing NGT version is already present on the VM and performs an upgrade.

Upgrading NGT in Bulk on Linux VMs

About this task

This sample procedure provides steps to upgrade NGT on Red Hat Package Manager (RPM) based operating systems. Use this procedure as a template to upgrade NGT on Debian-based operating systems.

Before you begin

- Ensure that the NGT version is compatible with the AOS version installed in your cluster. For more information, see the NGT section in the *Compatibility and Interoperability Matrix*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2167

- Ensure that the cluster meets all NGT requirements. For more information, see Nutanix Guest Tools Requirements in the *Prism Central Infrastructure Guide*.
- Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.

Procedure

1. To verify the package signatures, configure the third-party endpoint management tool deployed at your site to install the NUTANIX-NGT-GPG-KEY file on RPM-based operating systems.

   For more information, see the tool-specific documentation.

2. Configure the third-party endpoint management tool to set up the repositories.

   For more information, see the tool-specific documentation.

   For example, guest VMs running RedHat 8.x distribution might need a repository configuration in /etc/yum.repos.d/nutanix-guest-tools.repo similar to the following configuration:

   ```
   [NutanixGuestTools]
   name=Nutanix Guest Tools
   baseurl=http://local-web-server/ngt_repo
   enabled=1
   gpgcheck=1
   gpgkey=http://local-web-server/RPM-GPG-PUBLIC-KEY
   repo_gpgcheck=0
   ```

   Replace *local-web-server* with the name of the web server used to distribute the NGT installer files as described in Preparing the NGT installation files for the Distribution.

3. Configure the third-party endpoint management tool to upgrade the Nutanix guest agent package by running the package manager-specific upgrade command.

   For example, the yum update -y nutanix-guest-agent command upgrades Nutanix guest agent package using the yum package manager for RedHat-based distributions.

   ```
   [nutanix@localhost ~]$ yum update -y nutanix-guest-agent
   ```

   For information about the upgrade command specific to the package manager at your site, see the package manager-specific documentation.

Uninstall NGT in Bulk from Multiple VMs

You can uninstall NGT in bulk from guest VMs using the third-party management tool deployed at your site.

> **Note:** Before uninstalling NGT from a guest VM, ensure the communication link between guest VM and CVM remains active. The CVM displays that NGT is uninstalled only if the communication between CVM and guest VM is active during the uninstallation. If the communication link is down, CVM continues to display that NGT is installed on the guest VM even after the successful uninstallation of NGT. For information about how to verify that the communication link is active, see Step 4 in Enabling NGT and Mounting the NGT Installer on Cloned VMs on page 319.

Uninstalling NGT from Windows VMs

About this task

When you install NGT in a Windows VM, NGT registers an uninstaller in the VM that can be accessed manually using Add/Remove Programs in the Windows Control Panel. This uninstaller can also be used by a third-party endpoint management tool to remove NGT from the VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2168

Before you begin

Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.

Procedure

- Configure the third-party endpoint management tool to uninstall the Nutanix Guest Agent package using the uninstaller registered with Add/Remove Programs in the Windows Control Panel.

  For more information, see the tool-specific documentation or Microsoft Windows documentation.

Uninstalling NGT from Linux VMs

About this task

This sample procedure provides steps to remove NGT on Red Hat Package Manager (RPM) based operating systems. Use this procedure as a template to remove NGT on Debian-based operating systems.

Before you begin

Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.

Procedure

- Configure the third-party endpoint management tool to uninstall the Nutanix guest agent package in bulk by running the package manager-specific removal command.

  For example, the yum remove -y nutanix-guest-agent command uninstalls Nutanix guest agent package using the yum package manager for RedHat-based distributions.

  ```
  [nutanix@localhost ~]$ yum remove -y nutanix-guest-agent
  ```

  For information about the removal command specific to the package manager at your site, see the package manager-specific documentation.

Enabling NGT and Mounting the NGT Installer on Cloned VMs

If you cloned a VM or multiple VMs from a single VM (master VM), you must enable NGT and mount the NGT installer on the cloned VM to use the NGT feature in the VM.

Before you begin

Ensure the following before you perform this task:

- NGT is installed in the master VM.
- The required number of VMs were cloned from the master VM.

About this task

Perform the following steps to enable NGT and mount the NGT installer on cloned VMs.

> **Note:** After you perform the following steps, you do not need to separately install NGT on the cloned VMs.

Procedure

1. Enable NGT and mount the NGT installer on the cloned VM by following the instructions mentioned in Steps 1 through 6 of Enabling NGT and Mounting the NGT Installer in a VM.
2. Power on the cloned VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2169

3. (Optional) If you enable NGT and mount the NGT installer while the cloned VMs are powered on, do either of the following:

   » Restart the Nutanix Guest Agent (NGA) service.

   For Linux VMs – Run the $ sudo service ngt_guest_agent restart command or the $ sudo systemctl restart ngt_guest_agent command.

   For Windows VMs – Run the $ net stop “Nutanix Guest Agent” and $ net start “Nutanix Guest Agent” commands.

   » Power cycle the cloned guest VMs.

4. Verify whether the NGA service is communicating with the CVM by logging in to the CVM and running the following command:

```
nutanix@cvm$ nutanix_guest_tools_cli list_vm_tools_entities include_vm_info=true
 vm_name=vm-name
```

   Replace *vm-name* with the name of the guest VM.

   In the command output, communication_link_active = true indicates that the NGA is communicating with the CVM.

> **Note:** For information on troubleshooting any NGT related issues, see KB-3741 available on the Nutanix support portal.

Automatic Regeneration of NGT Certificates

The NGT service inside the controller VM (CVM) automatically reissues an updated NGT client certificate to the guest VM before its expiry date.

NGT client certificates have a fixed expiry of less than three years. The guest VM stops communicating with the CVM when the client certificate expires. When the certificate has less than a year remaining until the expiry date, the guest VM connects to the CVM, updates the certificates and continues IP-based communication with the CVM using the new or updated certificates.

Requirements

Following are the requirements for automatic regeneration of NGT client certificates:

- Ensure that the cluster is running AOS 7.0 or later and the guest VM is running NGT 4.2 or later versions.
- Ensure that the guest VM is powered on and the connection between the CVM and the guest VM is active.

The NGT client certificates are not automatically regenerated if the guest VM is powered off or if the communication link between CVM and guest VM is down. For information on how to regenerate the client certificates manually, see Manually Regenerating NGT Certificates for Guest VMs on page 320. To view the list of certificates that are not regenerated, see Step 3 in Manually Regenerating NGT Certificates for Guest VMs on page 320.

Manually Regenerating NGT Certificates for Guest VMs

Regenerate NGT client certificates manually if the guest VM cannot regenerate the certificates automatically.

About this task

To regenerate the client certificates, follow these steps:

Procedure

1. Log in to the Prism Element web console.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2170

2. Select **Alerts** from the drop-down list on the left of the main menu.
   The **Alerts** dashboard opens displaying all the alerts in the cluster.

3. Identify the alert that has **NGT client certificates expiring** in the **Title** with the **Severity** status as **Critical** or **Warning**.

   The **Alerts** dashboard displays the severity status as **Critical** if the certificate is expiring in less than seven days and as **Warning** if the certificate is expiring in less than 45 days. It also displays the name and UUID of the guest VMs for which the certificates are expiring in the **Source Entity** field.

4. Click the name of the guest VM in the **Source Entity** field.
   The system opens the **VM** dashboard displaying the details of the guest VM.

5. Click **Manage Guest Tools**.
   The system displays the **Manage Guest Tools** dialog box.

6. Select the **Mount Nutanix Guest Tools** checkbox.

7. Click **Submit**.
   The system generates a new certificate for the guest VM.

   > **Note:** After regenerating the NGT client certificates, the guest VM might take a few minutes to communicate with the CVM. To force the guest VM to communicate with the CVM immediately, restart the NGA service.

What to do next

Check the **Alerts** dashboard in the Prism Element web console and ensure that there are no guest VMs with expired certificates.

Upgrading NGT

After you upgrade AOS, you must reinstall NGT to upgrade NGT to the latest version.

Perform the following steps to upgrade NGT.

> **Note:** Unless you upgrade AOS, you cannot upgrade NGT.

1. Mount the NGT installer.

   For more information, see Enabling NGT and Mounting the NGT Installer in a VM on page 306.
2. Install NGT.

   For more information, see NGT Installation on page 307.

Reconfiguring NGT

If you reconfigure the cluster IP address, NGT loses connection with the CVM. You must reconfigure NGT to reestablish the connection.

To reconfigure NGT, mount the NGT installer. For more information, see Enabling NGT and Mounting the NGT Installer in a VM on page 306.

After you mount the NGT ISO, NGA fetches the latest configuration (new cluster IP address) mounted in the guest VM. The guest VM can now use the new IP address to communicate with the cluster.

> **Note:**
>
> - It takes a few minutes for the guest VM to communicate with the cluster because this is an asynchronous operation.
> - For information about troubleshooting any NGT-related issues, see KB-3741.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2171

Uninstalling and Removing Nutanix Guest Tools

About this task

Do the following to remove NGT from the VM completely.

- Uninstall NGT from the guest VM.
- Verify whether the NGT information of the guest VM is removed from the CVM.
- If the NGT information of the guest VM is not removed from the CVM, remove it from the CVM using nCLI.

Procedure

1. Uninstall NGT.

   Note: Before you uninstall NGT from a guest VM, ensure that the communication link between the guest VM and the CVM is active. If the communication link is down, the CVM continues to display that NGT is installed on the guest VM even after the successful uninstallation of NGT. The CVM displays that NGT is uninstalled only after the communication between the CVM and the guest VM is restored. For information about how to verify that the communication link is active, see Step 4 in Enabling NGT and Mounting the NGT Installer on Cloned VMs.

   - **Windows VM**

     You can uninstall NGT from a Windows VM through Control Panel. Log in to the Windows VM and perform the following.

     1. Navigate to **Control Panel** > **Programs** > **Programs and Features**.
     2. Select the **Nutanix Guest Tools** service.
     3. Click **Uninstall**.

        An Uninstall Successfully Completed message appears on successfully uninstalling NGT.

     (Optional) You can uninstall NGT from a Windows VM using the PowerShell command. Log in to the Windows VM and perform the following.

     1. Run the following command from Windows PowerShell to generate the output string required to uninstall NGT.

        ```
        $ Get-ChildItem -Path HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion
        \Uninstall, HKLM:\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion
        \Uninstall | Get-ItemProperty | Where-Object {$_.DisplayName -match "Nutanix
        ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2172

```
 Guest Tools" } | Select-Object -Property QuietUninstallString | Out-String -
Width 4096
```

Result: An output string appears on the console. For example, `"C:\ProgramData\Package Cache\{3cfa83ac-a36f-49f1-ad23-3a51c0e6964a}\NutanixGuestTools.exe" /uninstall /quiet`.

2. Run the output string that is generated to uninstall NGT.

```
"C:\ProgramData\Package Cache\{3cfa83ac-a36f-49f1-
ad23-3a51c0e6964a}\NutanixGuestTools.exe" /uninstall /quiet
```

> **Note:** If you do not want to restart the guest VM after uninstalling NGT, append /norestart to the generated output string, and run the updated output string. For example,
>
> ```
> "C:\ProgramData\Package Cache\{3cfa83ac-a36f-49f1-
> ad23-3a51c0e6964a}\NutanixGuestTools.exe" /uninstall /quiet /norestart
> ```

> **Tip:** After uninstalling NGT from a Windows VM, ensure the following entries that are created during NGT installation, are removed from the VM registry.
>
> ```
> HKEY_LOCAL_MACHINE\SOFTWARE\Nutanix HKEY_LOCAL_MACHINE\SOFTWARE\Nutanix
> \VSS\1.0 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Nutanix
> Guest Agent HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Nutanix
> Self Service Restore Gateway HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
> \Services\EventLog\Application\Nutanix HKEY_LOCAL_MACHINE\SYSTEM
> \CurrentControlSet\Services\EventLog\Application\Nutanix Guest Agent
> HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application
> \Nutanix Self Service Restore Gateway HKEY_LOCAL_MACHINE\SYSTEM
> \CurrentControlSet\Services\VSS
> ```

- **Linux VM**

  Log in to the Linux VM and run the following command.

  ```
  $ sudo sh /usr/local/nutanix/ngt/python/bin/uninstall_ngt.sh
  ```

  Output similar to the following is displayed.

  ```
  $ sudo sh /usr/local/nutanix/ngt/python/bin/uninstall_ngt.sh
  Stopping ngt_guest_agent.service systemctl service...
  ngt_guest_agent.service service stopped.
  Stopping ngt_self_service_restore.service systemctl service...
  ngt_self_service_restore.service service stopped.
  NGA is getting uninstalled.
  Removing Desktop icon and shortcuts.
  Notify CVM of agent uninstallation.
  Successfully notified CVM of agent uninstallation.
    Erasing    : nutanix-guest-agent-4.0-1.x86_64

   1/1
  warning: /usr/local/nutanix/ngt/config/ngt_config.json saved as /usr/local/
  nutanix/ngt/config/ngt_config.json.rpmsave
  RPM is getting removed/uninstalled.
  Successfully uninstalled Nutanix Guest Tools.
    Verifying  : nutanix-guest-agent-4.0-1.x86_64

   1/1
  Removed:
    nutanix-guest-agent.x86_64 0:4.0-1
  ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2173

```
Complete!
```

Additionally, clear the /usr/local/nutanix/ngt directory.

2. Verify whether the NGT information of the guest VM is removed from the CVM.

   a. Log in to the CVM with SSH.

   b. Check the NGT information status in the CVM by running the following command.

   ```
   nutanix@cvm$ ncli ngt list
   ```

   An output similar to the following is displayed if the NGT information of the guest VM is not removed from the CVM.

   ```
   nutanix@cvm$ ncli ngt list

       VM Id                     : 0005b6a7-6bcc-03f2-0000-0000000097fe::e4a1216a-
   a287-43c2-bbbf-28951e1bf615
       VM Name                   : win 2012
       NGT Enabled               : true
       Tools ISO Mounted         : false
       Vss Snapshot              : false
       File Level Restore        : false
       Communication Link Active : true
   ```

   In the VM ID column, the text after "::" is the ID of the VM as shown in the example.

3. If the NGT information of the guest VM appears when you run the command in Step 2b, remove the NGT information from the CVM by running the following command.

   ```
   nutanix@cvm$ ncli ngt delete vm-id=virtual_machine_id
   ```

   Replace *virtual_machine_id* with the ID of the VM displayed in the output of Step b.

   Note: For information about troubleshooting any NGT-related issues, see KB-3741.

NGT Metrics Collection for Windows Performance Monitor

You can monitor host-specific metrics for a VM in a guest VM running Windows OS. The supported metrics are fetched from the controller VM (CVM) and are published to the Microsoft Windows Performance Monitor on the guest VM.

Managing Metrics Collection in a Guest VM

Nutanix publishes VM-specific metrics in the NGT Metrics performance counter object in the Windows Performance Monitor. You can leverage all Perfmon functionalities to view the metrics data in different ways. For example, you can view the metrics in different graph formats. The options available for graphs are line, histogram, and report.

Important: By default, NGT metrics collection is disabled in a guest VM. Contact Nutanix Support to enable metrics collection in a guest VM.

The guest VM makes an RPC call to the CVM every 30 seconds to fetch the metrics data. Once the data is fetched successfully, it internally checks if this counter is already registered in the Perfmon utility. If the counter is not registered, it first registers the counter and then publishes this data to the Performance Monitor. By default, the following metrics are collected from the CVM after enabling NGT metrics collection in the guest VM.

- **hypervisor_cpu_usage_ppm**: Indicates the VM processor time in parts per million.
- **hypervisor_cpu_ready_time_ppm**: Indicates the VM stolen time in parts per million.

For information about monitoring or viewing NGT metrics in the guest VM, see Monitoring NGT Metrics for System Performance in Guest VM on page 325.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2174

Managing Metrics Collection from CVM

Although the NGT metrics collection is enabled by default on CVMs, you can monitor the NGT metrics in the Performance Monitor only in the guest VM.

> **Important:** Contact Nutanix Support to enable or disable NGT metrics collection in a CVM.

The default metrics available in the CVM are hypervisor_cpu_usage_ppm and hypervisor.cpu_ready_time_ppm. You can modify the metrics list from the CVM by editing the ~/config/nutanix_guest_tools/ngt_metrics_info.json file to add or remove the metrics to be published on the guest VMs.

For example, in the ngt_metrics_info.json file you can modify the array list to add or remove metrics in the metrics info block. Any changes in the metrics list reflect after you restart the NGA service on the CVM.

```
{
    "metrics_info" : [
        "hypervisor_cpu_usage_ppm",
        "hypervisor.cpu_ready_time_ppm"
    ]
}
```

After you modify the metrics list, you must restart the NGT service on the CVM by running the $ allssh "genesis stop nutanix_guest_tools && cluster start" command for the updated metrics data to reflect in the guest VM. After the guest VM fetches the metrics, it updates this data in the Perfmon utility without manual intervention (like service restart) in the guest VM.

> **Note:** The metrics list must be modified for all the nodes.

Known Issues and Limitations

- Any failure in registering a counter or in publishing the metrics data is logged in the Nutanix Guest Agent logs in the guest VM. Currently, you are not alerted if such an event occurs.
- In Windows Performance monitor, the NGT hypervisor CPU metrics is collected in parts per million. Because the default scale is 1, it gives values over 100%. Nutanix recommends to adjust the scale in the **Performance Monitor Properties** > **Data** tab to .0001.

Monitoring NGT Metrics for System Performance in Guest VM

Before you begin

- Verify that the guest VM has Microsoft Windows OS and NGT installed.
- Verify that the guest VM has Microsoft Windows Perfmon utility installed.
- Verify that the NGT metric collection is enabled in the guest VM. You can do this by checking if the Ngt Metrics collection capabilities got enabled message is logged in C:\Program Files\Nutanix\logs \guest_agent_service.INFO.
- Ensure that the CVM and the guest VM system clocks are in sync with the actual time to ensure that accurate metrics are generated.

About this task

Perform the following steps to view the NGT metrics in the guest VM.

Procedure

1. Log in to the Prism Element web console.
2. In the dropdown list of the main menu, select **VM**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2175

3. From the VM page that opens, select the **Table** view.
4. Select the target VM in the table, and click **Launch Console**.
5. Log in to the guest VM.
6. Navigate to **Start** > **Run**.
7. Type perfmon and click **OK**.
   This launches the **Performance Monitor** utility.
8. Under **Monitoring Tools**, select **Performance Monitor**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2176

9. Click the **Add** icon.
   The **Add Counters** window appears. NGT metrics is listed in the counter list.

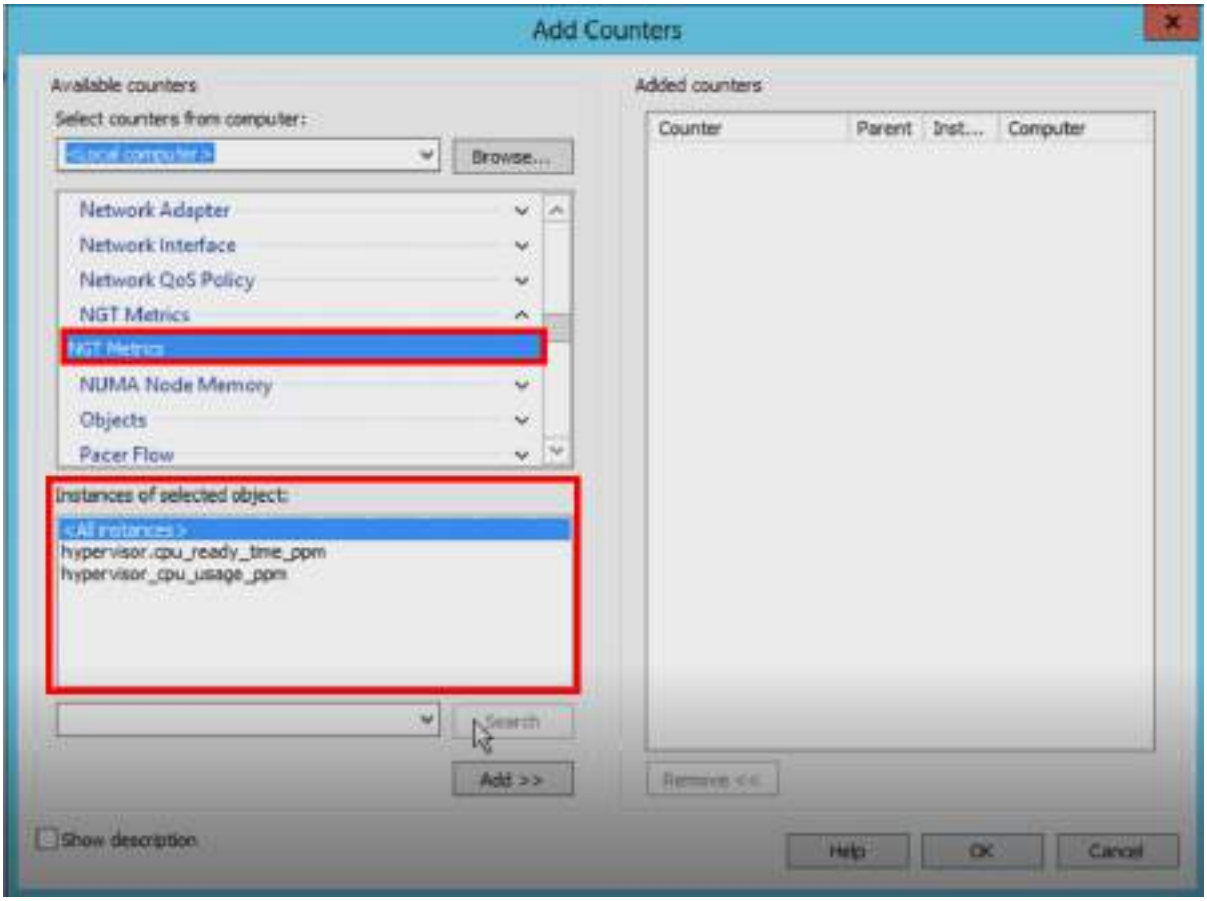


Figure 43: Performance Monitor (Add Counters)

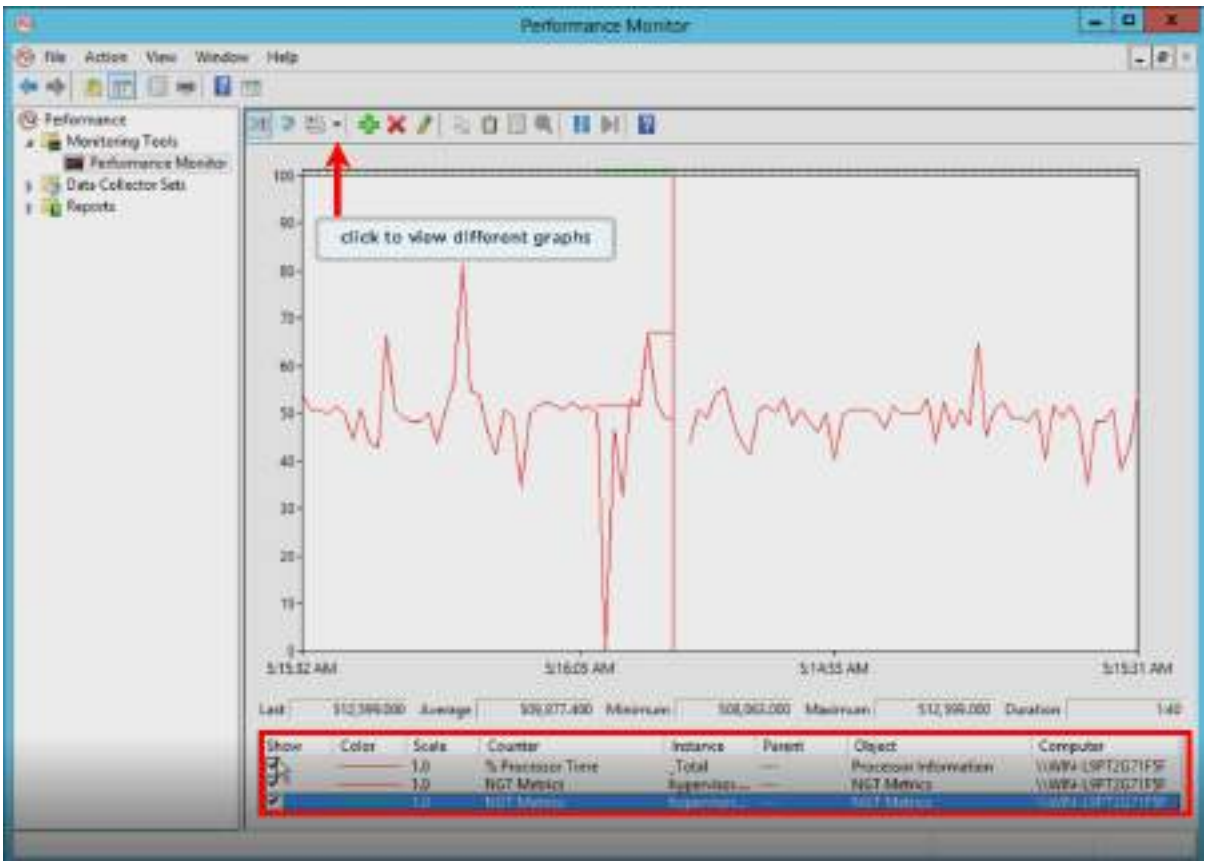


Figure 44: NGT Metrics (Graphical View)

What to do next

After metrics are collected, you can leverage all the Windows Performance Monitor functionalities like generating reports, viewing metrics graphically.

VM-Host Affinity Policies Defined in Prism Element

In Prism Element, you can define scheduling policies for virtual machines on an AHV cluster at a VM level. By defining these policies, you can control the placement of a virtual machine on specific hosts within a cluster.

You can define the VM-Host affinity policies by using Prism Element during the VM create or update operation. For more information, see Creating a VM (AHV).

For information on how the protection domain-based VM-Host affinity policies are handled during disaster recovery, see Affinity Policies Handling - Protection-Domain Based DR Solution with On-prem Clusters Only.

Limitations of Affinity Rules

Even though if a host is removed from a cluster, the host UUID is not removed from the host-affinity list for a VM.

Configuring Legacy VM-VM Anti-Affinity Policy

To configure the legacy VM-VM anti-affinity policies, you must first define a group and then add all the VMs on which you want to define the legacy VM-VM anti-affinity policy.

About this task

> **Important:** Starting with the AOS 7.0 and pc.2024.3 release, you can create category based VM-VM anti-affinity policies from Prism Central. For more information, see VM-VM Anti-Affinity Policies Defined in Prism Central.

To configure the legacy VM-VM anti-affinity policy, follow these steps:

Procedure

1. Log on to the Controller VM with SSH session.
2. Create a group:

   ```
   nutanix@cvm$ acli vm_group.create group_name
   ```

   Replace *group_name* with the name of the group.
3. Add the VMs on which you want to define the legacy anti-affinity to the group:

   ```
   nutanix@cvm$ acli vm_group.add_vms group_name vm_list=vm_name
   ```

   Replace *group_name* with the name of the group. Replace *vm_name* with the name of the VMs that you want to define anti-affinity on. In case of multiple VMs, you can specify comma-separated list of VM names.
4. Create the legacy VM-VM anti-affinity policy.

   ```
   nutanix@cvm$ acli vm_group.antiaffinity_set group_name
   ```

   Replace *group_name* with the name of the group.

   After you configure the group and then power on the VMs, the VMs that are part of the group are started (attempt to start) on the different hosts.

   > **Important:**
   >
   > The legacy VM-VM anti-affinity policy is a preferential policy. The system does not block any VM operation, such as VM maintenance mode or manual live migration of the VM, even if there is a policy violation. For example, when you manually migrate one VM of a VM-VM pair with an anti-affinity policy, the policy is applied on a commercially reasonable effort only.
   >
   > The Acropolis Dynamic Scheduling (ADS) always attempts to maintain compliance with the VM-VM anti-affinity policy and ensures that the legacy VM-VM anti-affinity policy is enforced on a commercially reasonable effort. For example, if you manually migrate a VM and the migration leads to non-compliance with the legacy VM-VM anti-affinity policy, the ADS checks if the host is specified in manual migration, and performs the following actions:
   >
   > - Ignores compliance to the legacy VM-VM anti-affinity policy, if a host is specified during manual migration.
   > - Attempts to enforce the policy back into compliance on a best-effort basis, if a host is not specified during manual migration.
   >
   > For more information on ADS, see Acropolis Dynamic Scheduling in AHV section in AHV Administration Guide.

Removing Legacy VM-VM Anti-Affinity Policy

Perform the following procedure to remove the legacy VM-VM anti-affinity policy.

Procedure

1. Log on to the Controller VM with SSH session.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2179

2. Remove the legacy VM-VM anti-affinity policy.

```
nutanix@cvm$ acli vm_group.antiaffinity_unset group_name
```

Replace *group_name* with the name of the group.

The legacy VM-VM anti-affinity policy is removed for the VMs that are present in the group, and they can start on any host during the next power on operation (as necessitated by the ADS feature).

Connect to Citrix Cloud

The **Connect to Citrix Cloud** feature leverages the automated installer functionality of the Citrix Cloud connector to establish a secure communication channel between Nutanix and Citrix Cloud. This feature provides single-click integration of the on-premise Nutanix clusters as a resource location with the Citrix Cloud environment.

> **Note:** This feature is supported on AHV only.

This feature helps you configure the Citrix Cloud integration settings in the following way:

1. Establishes the connection to the Citrix Cloud workspace.
2. Configures Nutanix cluster as resource location in the Citrix cloud.
3. Configures the Citrix Cloud connector VM.
4. Registers the Citrix Cloud connector VM to the Active Directory (AD) domain on the Citrix cloud.

Once the integration is complete, VDIs can be created using the *Nutanix AHV MCS Plug-in for Citrix XenDesktop* 1.1.1.0 or later. The AHV MCS Plug-in is designed to create and manage VDIs in a Nutanix Acropolis infrastructure environment. For more information, see AHV Plug-in for Citrix install guide and release notes.

Thus, to begin deploying your VMs and applications, you must perform the following:

- Configure the Citrix cloud integration settings using the **Connect to Citrix Cloud** feature.
- Install the *Nutanix CWA Plug-In for Citrix Cloud Connector*.

Refer to the *Citrix documentation* for details on Citrix Cloud connector.

Connecting to the Citrix Cloud

To integrate with the Citrix Cloud workspace, perform the following procedure.

Before you begin

Ensure that you have created a Sysprep (System Preparation) VM with Windows 2012 R2 server or newer versions of Windows server 2016, 2019 and 2022 as the base image and the VM should be available on the Nutanix cluster.

> **Caution:** The Sysprep VM must be in the powered-off state. If you power on the VM, you will lose the Sysprep state and the configuration will fail.

For more information, see *Microsoft documentation* on *Sysprep (Generalize) a Windows installation*.

Procedure

1. Log on to the Prism Element web console using your Nutanix administrator credentials.

   > **Note:** The procedure does not work if Prism Element is launched from Prism Central web console.

2. Click the gear icon in the main menu and then select **Connect to Citrix Cloud** from the **Setup** section in the **Settings** page.
   The **Connect to Citrix Cloud** dialog box opens.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2180

3. Authenticate your connection to the Citrix cloud by using one of the following methods:

   - **Enter Manually**

     1. Enter your **Customer ID** for the Citrix Cloud.
     2. Enter your secure **Client ID** for the Citrix Cloud.
     3. Enter the downloaded secure client **Secret Key**.

        Note: You can find the **Customer ID**, **Client ID**, and **Secret Key** from the *API Access* page in the Citrix Cloud console.

     4. Click **Connect**.

   - **Upload Credential Key**

     1. Click **Upload Key File** to browse and select the key file in the CSV format.

        You can create or download the key file from the *API Access* page in the Citrix Cloud console (within *Identity and Access Management*). This key file is used for the Citrix Cloud connector installation.
     2. Enter your **Customer ID** for the Citrix Cloud.
     3. Click **Connect**.

4. Select the **Resource Location** from the drop-down menu.

   The drop-down menu displays the resource locations that are created on the Citrix Cloud. If you have not previously created any resource locations, enter a name for the resource location that you want to create in the **Resource location** field.

5. (Optional) Review the **Citrix Cloud** details. If any change is required, click the **Change** hyperlink to edit the connection details.

6. (Optional) Select the **High Availability** check-box to enable or disable high availability for the connector nodes.

   By default, high availability is enabled. On enabling high availability, two connector nodes are created for the redundancy purpose.

   Note: Citrix Cloud recommends that you install two connectors for redundancy and high availability.

7. In the **VM Master Image** search box, start typing the initial letters of the previously created Sysprep VM image and select the auto-completed option.

8. Enter the **Connector VM Name**.

9. If high availability is enabled, enter the **Secondary Connector VM Name (for high availability)**.

10. Enter the **Connector VM Password**.

11. Enter the **Domain Credentials** to join your enterprise domain to the resource location.

    a. Enter the **Domain Username** in the format USERDOMAIN\USERNAME.

    b. Enter the **Domain Password**.

    c. Enter the **Machine Domain Name**.

    d. Enter the **DNS Gateway**.

12. Click **Save and Continue**.
    The connector VM or VMs are configured successfully.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2181

What to do next

- Verify the connection status. For more information, see Viewing Citrix Connection Status on page 332.
- Verify if the connector VM or VMs are created from the **VM Dashboard**.
- Wait for the state of the connector VM or VMs to change from powered off to powered on and then click **Launch Console**. The VM preparation process starts.
- Once the VM starts, install the *Nutanix CWA Plug-In for Citrix Cloud Connector* to start the application deployment.

Viewing Citrix Connection Status

You can view the current status of your Citrix Cloud connection. This helps to verify the registration of the connector VM to the Citrix cloud.

To view details of the Citrix connection, click the gear icon and select **Connect to Citrix Cloud**. If the connector VM is configured, the connector VM name and the status are listed under Connector VMs. It might take some time for the connection status to refresh.

The Connection Status shows the following statuses:

- Connected - The connector VM is successfully registered with Citrix cloud.
- Connection in progress - The connector VM is registration with Citrix cloud is in progress.
- Not Connected - The connector VM is not registered with the Citrix cloud or the Citrix registration has failed. In this case, wait for the connection status to refresh, it may take several minutes depending on your environment. Otherwise, click **Delete Connection** to delete the Citrix cloud connection and configure it again. The **Delete Connection** option deletes the connector VM and unregisters the account from the Citrix Cloud.

> **Note:** For XenServer, the **Delete Connection** option does not delete the connector VMs. You must delete the connector VMs manually.

Guest VM Cluster Configuration (AHV Only)

In AHV clusters, you can create guest VM clusters by either directly attaching volume groups to guests VMs or by using iSCSI. Follow this document if you want to create guest VM clusters by directly attaching volume groups to guests VMs.

For information on how to create guest VM clusters by using iSCSI, see the Nutanix Volumes Guide.

Creating a Guest VM Cluster by Directly Attaching a Volume Group (AHV Only)

In AHV clusters, you can create a guest VM cluster by directly attaching a volume group to guest VMs. After you attach a volume group to guest VMs, vDisks appear as SCSI devices to the guest operating system and you do not need to set up any in-guest connections when you are creating a guest cluster. If you directly attach volume groups to guest VMs, you can seamlessly share vDisks across VMs in the guest cluster.

About this task

You can directly attach a volume group to guest VMs to create the following guest clusters:

- Microsoft Failover Cluster (MSFT)
- Red Hat Enterprise Linux (RHEL) Cluster

> **Note:** To create an MSFT cluster, ensure that the minimum Nutanix VirtIO version installed on the guest VM is 1.1.4. For more information about VirtIO drivers, see Nutanix VirtIO for Windows in *AHV Administration Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2182

You cannot create a guest VM cluster by directly attaching a volume group to guest VMs in ESXi and Hyper-V clusters.

Perform the following sequence of tasks to create a guest cluster by directly attaching a volume group to guest VMs.

Procedure

1. Log on to the Prism Element web console.
2. Create the number of VMs you want in the guest cluster.

   For information on how to create a VM in an AHV cluster, see Creating a VM (AHV).
3. Create a volume group for the guest cluster.

   For information on how to create a volume group, see Creating a Volume Group.
4. Attach the volume group you created to each VM in the guest cluster.

   For information on how to attach a volume group to a VM, see Managing a VM (AHV).
5. Create a guest cluster.

   For information on how to create a guest cluster, see the documentation of your guest operating system.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2183

PERFORMANCE MONITORING

Nutanix provides several mechanisms to maximize performance in the cluster. The converged Distributed Storage Fabric (DSF) architecture is designed to service the VM requests locally on each node whenever possible. Each node employs data tiers so that frequently accessed (*hot*) data is retained in memory or solid state disk (SSD) storage while seldom accessed (*cold*) data is moved to hard disk drive (HDD) storage. Each Controller VM has an in-memory read cache to access highly requested data directly from memory.

The web console allows you to monitor and analyze performance across the cluster. For more information, see Analysis Dashboard on page 334.

Analysis Dashboard

The Analysis dashboard allows you to create charts that can monitor dynamically a variety of performance measures. To view the Analysis dashboard, select **Analysis** from the pull-down list on the left of the main menu.

Menu Options

The Analysis dashboard does not include menu options other than those available from the main menu.

Analysis Screen Details

The Analysis dashboard includes three sections.

- *Chart definitions*. The pane on the left lists the charts that can be run. No charts are provided by default, but you can create any number of charts. A chart defines the metrics to monitor. There are two types of charts, metric and entity. A metric chart monitors a single metric for one or more entities. An entity chart monitors one or more metrics for a single entity.

  > **Note:** You can change the color assigned to a metric or entity by clicking that color box in the chart (left pane) and then selecting a different color from the displayed palette.

- *Chart monitors*. When a chart definition is checked, the monitor appears in the middle pane. An Alerts & Events monitor always appears first. The remaining monitors are determined by which charts are checked in the left pane. You can customize the display by selecting a time interval (from 3 hours to a month) from the **Range** drop-down (above the charts) and then refining the monitored period by moving the time interval end points to the desired length.
- *Alerts and events*. Any alerts and events that occur during the interval specified by the time line in the middle pane appear in the pane on the right. For more information, see Prism Element Alerts and Events Reference Guide.

The following table describes each field in the Analysis dashboard. Some fields can include a slide bar on the right to view additional information in that field. The displayed information is dynamically updated to remain current.

> **Note:** For information about how the metrics are measured, see Understanding Displayed Statistics on page 70.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2184

Table 64: Analysis Screen Fields

Name	Description
Charts	Displays the set of defined charts. Check the box next to a chart name to run that chart in the middle pane. The chart monitor appears in the middle pane shortly after checking the box. Uncheck the box to stop that monitor and remove it from the middle pane. To edit a chart definition, click the pencil icon to the right of the name. This opens the edit chart window, which is the same as the new chart window except for the title. To delete a chart, click the cross icon on the right.
New Metric Chart	Allows you to create a chart that tracks a single metric for one or more entities. For more information, see Creating a Metric Chart on page 337.
New Entity Chart	Allows you to create a chart that tracks one or more metrics for a single entity. For more information, see Creating an Entity Chart on page 336.
(range time line and monitor period)	Displays a time line that sets the duration for the monitor displays. To set the time interval, select the time period (3 hour, 6 hour, 1 day, 1 week, WTD [week to date], 1 month) from the **Range** field pull-down menu (far right of time line). To customize the monitor period, you may move through the timeline by manipulating the translucent blue bar on the top of the Analysis pane. To reach a specific point in time, use the solid blue bar at the bottom of the Analysis pane. • By default, if you select a scale that is greater than the current, the translucent time scrubber tends to jump to the most recent record. • If you need to move further back in time than the scrubber allows at the current scale, increase the scale of the scrubber. • After you have the scale of your choice, move the translucent scrubber across the timeline to the period in time that you wish to examine. • After you have a time period selected, slide the solid blue time slider to a specific point in time. • To move down further into the time period, lower the scale and move the scrubber accordingly. • The lowest choice for scale is 3 hours, but you can shrink the translucent scrubber down to approximately five minutes within the UI. • When exporting the charts, the selected scale is used for the file regardless of whether the scrubber has been resized to a custom value.
Alerts & Events Monitor	Displays a monitor of alert and event messages that were generated during the time interval. Alerts and events are tracked by a moving histogram with each bar indicating the number of messages generated during that time. The message types are color coded in the histogram bars (critical alert = red, warning alert = orange, informational alert = blue, event = gray).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2185

Name	Description
(defined chart monitors)	Displays monitors for any enabled (checked) charts. In the figure above, three charts are enabled (memory usage, CPU/memory, and disk IOPS). You can export the chart data by clicking on the chart header. This displays a drop-down menu (below) to save the data in CSV or JSON format. It also includes a chart link option that displays the URL to that chart, which you can copy to a clipboard and use to import the chart.
Alerts	Displays the alert messages that occurred during the time interval. For more information, see Alerts Dashboard in *Prism Element Alerts and Events Reference Guide*. Clicking a message causes the monitor line to move to the time when that alert occurred.
Events	Displays the event messages that occurred during the time interval. Clicking a message causes the monitor line to move to the time when that event occurred.

Creating an Entity Chart

About this task

An entity chart monitors the performance of one or more metrics for a single entity. To create an entity chart definition, do the following:

Procedure

1. Log in to the Prism Element web console.
2. In the Analysis Dashboard on page 334, click **New** > **New Entity Chart**.
   The **New Entity Chart** dialog box appears.
3. Do the following in the indicated fields:
   a. **Chart Title**: Enter a title for this chart.
   b. **Entity type**: Select an entity from the pull-down list.
      The entity types include host, disk, storage pool, storage container, virtual machine, volume group, remote site, protection domain, replication link, virtual disk, and cluster.
   c. **Entity**: Enter the name of the target entity.
      As you enter characters in this field, it displays a list of matching entries of that entity type. Click the name when it appears in the search list.

      Note: If you are creating this chart for *Prism Central*, the list spans the registered clusters. Otherwise, the list is limited to the current cluster.

   d. **Metric**: Select a metric from the drop-down list. (Repeat to include additional metrics.)
      For descriptions of the available metrics, see Chart Metrics on page 337.
4. When all the field entries are correct, click the **Save** button.
   The Analysis dashboard reappears with the new chart appearing in the list of charts on the left of the screen.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2186

Creating a Metric Chart

About this task

A metric chart monitors the performance of a single metric for one or more entities. To create a metric chart definition, do the following:

Procedure

1. Log in to the Prism Element web console.
2. In the Analysis Dashboard on page 334, click **New** > **New Metric Chart**.
   The **New Metric Chart** dialog box appears.
3. Do the following in the indicated fields:
   a. **Chart Title**: Enter a title for this chart.
   b. **Metric**: Select a metric to monitor from the pull-down list.
      For descriptions of the available metrics, see Chart Metrics on page 337.
   c. **Entity Type**: Select an entity type from the pull-down list. (Repeat to include additional entities.)
      The entity types include host and cluster.
   d. **Entity**: Enter the name of the target entity.
      As you enter characters in this field, it displays a list of matches of the entity type. Click the name when it appears in the search list. (Repeat to include additional names.)

      Note: If you are creating this chart for *Prism Central* the list spans the registered clusters. Otherwise, the list is limited to the current cluster.
4. When all the field entries are correct, click the **Save** button.
   The Analysis dashboard reappears with the new chart appearing in the list of charts on the left of the screen.

Chart Metrics

The following metrics can be added to charts.

Note: The mapping between a metric and an entity type is hypervisor dependent.

Memory Usage **Metric**	**Entity Type(s)**	**Description**
Content Cache Hit Rate (%)	• Host • Cluster	Content cache hits over all lookups. ID: `CONTENT_CACHE_HIT_PPM`
Content Cache Hits	• Host • Cluster	Number of hits on the content cache. ID: `CONTENT_CACHE_NUM_HITS`
Content Cache Logical Memory Usage	• Host • Cluster	Logical memory (in bytes) used to cache data without deduplication. ID: `CONTENT_CACHE_LOGICAL_MEMORY_USAGE_BYTES`

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2187

Memory Usage **Metric**	**Entity Type(s)**	**Description**
Content Cache Logical SSD Usage	• Host • Cluster	Logical SSD memory (in bytes) used to cache data without deduplication. ID: `CONTENT_CACHE_LOGICAL_SSD_USAGE_BYTES`
Content Cache Lookups	• Host • Cluster	Number of lookups on the content cache. ID: `CONTENT_CACHE_NUM_LOOKUPS`
Content Cache Physical Memory Usage	• Host • Cluster	Real memory (in bytes) used to cache data by the content cache. ID: `CONTENT_CACHE_PHYSICAL_MEMORY_USAGE_BYTES`
Content Cache Reference Count	• Host • Cluster	Average number of content cache references. ID: `CONTENT_CACHE_NUM_DEDUP_REF_COUNT_PPH`
Content Cache SSD Usage	• Host • Cluster	Real SSD usage (in bytes) used to cache data by the content cache. ID: `CONTENT_CACHE_PHYSICAL_SSD_USAGE_BYTES`
Deduplication Fingerprints Cleared	• Host • Cluster	Number of written bytes for which fingerprints have been cleared. ID: `DEDUP_FINGERPRINT_CLEARED_BYTES`
Deduplication Fingerprints Written	• Host • Cluster	Number of written bytes for which fingerprints have been added. ID: `DEDUP_FINGERPRINT_ADDED_BYTES`
Disk I/O Bandwidth	• Host • Cluster • Disk • Storage Pool	Data transferred per second in KB/second from disk. ID: `STATS_BANDWIDTH`
Disk I/O Bandwidth - Read	• Host • Cluster • Disk • Storage Pool	Read data transferred per second in KB/second from disk. ID: `STATS_READ_BANDWIDTH`

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2188

Memory Usage **Metric**	**Entity Type(s)**	**Description**
Disk I/O Bandwidth - Write	• Host • Cluster • Disk • Storage Pool	Write data transferred per second in KB/second from disk. ID: `STATS_WRITE_BANDWIDTH`
Disk I/O Latency	• Host • Cluster • Disk • Storage Pool	I/O latency in milliseconds from disk. ID: `STATS_AVG_IO_LATENCY`
Disk IOPS	• Host • Cluster • Disk • Storage Pool	Input/Output operations per second from disk. ID: `STATS_NUM_IOPS`
Disk IOPS - Read	• Host • Cluster • Disk • Storage Pool	Input/Output read operations per second from disk. ID: `STATS_NUM_READ_IOPS`
Disk IOPS - Write	• Host • Cluster • Disk • Storage Pool	Input/Output write operations per second from disk. ID: `STATS_NUM_WRITE_IOPS`
GPU Framebuffer Usage	Virtual Machine	Framebuffer usage in percentage. ID: `FRAMEBUFFER_USAGE_PPM` **Note:** The Virtual Machine entity is applicable for AHV hypervisor.
GPU Usage	Virtual Machine	GPU compute usage in percentage. ID: `GPU_USAGE_PPM` **Note:** The Virtual Machine entity is applicable for AHV hypervisor.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2189

Memory Usage **Metric**	**Entity Type(s)**	**Description**
GPU video decoder Usage	Virtual Machine	GPU video decoder usage in percentage. ID: `DECODER_USAGE_PPM` **Note:** The Virtual Machine entity is applicable for AHV hypervisor.
GPU video encoder usage	Virtual Machine	GPU video encoder usage in percentage ID: `ENCODER_USAGE_PPM` **Note:** The Virtual Machine entity is applicable to AHV hypervisor.
Hypervisor CPU Ready Time (%)	Virtual Machine	Percentage of time that the virtual machine was ready, but could not get scheduled to run. ID: `STATS_HYP_CPU_READY_TIME`
Hypervisor CPU Usage (%)	• Host • Cluster • Virtual Machine	Percent of CPU used by the hypervisor. ID: `STATS_HYP_CPU_USAGE`
Hypervisor I/O Bandwidth	• Host • Cluster • Virtual Machine	Data transferred per second in KB/second from Hypervisor. ID: `STATS_HYP_BANDWIDTH` **Note:** Virtual Machine entity is applicable for ESXi. hypervisor
Hypervisor I/O Bandwidth - Read	• Host • Cluster • Virtual Machine	Read data transferred per second in KB/second from Hypervisor. ID: `STATS_HYP_READ_BANDWIDTH` **Note:** Virtual Machine entity is applicable for ESXi hypervisor.
Hypervisor I/O Bandwidth - Write	• Host • Cluster • Virtual Machine	Write data transferred per second in KB/second from Hypervisor. ID: `STATS_HYP_WRITE_BANDWIDTH` **Note:** Virtual Machine entity is applicable for ESXi hypervisor.
Hypervisor I/O Latency	• Host • Cluster • Virtual Machine	I/O latency in milliseconds from Hypervisor. ID: `STATS_HYP_AVG_IO_LATENCY` **Note:** Virtual Machine entity is applicable for ESXi hypervisor.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2190

Memory Usage **Metric**	**Entity Type(s)**	**Description**
Hypervisor I/O Latency - Read	• Host • Cluster	I/O read latency in milliseconds from Hypervisor. ID: `STATS_HYP_AVG_READ_IO_LATENCY` **Note:** Cluster entity is applicable only for AHV hypervisor.
Hypervisor I/O Latency - Write	• Host • Cluster	I/O write latency in milliseconds from Hypervisor. ID: `STATS_HYP_AVG_WRITE_IO_LATENCY` **Note:** Cluster entity is applicable only for AHV hypervisor.
Hypervisor IOPS	• Host • Cluster • Virtual Machine	Input/Output operations per second from Hypervisor. ID: `STATS_HYP_NUM_IOPS` **Note:** • Cluster entity is applicable for AHV hypervisor. • Virtual Machine entity is applicable for ESXi.
Hypervisor IOPS - Read	• Host • Cluster • Virtual Machine	Input/Output read operations per second from Hypervisor. ID: `STATS_HYP_NUM_READ_IOPS` **Note:** • Cluster entity is applicable for AHV hypervisor. • Virtual Machine entity is applicable for ESXi.
Hypervisor IOPS - Write	• Host • Cluster • Virtual Machine	Input/Output write operations per second from Hypervisor. ID: `STATS_HYP_NUM_WRITE_IOPS` **Note:** • Cluster entity is applicable for AHV hypervisor. • Virtual Machine entity is applicable for ESXi.
Hypervisor Memory Usage (%)	• Host • Cluster • Virtual Machine	Percent of memory used by the hypervisor. ID: `STATS_HYP_MEMORY_USAGE`

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2191

Memory Usage **Metric**	**Entity Type(s)**	**Description**
Logical Usage	Storage Container	Logical usage of storage (physical usage divided by replication factor). ID: `STATS_UNTRANSFORMED_USAGE`
Memory Usage (%)	• Host • Cluster • Virtual Machine	Percentage of memory usage used by (any) hypervisor without HA. ID: `AGGREGATE_MEMORY_USAGE_PPM`
Overall Memory Usage (%)	• Host • Cluster	Percentage of memory usage used by AHV with HA. ID: `OVERALL_MEMORY_USAGE_PPM`
Network Rx Bytes	Virtual Machine	Network transmitted bytes reported by the hypervisor. ID: `HYPERVISOR_NUM_RECEIVED_BYTES` **Note:** Virtual Machine entity is applicable for AHV hypervisor.
Network Tx Bytes	Virtual Machine	Write data transferred per second in KB/second. ID: `HYPERVISOR_NUM_TRANSMITTED_BYTES` **Note:** Virtual Machine entity is applicable for AHV hypervisor.
Physical Usage	• Host • Cluster • Disk • Storage Pool • Storage Container	Actual usage of storage. ID: `STATS_TRANSFORMED_USAGE`
Read IOPS (%)	• Host • Cluster • Disk • Storage Pool	Percent of IOPS that are reads. ID: `STATS_READ_IO_PPM`
Replication Bandwidth - Received	• Cluster • Remote Site • Protection Domain • Replication Link	Replication data received per second in KB/second ID: `STATS_REP_BW_RECEIVED`

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2192

Memory Usage **Metric**	**Entity Type(s)**	**Description**
Replication Bandwidth - Transmitted	• Cluster • Remote Site • Protection Domain • Replication Link	Replication data transferred per second in KB/second ID: `STATS_REP_BW_TRANSFERRED`
Replication Bytes - Received	• Cluster • Remote Site • Protection Domain • Replication Link	Number of bytes received. ID: `STATS_REP_NUM_RECEIVED_BYTES` **Note:** Cluster entity is applicable for AHV hypervisor.
Replication Bytes - Total Received	Replication Link	Total number of bytes received. ID: `STATS_REP_TOT_RECEIVED_BYTES`
Replication Bytes - Total Transmitted	Replication Link	Total number of bytes transmitted. ID: `STATS_REP_TOT_TRANSMITTED_BYTES`
Replication Bytes - Transmitted	• Cluster • Remote Site • Protection Domain • Replication Link	Number of bytes transmitted. ID: `STATS_REP_NUM_TRANSMITTED_BYTES` **Note:** Cluster entity is applicable for AHV hypervisor.
Storage Controller Bandwidth	• Cluster • Storage Container • Virtual Machine • Volume Group • Virtual Disk	Data transferred in KB/second from the Storage Controller. ID: `STATS_CONTROLLER_BANDWIDTH`
Storage Controller Bandwidth - Read	• Cluster • Storage Container • Virtual Machine • Volume Group • Virtual Disk	Read data transferred in KB/second from the Storage Controller. ID: `STATS_CONTROLLER_READ_BANDWIDTH`

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2193

Memory Usage **Metric**	**Entity Type(s)**	**Description**
Storage Controller Bandwidth - Write	• Cluster • Storage Container • Virtual Machine • Volume Group • Virtual Disk	Write data transferred in KB/second from the Storage Controller. ID: `STATS_CONTROLLER_WRITE_BANDWIDTH`
Storage Controller IOPS	• Host • Cluster • Storage Container • Virtual Machine • Volume Group • Virtual Disk	Input/Output operations per second from the Storage Controller ID: `STATS_CONTROLLER_NUM_IOPS` **Note:** The Host entity is applicable for AHV hypervisor only.
Storage Controller IOPS - Read	• Host • Cluster • Storage Container • Virtual Machine • Volume Group • Virtual Disk	Input/Output read operations per second from the Storage Controller ID: `STATS_CONTROLLER_NUM_READ_IOPS` **Note:** The Host entity is applicable for AHV hypervisor.
Storage Controller IOPS - Read (%)	• Cluster • Storage Container • Virtual Machine • Volume Group • Virtual Disk	Percent of Storage Controller IOPS that are reads. ID: `STATS_CONTROLLER_READ_IO_PPM` **Note:** The Host entity is applicable for AHV hypervisor.
Storage Controller IOPS - Write	• Host • Cluster • Storage Container • Virtual Machine • Volume Group • Virtual Disk	Input/Output write operations per second from the Storage Controller ID: `STATS_CONTROLLER_NUM_WRITE_IOPS`

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2194

Memory Usage **Metric**	**Entity Type(s)**	**Description**
Storage Controller IOPS - Write (%)	• Cluster • Storage Container • Virtual Machine • Volume Group • Virtual Disk	Percent of Storage Controller IOPS that are writes. ID: `STATS_CONTROLLER_WRITE_IO_PPM`
Storage Controller Latency	• Cluster • Storage Container • Virtual Machine • Volume Group • Virtual Disk	I/O latency in milliseconds from the Storage Controller. ID: `STATS_CONTROLLER_AVG_IO_LATENCY` **Note:** • Cluster entity is applicable only for AHV hypervisor. • Virtual Machine entity is applicable for AHV and Hyper-V hypervisors.
Storage Controller Latency - Read	• Cluster • Storage Container • Virtual Machine • Volume Group • Virtual Disk	Storage Controller read latency in milliseconds. ID: `STATS_CONTROLLER_AVG_READ_IO_LATENCY` **Note:** Cluster entity is applicable for AHV hypervisor.
Storage Controller Latency - Write	• Cluster • Storage Container • Virtual Machine • Volume Group • Virtual Disk	Storage Controller write latency in milliseconds. ID: `STATS_CONTROLLER_AVG_WRITE_IO_LATENCY` **Note:** Cluster entity is applicable for AHV hypervisor.
Storage container own usage	Storage Container	Storage container's own usage + Reserved (not used). ID: `NEW_CONTAINER_OWN_USAGE_LOGICAL`
Swap In Rate	Virtual Machine	Rate of data being swapped in. ID: `STATS_HYP_SWAP_IN_RATE` **Note:** Virtual Machine entity is applicable for ESXi and Hyper-V hypervisors.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2195

Memory Usage **Metric**	**Entity Type(s)**	**Description**
Swap Out Rate	Virtual Machine	Rate of data being swapped out. ID: `STATS_HYP_SWAP_OUT_RATE` **Note:** Virtual Machine entity is applicable for ESXi and Hyper-V hypervisors.
Virtual NIC bytes received packets with error.	Virtual Machine	Virtual NIC bytes received packets with error. `STATS_NETWORK_ERROR_RECEIVED_PACKETS` **Note:** Virtual Machine entity is applicable for ESXi hypervisor.
Virtual NIC bytes received rate.	Virtual Machine	Virtual NIC bytes received rate in kbps. `STATS_NETWORK_RECEIVED_RATE` **Note:** Virtual Machine entity is applicable only for ESXi hypervisor.
Virtual NIC bytes transmitted rate.	Virtual Machine	Virtual NIC bytes transmitted rate in kbps. `STATS_NETWORK_TRANSMITTED_RATE` **Note:** Virtual Machine entity is applicable for ESXi hypervisor.
Virtual NIC dropped transmitted packets.	Virtual Machine	Number of dropped transmitted packets by the Virtual NIC. `STATS_NETWORK_DROPPED_TRANSMITTED_PACKETS` **Note:** Virtual Machine entity is applicable for ESXi hypervisor.
Virtual NIC receive packets dropped.	Virtual Machine	Number of receive packets dropped by the Virtual NIC. `STATS_NETWORK_DROPPED_RECEIVED_PACKETS` **Note:** Virtual Machine entity is applicable for ESXi hypervisor.
Write IOPS (%)	• Host • Cluster • Disk • Storage Pool	Percent of IOPS that are writes. ID: `STATS_WRITE_IO_PPM`

Exporting Performance Data

This topic describes how to view and export the performance chart.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2196

About this task

Performance data is available for three months. You can export the performance data results in CSV or JSON format.

Procedure

1. Log into the Prism Element web console.
2. In the Analysis Dashboard on page 334, click **Home** > **Analysis**.
   The **Analysis** page displays.
3. Click the **Range** drop-down list and set the range to **1 Month**.
   The **1 Month** range shows the data in monthly segments.
4. Export the performance data into a CSV or JSON file. Click the drop-down arrow next to the cluster chart you want to export.

Figure 45: Export Performance Data

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2197

ALERTS AND EVENTS

For information about Alerts and Events in Prism Element web console, see Prism Element Alerts and Events Reference Guide.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2198

VIEW TASK STATUS

The web console displays detailed information about all tasks that have been performed on the cluster.

Task Page Navigation

- To view the Task dashboard, log in to Prism Element web console, and select **Home** > **Tasks**.
- An icon also appears in the main menu when one or more tasks are active (running or completed within the last 48 hours). The icon appears blue when a task runs normally, yellow when it generates a warning, or red when it fails. Clicking the icon displays a drop-down list of active tasks; clicking the **View All Tasks** button at the bottom of that list displays a details screen with information about all tasks for this cluster.

  > **Note:** The drop-down list of active tasks may include a **Clean Up** button (top right). Clicking this button removes from the list any tasks that are no longer running. However, this applies to the current session only. The full active list (including the non-running tasks) appears when you open a new Prism Element web console session.

- When multiple tasks are active, you can filter the list by entering a name in the filter by field.
- You can also filter the list by clicking the **Filters** button and selecting the desired filter options

Each task appears in the list for a minimum of one hour after completion, but how long that task remains in the list depends on several factors. In general, the maximum duration is two weeks. However, tasks are rotated off the list as new tasks arrive, so a task might disappear from the list much sooner when activity is high. In some cases a task appears for longer than two weeks because the last task for each component is retained in the listing.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2199

View Task Status Dashboard

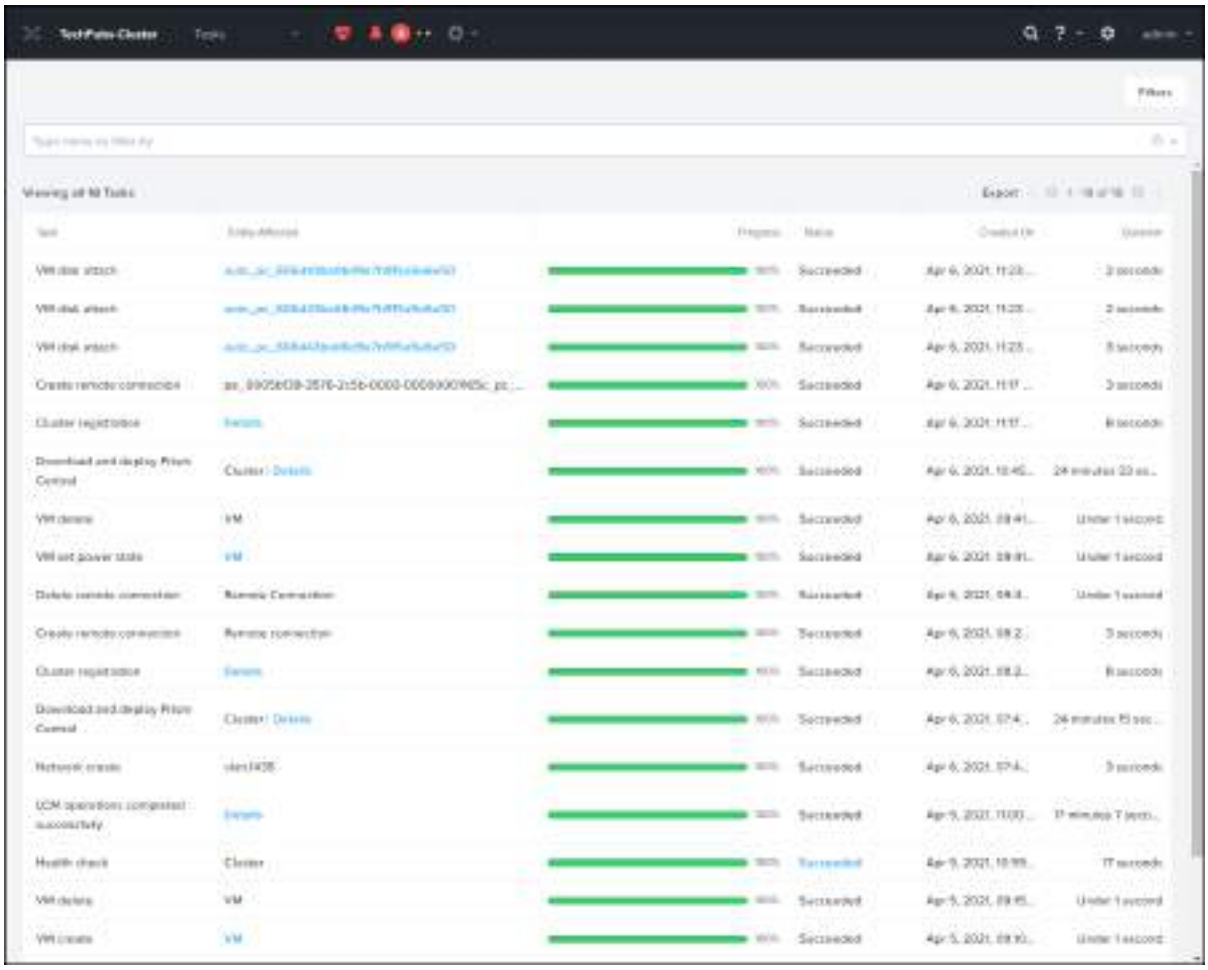


Figure 46: Task Dashboard

Table 65: Tasks List Fields

Parameter	Description	Values
Task	Specifies which type of operation the task is performing.	Any cluster operation you can perform in the Prism Element web console
Entity Affected	Display the entity on which task has been performed. If the link appears on the entity, click it to display the details.	Entity description
Percent	Indicates the current percentage complete for the task.	0%-100%
Status	Indicates the task status, which can be pending, running, completed, or failed.	pending, running,completed,failed
Created On	Displays when the task began.	seconds, minutes, hours

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2200

Parameter	Description	Values
Duration	Displays how long the task took to complete.	seconds, minutes, hours

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2201

SYSTEM MANAGEMENT

The web console allow you to configure various system settings.

- You can specify one or more name servers. For more information, see Configuring Name Servers on page 353.
- If Acropolis is enabled, you can configure one or more network connections. For more information, see Network Configuration for VM Interfaces on page 167.
- You can create a whitelist of IP addresses that are allowed access. For more information, see Configuring a Filesystem Whitelist on page 352.
- You can specify one or more NTP servers for setting the system clock. For more information, see Configuring NTP Servers on page 354.
- You can configure one or more network switches for statistics collection. For more information, see Configuring Network Switch Information on page 172.
- You can specify an SMTP mail server. For more information, see Configuring an SMTP Server on page 355.
- You can configure SNMP. For more information, see Configuring SNMP on page 355.
- You can configure a login banner page. For more information, see Configuring a Banner Page on page 365.

Configuring a Filesystem Whitelist

About this task

An allowlist is a set of addresses that are allowed access to the cluster. Allowlists are used to allow appropriate traffic when unauthorized access from other sources is denied. If you set an allowlist at storage container level, the system overrides any global whitelist for this storage container.

Setting an allowlist helps you provide access to the container via NFS. Some manual data migration workflows might require the allowlist to be configured temporally, while some third-party backup vendors might require the allowlist to be configured permanently to access the container via NFS.

Caution:

- There is no user authentication for NFS access, and the IP address in the allowlist has full read or write access to the data on the container.
- It is recommended to allow single IP addresses (with net mask such as 255.255.255.255) instead of allowing subnets (with netmask such as 255.255.255.0).
- Using a Nutanix storage container as a general-purpose NFS or SMB share is not supported. Because the Nutanix solution is VM-centric, the preferred mechanism is to deploy a VM that provides file share services.

To add (or delete) an address to (from) the filesystem allowlist, do the following:

Procedure

1. Click the gear icon in the main menu and then select **Filesystem Whitelists** in the **Settings** page.
   The **Filesystem Whitelists** dialog box appears.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2202

2. To add an address to the allowlist, do the following in the indicated fields:

   a. **IP address**: Enter the IP address.

   b. **Netmask**: Enter the netmask value.

   c. Click the **+Add** button.

   The entry is added to the **Whitelist Entry** list. An NFS allowlist is created when the hypervisor is ESXi or AHV; a CIFS allowlist is created when the hypervisor is Hyper-V.

3. To delete an entry from the allowlist, click the X icon for that entry in the **Whitelist Entry** list.

   A window prompt appears to verify the action; click the **OK** button. The entry is removed from the list.

Configuring Name Servers

About this task

Name servers are computers that host a network service for providing responses to queries against a directory service, such as a DNS server. To add (or delete) a name server, do the following:

Procedure

1. Log in to the Prism Element web console.

2. Click the gear icon in the main menu and then select **Name Servers** in the **Settings** page.
   The **Name Servers** dialog box appears.

3. To add a name server, enter the server IP address in the **Server IP** field and then click the **Add** button to the right of that field.
   The server is added to the **IP Address** list (below the **Server** field).

   > **Note:** Changes in name server configuration may take up to 5 minutes to take effect. Functions that rely on DNS may not work properly during this time. You can configure a maximum of three name servers.

4. To delete a name server entry, click the X icon for that server in the **IP Address** list.
   A window prompt appears to verify the action; click the **OK** button. The server is removed from the list.

Cluster Time Synchronization

Network Time Protocol (NTP) is a protocol for clock synchronization between computers. The hosts and CVMs in a Nutanix cluster must be configured to synchronize their system clocks with a list of stable NTP servers. Accurate timestamps are important for troubleshooting interactions with third-party software products such as Veeam or CommVault, which might require time synchronization between the hypervisor and the Controller VM to determine which files to back up. Accurate time synchronization between Nutanix clusters paired in Disaster Recovery (DR) configurations also ensures that snapshots do not expire too quickly or too late.

Graphs in the Prism interface rely on CVM time, and incorrect time skews graphs, especially in relation to other monitoring platforms such as vCenter, which rely on other clock sources.

Recommendations for Time Synchronization

Adhere to the following guidelines when configuring time synchronization on a Nutanix cluster:

- Where possible, synchronize Nutanix clusters with internal NTP sources to ensure stability from both a network and a security vulnerability perspective. When you cannot avoid using an external NTP source, Nutanix recommends that you use a time source maintained by your national government.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2203

- Make sure to specify at least five stable time sources that have a high degree of accuracy and that can be reached over a reliable network connection. Generally, the lower the stratum of an NTP source, the higher its accuracy.

  Note that three is the minimum to identify one time source as a false ticker but provides no redundancy, four is the minimum for redundancy, and five is the recommended minimum for a good configuration.

  If you want to use off-site NTP servers, see Selecting Offsite NTP Servers from the Network Time Protocol site for various recommendations. Review all the information in this section before choosing pool.ntp.org servers for your NTP use.

  > **Note:** Using a pool.ntp.org server is not appropriate for all circumstances. For more context, see the Additional Notes section.

- Do not use rate-limited NTP servers.
- Synchronizing a Nutanix cluster with a Windows time source is known to cause issues over a period of time, so Nutanix recommends that you not synchronize a cluster's time with Windows NTP sources. Use reliable non-Windows time sources instead. In an Active Directory domain, the best practice (a design that both works around and improves upon having to include domain controllers in the list of NTP sources) is to bypass the domain controllers and to synchronize the Nutanix hosts and CVMs directly with the NTP sources with which the domain controllers synchronize their time. Specify a common list of at least five reliable non-Windows NTP sources for both the domain controllers and the Nutanix cluster.

  Bypassing the domain controller as a time source is not an option for Hyper-V clusters owing to Kerberos requirements. When being joined to a domain, Nutanix clusters running Hyper-V detect local domain controllers and add them to all CVMs as NTP sources. For Hyper-V clusters, supplement the list of detected domain controllers with as many reliable non-Windows NTP sources as are required to meet the recommendation of a minimum of five NTP time sources. For example, if the Nutanix cluster adds two domain controllers as time sources, specify at least three reliable non-Windows NTP sources in the NTP server list. Specifying additional non-Windows NTP sources is necessary even if the domain controllers synchronize their time with a time source that is considered to be reliable.

- Specify public NTP servers by using their FQDN to help mitigate issues caused by IP address changes.

Configuring NTP Servers

About this task

To add (or delete) an NTP server entry, do the following:

Procedure

1. Log in to the Prism Element web console.
2. Click the gear icon in the main menu and then select **NTP Servers** in the **Settings** page.
   The **NTP Servers** dialog box appears.
3. To add an NTP server entry, enter the server IP address or fully qualified host name in the **NTP Server** field and then click the **Add** button to the right of that field.
   The name or address is added to the **HOST NAME OR IP ADRESS** list (below the **NTP Server** field).
4. To delete an NTP server entry, click the cross icon for that server in the **Servers** list.
   A window prompt appears to verify the action; click the **OK** button. The server is removed from the list.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2204

Configuring an SMTP Server

About this task

Simple Mail Transport Protocol (SMTP) is an Internet standard protocol for electronic mail transmission across Internet Protocol (IP) networks, and Nutanix systems use SMTP to send alert emails.

If you have an external firewall deployed in your organization, see Ports and Protocols to allow traffic from the cluster to Nutanix Support servers.

> **Note:** Since Nutanix CVM has FIPS authentication enabled, the SMTP client in the Nutanix CVM is incompatible with an SMTP server with CRAM-MD5 Authentication enabled.

To configure an SMTP server entry, do the following:

Procedure

1. Log in to the Prism Element web console.
2. Click the gear icon in the main menu and then select **SMTP Server** in the **Settings** page.
   The **SMTP Server Settings** dialog box appears.
3. Do the following in the indicated fields:
   a. **Host Name or IP Address**: Enter the IP address or fully qualified domain name for the SMTP server.
   b. **Port**: Enter the port number to use.
      The standard SMTP ports are 25 (unencrypted), 587 (TLS), and 465 (SSL). For the complete list of required ports, see Port Reference.
   c. **Security Mode**: Enter the desired security mode from the pull-down list.
      The options are NONE (unencrypted), STARTTLS (use TLS encryption), and SSL (use SSL encryption).
   d. **User**: Enter a user name.
      The **User** and **Password** fields apply only when a secure option (STARTTLS or SSL) is selected. The user name might need to include the domain depending on the authentication process.
   e. **Password**: Enter the user password.
   f. **From Email Address** (optional): Enter an e-mail address that appears as the sender address.
      By default, alert and cluster status information e-mails display *cluster@nutanix.com* as the sender address. You have the option to replace that address with a custom address by entering a sender address in this field.
4. When all the fields are correct, click the **Save** button.

Configuring SNMP

About this task

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. Nutanix systems include an SNMP agent that provides interoperability with industry standard SNMP manager systems. Nutanix also provides a custom Management Information Base (MIB) for Nutanix-specific information.

> **Note:**
>
> - The Net-SNMP package version 5.7.2 does not support 256-bit AES encryption.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2205

- Nutanix recommends that you configure your SNMP manager to use the virtual IP address of the cluster to communicate with the Nutanix SNMP agent instead of the Controller VM IP address.

To configure SNMP, do the following:

Procedure

1. Log in to the Prism Element web console.
2. Click the gear icon in the main menu and then select **SNMP** in the **Settings** page.
   The **SNMP Configuration** dialog box appears.
3. To enable SNMP for this cluster, select the **Enable SNMP** checkbox. To disable SNMP, clear the checkbox.

   Note:

   SNMP traps are sent by the Controller VM that functions as the Alert Manager leader. If you need to open your firewall to receive the traps, keep in mind that the Alert Manager leader can rotate during tasks like AOS or host upgrades. Therefore, it might be necessary to open all the Controller VM IP addresses to ensure that the traps are received.

4. To view the Nutanix MIB (NUTANIX-MIB.txt), click the **View MIB** link. To download NUTANIX-MIB.txt, right-click and select the appropriate download action for your browser and then copy NUTANIX-MIB.txt to your SNMP manager systems.

   See your SNMP manager documentation for instructions on how to install the Nutanix MIB.
5. To add an SNMP transport, click the **Transports** tab and the **New Transport** button, and then do the following in the indicated fields. An SNMP transport is a combination of the transport protocol and port number on which you want the Nutanix SNMP agent to receive queries. SNMP transports enable you to combine transport protocols and port numbers other than the default port number. The port numbers that are specified in SNMP transports are unblocked on the Controller VM, making them available to receive queries:

   a. **Protocol**: Select the protocol to use from the drop-down list.

      The options are **TCP**, **TCP6**, **UDP**, and **UDP6**.

   b. **Port**: Enter the port number to use.

      The standard SNMP port number is 161. For the complete list of required ports, see Ports and Protocols.

   c. When the fields are correct, click the **Save** button (lower right).
      This saves the configuration and redisplays the dialog box with the new transport appearing in the list.

      Note: To return to the **SNMP Configuration** window without saving, click the **Cancel** button.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2206

6. To add an SNMP user entry, click the **Users** tab and the **New User** button and then do the following in the indicated fields:

   a. **Username**: Enter a user name.

   b. **Priv Type**: Select the privacy encryption type from the pull-down list.
   The only option is **AES** (Advanced Encryption Standard). In the nCLI, this setting is optional.

   c. **Priv Key**: Enter a privacy key phrase (password) into this field.

      - The key phrase is AES encrypted when the user is created.
      - The password you choose must meet the following complexity requirements:
        - Contain a minimum 8 characters and a maximum 64 characters.
        - Contain one upper case letter (A-Z).
        - Contain one lower case letter (a-z).
        - Contain one digit (0-9).
        - Contain only the following special characters: ~ @ # $ % * - = _ + { } | [ ] ? , . : &.

   d. **Auth Type**: Select the authentication hash function type from the drop-down list.
   The only option is **SHA** (Secure Hash Algorithm).

   e. **Auth Key**: Enter an authentication key phrase (password) into this field.

      - The key phrase is SHA-1 encrypted when the user is created.
      - The password you choose must meet the following complexity requirements:
        - Contain a minimum 8 characters and a maximum 64 characters.
        - Contain one upper case letter (A-Z).
        - Contain one lower case letter (a-z).
        - Contain one digit (0-9).
        - Contain only the following special characters: ~ @ # $ % * - = _ + { } | [ ] ? , . : &.

   f. When all the fields are correct, click the **Save** button (lower right).
   This saves the configuration and redisplays the dialog box with the new user entry appearing in the list.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2207

7. To add an SNMP trap receiver, click the **Traps** tab and the **New Trap Receiver** button, and then do the following in the indicated fields:

   a. **Receiver Name**: Enter the receiver name.

   b. **SNMP Version**: Select (click the radio button for) the SNMP version, either v3 or v2c. For SNMP v2c, Nutanix supports only SNMP TRAP and not SNMP GET.

   c. This field is displayed based on your selection in the **SNMP Version**:

      - **Trap Username**: This field is displayed if you select v3 in the **SNMP Version**. Select a user from the drop-down list.
      - **Community**: This field is displayed if you select v2c in the **SNMP Version**. The default value for v2c trap community is public, or you can enter any other name of your choice.

      All users added previously (see Step 5) appear in the drop-down list. You cannot add a trap receiver entry until at least one user has been added.

   d. **Address**: Enter the target address.

      An SNMP target address specifies the destination and user that receives outgoing notifications, such as trap messages. SNMP target address names must be unique within the managed device.

   e. **Port**: Enter the port number to use.

      The standard SNMP port number is 161. For the complete list of required ports, see Ports and Protocols.

   f. **Engine ID**: Optionally, enter an engine identifier value, which must be a hexadecimal string between 5 and 32 characters long.

      If you do not specify an engine ID, an engine ID is generated for you for use with the receiver. Every SNMP v3 agent has an engine ID that serves as a unique identifier for the agent. The engine ID is used with a hashing function to generate keys for authentication and encryption of SNMP v3 messages.

   g. **Inform**: Select **True** from the drop-down list to use inform requests as the SNMP notification method; select **False** to use traps as the SNMP notification method.

      SNMP notifications can be sent as traps or inform requests. Traps are one-way transmissions; they do not require an acknowledgment from the receiver. Informs expect a response. If the sender never receives a response, the inform request can be sent again. Therefore, informs are more reliable than traps. However, informs consume more resources. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, while an inform may be retried several times. The retries increase traffic and add overhead on the network. Thus, traps and inform requests provide a trade-off between reliability and resources.

      > **Note:** The SNMP server is blocked if it doesn't get a response to the inform traps in five consecutive attempts.

   h. **Transport Protocol**: Select the protocol to use from the drop-down list.

      The options are **TCP**, **TCP6**, **UDP**, and **UDP6**.

   i. When all the fields are correct, click the **Save** button (lower right).
      This saves the configuration and redisplays the dialog box with the new trap entry appearing in the list.

   j. To test all configured SNMP traps, click the **Traps** tab, and then click **Test All**.
      The Nutanix cluster sends test alerts to all the SNMP trap receivers configured on the cluster.

8. To edit a user or trap receiver entry, click the appropriate tab (**Users** or **Traps**) and then click the pencil icon for that entry in the list.
   An edit window appears for that user or trap receiver entry with the same fields as the add window. (Transport entries cannot be edited.) Enter the new information in the appropriate fields and then click the **Save** button.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2208

9. To delete an SNMP entry, click the appropriate tab (**Transports**, **Users**, or **Traps**) and then click the X icon for that entry in the list.
   A window prompt appears to verify the delete action; click the **OK** button. The entry is removed from the list.

Nutanix MIB

Overview

The Simple Network Management Protocol (SNMP) enables administrators to monitor network-attached devices for conditions that warrant administrative attention. In the Nutanix SNMP implementation, information about entities in the cluster is collected and made available through the Nutanix MIB (NUTANIX-MIB.txt). The Nutanix enterprise tree is located at 1.3.6.1.4.1.41263.

The Nutanix MIB is divided into the following sections:

- *Cluster information*. Status information about the cluster as a whole.
- *Software version information*. Version information about the software packages that comprise the Controller VM.
- *Service status information*. Information about the status of essential services on each Controller VM.
- *Hypervisor information*. Information about each hypervisor instance.
- *Virtual machine information*. Information about hosted virtual machines.
- *Disk information*. Status information about the disks in the cluster.
- *Controller VM resource information*. Indicate how much CPU and memory capacity is available to a Controller VM.
- *Storage pool information*. Status information about the storage pools in the cluster.
- *Storage Container information*. Status information about the disks in the cluster.
- *Alerts information*. Information about generated alerts that can be captured through the SNMP trap (or inform) mechanism.

> **Important:** A statistic (counter) value resets to zero and starts increasing again after it reaches the maximum limit defined for its corresponding data type. The counter reinitialization is compliant with the *RFC 2578* standard.
>
> For example, the *vmRxBytes* statistic monotonically increases until it reinitializes on reaching a maximum value of its data type (Counter64).

Table 66: Cluster Information Fields

Name	Description	Data Type
clusterName	Cluster name.	Display string
clusterVersion	Cluster version number. This is the Nutanix core package version expected on all the Controller VMs.	Display string
clusterStatus	Current status of the cluster. Possible values are *started* and *stopped*.	Display string
clusterTotalStorageCapacity	Total storage capacity of the cluster in bytes.	Unsigned 64-bit integer
clusterUsedStorageCapacity	Storage used on the cluster, in bytes.	Unsigned 64-bit integer

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2209

Name	Description	Data Type
clusterIops	Average I/O operations per second (IOPS) in the cluster.	Unsigned 64-bit integer
clusterLatency	Average I/O latency in the cluster, in milliseconds.	Unsigned 64-bit integer
clusterIOBandwidth	Cluster-wide I/O bandwidth in kilobytes per second (KBps).	Unsigned 64-bit integer

Table 67: Software Version Information Fields

Name	Description	Data Type
svtIndex	Unique index that is used to identify an entry in the software version information table.	Signed 32-bit integer
svtControllerVMId	Nutanix Controller VM identification number.	Display string
svtNutanixBootstrap	Nutanix bootstrap software package version.	Display string
svtNutanixInfrastructure	Nutanix infrastructure software package version.	Display string
svtNutanixCore	Nutanix core software package version.	Display string
svtNutanixToolchain	Nutanix toolchain software package version.	Display string
svtNutanixServiceability	Nutanix serviceability software package version.	Display string
svtLinuxKernel	Linux kernel version currently installed.	Display string

Table 68: Service Status Information Fields

Name	Description	Data Type
cstIndex	Unique index that is used to identify an entry in the service status information table.	Signed 32-bit integer
cstControllerVMId	Nutanix Controller VM identification number.	Display string
cstControllerVMStatus	Status of the Nutanix node.	Display string
cstDataServiceStatus	Status of the core data services on the Controller VM.	Display string
cstMetadataServiceStatus	Status of the metadata services on the Controller VM.	Display string

Table 69: Hypervisor Information Fields

Name	Description	Data Type
hypervisorIndex	Number that is used to uniquely identify an entry in the hypervisor information table.	Signed 32-bit integer

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2210

Name	Description	Data Type
hypervisorID	System-generated string that Nutanix uses to uniquely identify a hypervisor instance.	Display string
hypervisorName	Name of the hypervisor instance.	Display string
hypervisorVmCount	Number of VMs configured on the hypervisor instance.	Unsigned 32-bit integer
hypervisorCpuCount	Number of CPU cores available to the hypervisor instance.	Unsigned 32-bit integer
hypervisorCpuUsagePercent	Percentage of CPU resources in use by the hypervisor instance.	Unsigned 32-bit integer
hypervisorMemory	Total memory available to the hypervisor instance, in bytes.	Counter64
hypervisorMemoryUsagePercent	Memory in use by the hypervisor instance, as a percentage of the total available memory.	Unsigned 64-bit integer
hypervisorReadIOPerSecond	Total number of read I/O operations per second (IOPS) being performed by the hypervisor.	Unsigned 32-bit integer
hypervisorWriteIOPerSecond	Total number of write I/O operations per second (IOPS) being performed by the hypervisor.	Unsigned 32-bit integer
hypervisorAverageLatency	Average I/O latency of the hypervisor in microseconds (µs).	Counter64
hypervisorIOBandwidth	I/O bandwidth of the hypervisor in kilobytes per second (KBps).	Counter64
hypervisorRxBytes	Total number of bytes received by the hypervisor.	Counter64
hypervisorTxBytes	Total number of bytes transmitted by the hypervisor.	Counter64
hypervisorRxDropCount	Total number of packets dropped by the hypervisor when receiving data.	Counter64
hypervisorTxDropCount	Total number of packets dropped by the hypervisor when transmitting data.	Counter64

Table 70: Virtual Machine Information Fields

Name	Description	Data Type
vmIndex	Number that is used to uniquely identify an entry in the VM information table.	Signed 32-bit integer
vmId	System-generated string that Nutanix uses to uniquely identify a virtual machine.	Display string
vmName	Name of the VM.	Display string
vmHypervisorId	System-generated ID of the hypervisor on which the VM is provisioned.	Display string
vmPowerState	Power state of the VM.	Display string

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2211

Name	Description	Data Type
vmCpuCount	Number of CPU cores available to the VM.	Unsigned 32-bit integer
vmCpuUsagePercent	Percentage of CPU resources in use by the VM.	Unsigned 32-bit integer
vmMemory	Total memory allocated to the VM, in bytes.	Counter64
vmMemoryUsagePercent	Memory in use by the VM, as a percentage of the total allocated memory.	Unsigned 64-bit integer
vmReadIOPerSecond	Total number of read I/O operations per second (IOPS) being performed by the VM.	Unsigned 32-bit integer
vmWriteIOPerSecond	Total number of write I/O operations per second (IOPS) being performed by the VM.	Unsigned 32-bit integer
vmAverageLatency	Average I/O latency of the VM, in microseconds (µs).	Counter64
vmIOBandwidth	I/O bandwidth of the VM in kilobytes per second (KBps).	Counter64
vmRxBytes	Total number of bytes received by the VM.	Counter64
vmTxBytes	Total number of bytes transmitted by the VM.	Counter64
vmRxDropCount	Total number of packets dropped by the VM when receiving data.	Counter64
vmTxDropCount	Total number of packets dropped by the VM when transmitting data.	Counter64

Table 71: Disk Information Fields

Name	Description	Data Type
dstIndex	Number that is used to uniquely identify an entry in the disk information table.	Signed 32-bit integer
dstDiskId	Disk identification number. The number is unique for each disk.	Display string
dstControllerVMId	Nutanix Controller VM identification number.	Display string
dstSerial	Disk serial number.	Display string
dstNumRawBytes	Physical storage capacity on the device, in terms of number of raw bytes.	Unsigned 64-bit integer
dstNumTotalBytes	Usable storage on the device through its file system, in terms of number of usable bytes.	Unsigned 64-bit integer
dstNumFreeBytes	Available storage on the device through its file system for non-root users, in terms of number of free bytes.	Unsigned 64-bit integer
dstNumTotalInodes	Total number of usable inodes on the device through its file system.	Unsigned 64-bit integer

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2212

Name	Description	Data Type
dstNumFreeInodes	Total number of available (free) inodes on the device through its file system for non-root users.	Unsigned 64-bit integer
dstAverageLatency	Average I/O latency of the disk in microseconds (µs).	Unsigned 64-bit integer
dstIOBandwidth	I/O bandwidth of the disk in kilobytes per second (KBps).	Unsigned 64-bit integer
dstNumberIops	Current number of I/O operations per second (IOPS) for the disk.	Unsigned 64-bit integer
dstState	State of the disk.	Signed 32-bit integer

Table 72: Controller VM Resource Information Fields

Name	Description	Data Type
crtIndex	Number that is used to uniquely identify an entry in the Controller VM resource information table.	Signed 32-bit integer
crtControllerVMId	Nutanix Controller VM identification number.	Display string
crtMemory	Total memory available to the Controller VM in bytes.	Unsigned 64-bit integer
crtNumCpus	Total number of CPUs allocated to the Controller VM.	Signed 32-bit integer
crtName	Name of the Controller VM.	Display string

Table 73: Storage Pool Information Fields

Name	Description	Data Type
spitIndex	Number that is used to uniquely identify an entry in the storage pool information table.	Signed 32-bit integer
spitStoragePoolId	Storage pool identification number.	Display string
spitStoragePoolName	Storage pool name.	Display string
spitTotalCapacity	Total storage pool capacity in bytes.	Unsigned 64-bit integer
spitUsedCapacity	Used storage pool capacity in bytes.	Unsigned 64-bit integer
spitIOPerSecond	Current number of I/O operations per second (IOPS) for this storage pool.	Signed 32-bit integer
spitAvgLatencyUsecs	Average I/O latency for the storage pool in microseconds.	Unsigned 64-bit integer
spitIOBandwidth	I/O bandwidth of the storage pool in kilobytes per second (KBps).	Unsigned 64-bit integer

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2213

Table 74: Storage Container Information Fields

Name	Description	Data Type
citIndex	Number that is used to uniquely identify an entry in the storage container information table.	Signed 32-bit integer
citContainerId	Storage Container identification number.	Display string
citContainerName	Storage Container name.	Display string
citTotalCapacity	Total storage container capacity in bytes.	Unsigned 64-bit integer
citUsedCapacity	Used storage container storage in bytes.	Unsigned 64-bit integer
citIOPerSecond	Current number of I/O operations per second (IOPS) for this storage container.	Signed 32-bit integer
citAvgLatencyUsecs	Average I/O latency for the storage container in microseconds.	Unsigned 64-bit integer
citIOBandwidth	I/O bandwidth of the storage container in kilobytes per second (KBps).	Unsigned 64-bit integer

Trap Resolution

In addition to generating an SNMP trap when an alert condition is detected, Nutanix clusters generate a trap when an alert condition is resolved. The resolved trap, named ntxTrapResolved, is generated regardless of whether the alert condition is resolved manually or automatically. If a Prism Central alert is resolved in Prism Central, Prism Central sends a resolved trap. If a Nutanix cluster alert is resolved in either the Prism Element web console or Prism Central, both Prism Central and the cluster send a resolved trap.

In this section, the terms *original alert* and *original trap* are used to refer, respectively, to the alert and trap that are generated when the alert condition is detected, and the terms *resolved alert* and *resolved trap* are used to refer, respectively, to the alert and trap that are generated when the alert condition is resolved.

To enable you to associate a resolved trap with the original alert and original trap, the UUID of the original alert is included in the original trap, as part of the alert message (ntxAlertDisplayMsg), and in the resolved trap, as a MIB object (ntxAlertUuid).

A resolved trap has the following MIB objects:

- ntxTrapName (name of the original trap)
- ntxAlertUuid (UUID of the original alert)
- ntxAlertResolvedTime
- ntxAlertDisplayMsg (message of the original alert)
- ntxAlertTitle (title of the original alert)
- ntxAlertSeverity (severity of the original alert)

The fields are described in the rows that follow.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2214

Table 75: Alerts Information Fields

Name	Description	Data Type
ntxAlertCreationTime	Time of alert creation. The value is the number of seconds since the UNIX epoch (01/01/1970).	Unsigned 64-bit integer
ntxAlertDisplayMsg	Alert message text.	Display string
ntxAlertTitle	Alert title.	Display string
ntxAlertSeverity	Alert severity, which has one of the following values: 1. Informational 2. Warning 3. Critical 4. Audit	Integer
ntxTrapName	Name of the trap that was generated when the alert condition was detected. This MIB object is included in resolved traps.	Display string
ntxAlertUuid	UUID of the alert that was generated when the alert condition was detected. This MIB object is included in resolved traps.	Display string
ntxAlertResolvedTime	Time at which the alert was resolved. The value is the number of seconds since the UNIX epoch (01/01/1970). This MIB object is included in resolved traps.	Unsigned 64-bit integer

Configuring a Banner Page

You have the option to create a welcome banner, which will be the first screen that appears when a user attempts to log into the web console. The content of the banner page is configurable, and it can include a custom message and graphics.

About this task

To configure a banner page, do the following:

Procedure

1. Log in to the Prism Element web console.
2. Click the gear icon in the main menu and then select **Welcome Banner** in the **Settings** page.
   The **Edit Welcome Banner** dialog box appears.
3. Enter (paste) the desired content in HTML format in the pane on the left.
   Only *safe* HTML tags are supported. Inline event handlers, scripts, and externally-sourced graphics are not allowed.
4. Click the **Preview** button to display the banner in the pane on the right.
5. If the banner is not correct, update the HTML code as needed until the preview pane displays the desired message.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2215

6. When the preview is correct, check the **Enable Banner** box (lower left) and then the **Save** button.

   You can disable (or enable) the banner at any time by clearing (selecting) the **Enable Banner** checkbox.

   Note: A live banner page includes an *Accept terms and conditions* bar at the bottom. Clicking on this bar sends the user to the login page.

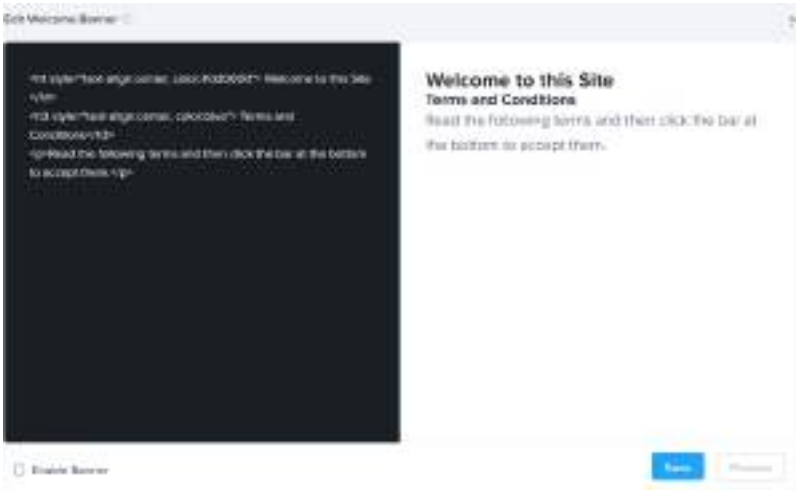


Figure 47: Welcome Banner Window

Registering a Cluster to vCenter Server

To perform core VM management operations directly from Prism without switching to vCenter Server, you need to register your cluster with the vCenter Server.

Before you begin

Ensure that you have vCenter Server Extension privileges as these privileges provide permissions to perform vCenter registration for the Nutanix cluster.

About this task

Following are some of the important points about registering vCenter Server.

- Nutanix does not store vCenter Server credentials.
- Whenever a new node is added to Nutanix cluster, vCenter Server registration for the new node is automatically performed.
- Nutanix supports vCenter Enhanced Linked Mode.

  When registering a Nutanix cluster to a vCenter Enhanced Linked Mode (EHM) enabled ESXi environment, ensure that Prism is registered to the vCenter containing the vSphere Cluster and Nutanix nodes (often the local vCenter). For information on vCenter Enhanced Linked Mode, see *vCenter Enhanced Linked Mode* in the *vCenter Server Installation and Setup* documentation.

Procedure

1. Log into the Prism Element web console.
2. Click **Settings** from the drop-down menu of the Prism Element web console and then select **vCenter Registration** in the **Settings** page.

   The vCenter Server that is managing the hosts in the cluster is auto-discovered and displayed.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2216

3. Click the **Register** link.

   The IP address is auto-populated in the **Address** field. The port number field is also auto-populated with 443. Do not change the port number. For information on the complete list of required ports, see Ports and Protocol.

4. Type the administrator user name and password of the vCenter Server in the **Admin Username** and **Admin Password** fields.

5. Click **Register**.

   During the registration process a certificate is generated to communicate with the vCenter Server. If the registration is successful, relevant message is displayed in the **Tasks** dashboard. The Host Connection field displays as Connected, which implies that all the hosts are being managed by the vCenter Server that is registered.

Unregistering a Cluster from the vCenter Server

To unregister the vCenter Server from your cluster, perform the following procedure.

About this task

- Ensure that you unregister the vCenter Server from the cluster before changing the IP address of the vCenter Server. After you change the IP address of the vCenter Server, you should register the vCenter Server again with the new IP address with the cluster.
- The vCenter Server Registration page displays the registered vCenter Server. If for some reason the Host Connection field changes to **Not Connected**, it implies that the hosts are being managed by a different vCenter Server. In this case, there will be new vCenter entry with host connection status as Connected and you need to register to this vCenter Server.

Procedure

1. Log into the Prism Element web console.

2. Click **Settings** from the drop-down menu of the Prism Element web console and then select **vCenter Registration** in the **Settings** page.

   A message that cluster is already registered to the vCenter Server is displayed.

3. Type the administrator user name and password of the vCenter Server in the **Admin Username** and **Admin Password** fields.

4. Click **Unregister**.

   If the credentials are correct, the vCenter Server is unregistered from the cluster and a relevant message is displayed in the **Tasks** dashboard.

Managing vCenter Server Registration Changes

After you change the password or the IP address of the vCenter Sever or if current vCenter Server is not managing the hosts then the Host Connection field changes to **Not Connected** (may occur if current vCenter Server is not managing the hosts), you must register your cluster with the new vCenter Server. Perform the following procedure to re-register the vCenter Server.

Procedure

1. Log into the Prism Element web console.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2217

2. Click the gear icon in the main menu and then select **vCenter Registration** in the **Settings** page.

   The vCenter Server that is managing the hosts in the cluster is displayed along with the vCenter Server that you must unregister.

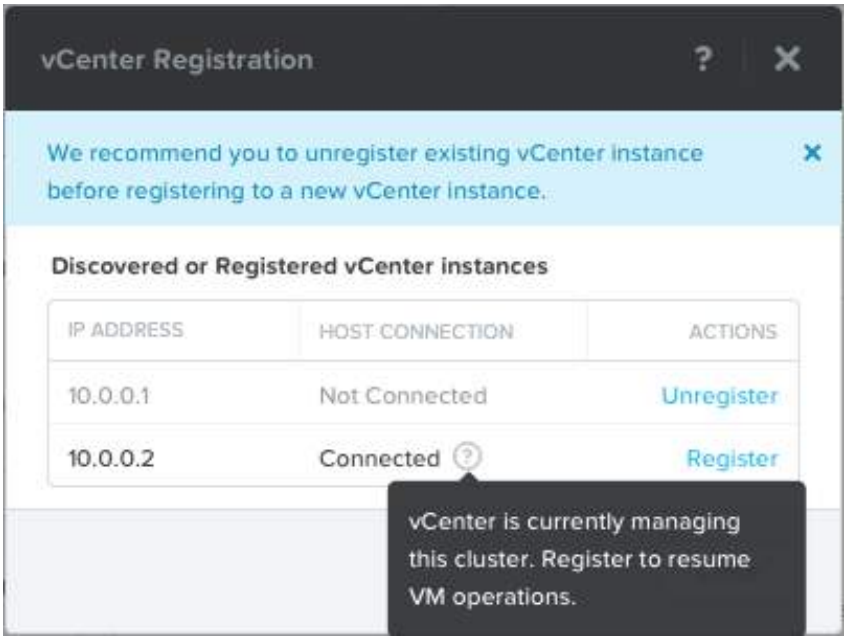


Figure 48: vCenter Registration Management

3. Unregister the existing vCenter Server instance by clicking **Unregister**.

   For more information about unregistering vCenter Server, see Unregistering a Cluster from the vCenter Server on page 367.

4. Register the new vCenter Server instance by clicking **Register**.

   For more information about registering vCenter Server, see Registering a Cluster to vCenter Server on page 366.

In-Place Hypervisor Conversion

The In-place hypervisor conversion feature provides you with an option to convert your existing ESXi cluster to an AHV cluster. All the VMs that are running in the ESXi cluster are converted so that they can run on the AHV cluster. The VM conversion is independent of the host that the VM is running on. The conversion process occurs in such a way that the VM down time is minimised. You can also convert the cluster back to ESXi. This conversion from AHV to ESXi is a file system restore of the host. Hence the cluster will be similar to what it was before the conversion.

Note:

- This feature converts your existing ESXi cluster to an AHV cluster. You cannot start the conversion process on the AHV cluster.
- Do not remove the hosts from the vCenter Server if you want to perform the reverse conversion process (AHV to ESXi).
- This feature is supported on the clusters with multiple hypervisors (combination of ESXi nodes with one AHV node or multiple AHV nodes).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2218

- When you are converting the cluster from ESXi to AHV, remove the unused adapters displayed under **Teaming and Failover** in vCenter Server and keep only those adapters that are active and of the same speeds as the standby and active adapters.

Following are enhancements to In-Place Hypervisor Conversion feature.

- **Decreased VM downtime**: With the implementation of the new workflow of converting the nodes in the cluster in a rolling manner, the VM downtime is reduced to only shutdown time and conversion time required for that particular VM. Approximately, the VM downtime has been reduced from 3 to 4 hours to less than 5 minutes.
- **Prism state**: The Prism console is responsive during the conversion process. However, Prism goes into read-only state.
- **State of the VM**: The current state of the VM is preserved and the VM is brought back into the same state post conversion. For example, the VM is automatically powered on post conversion if that VM was powered on before you started the conversion.
- **Preservation of the MAC addresses of the VM NICs**: After cluster conversion to AHV or ESXi, the MAC addresses of the VM NICs are preserved. The preservation of the IP address depends on the operating system. Typically, some Linux operating systems preserve the IP address when the MAC address is preserved, but Windows operating systems do not.
- VMs that were created after conversion to AHV are retained post conversion back to ESXi.

Requirements and Limitations for In-Place Hypervisor Conversion

Following are the prerequisites with the requirements and limitations for an in-place hypervisor conversion.

Prerequisites

- Before performing In-place hypervisor conversion, ensure that you resolve all the NCC health check alerts (warnings, failures and errors) and upgrade the firmware to the latest version using LCM firmware upgrade.
- HA and DRS must be enabled.
- All the hosts must be managed by the same vCenter Server.
- The vCenter Server VM that is managing the cluster must not be running on the cluster which is being converted.
- Install NGT on all the VMs. For more information, see Enabling NGT and Mounting the NGT Installer in a VM on page 306. If NGT is not installed, the VM does not boot after conversion.

  Note: You can convert an ESXi cluster, which hosts a Prism Central VM, to an AHV cluster without installing NGT in the Prism Central VM. After the conversion, the Prism Central VM starts successfully.
- All hardware platforms are supported.
- Ensure that you have all the ESXi ISOs (if you have more than one version of ESXi running in your cluster) at the foundation/isos/hypervisor/esx/ location. This ISO image or images are used to bring the cluster back to its pre-conversion state if you abort the cluster conversion operation from ESXi to AHV.

General Limitations

In-place hypervisor conversion has the following limitations:

- Clusters with container-level encryption are not supported for conversion.
- Metro availability protection domains cannot be enabled in your environment.
- You cannot have Nutanix Files deployed in your cluster.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2219

- Affinity policies (if configured) are not honored after conversion to AHV.
- In-place hypervisor conversion is not supported for single-node clusters and two-node clusters.
- VMware snapshots (snapshots created through vCenter or ESXi) must not be created during in-place hypervisor conversion because it can lead to cluster conversion failure. Therefore, pause any backup schedules (created manually or by backup applications) before starting an in-place hypervisor conversion.

ESXi Supported Versions

Table 76: Supported ESXi Versions

Version	Support
5.5	All the versions that are included in the ISO Whitelist (see ~/foundation/config/iso_whitelist.json file) that is bundled with AOS are supported. If you have upgraded foundation by using standalone foundation, the ISO Whitelist is invalidated. In this case, you need to see the original Whitelist that was present before you performed the upgrade. To verify the json file that was bundled with AOS, see the nutanix-packages.json file.
6.0	
6.5	
6.7	
7.0	
8.0	

ESXi Network Requirements and Limitations

Table 77: ESXi Network Requirements and Limitations

Component	Description
NIC	Minimum of two or more homogenous NICs of 1 GB, 10 GB, or 40 GB are supported.
vSwitch	• Each host must have only one external vSwitch. If you have more than one external vSwitch conversion validation fails. • Ensure you have one active and multiple passive failover configuration of NICs on vSwitch. • Active/active load balancing policies are not supported and is converted to active/passive on AHV. • For a standard switch configuration it is recommended that all the port groups are present on all the hosts because there might be a possibility that the conversion process might move the VMs to a different host.
Distributed vSwitch	Each host must have only one external distributed vSwitch. If you have more than one external distributed vSwitch conversion validation fails.
Internal vSwitch	Internal vSwitch apart from Nutanix vSwitch is not supported.
LACP	Not supported.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2220

- The vSwitch is converted to an open vSwitch on the AHV side. If you perform any configuration changes on AHV, these changes may not be maintained after converting the cluster back to ESXi.
- Networks not in use by a VM prior to the cluster conversion may not be converted.
- All the VMs may end up on a single host during conversion back to ESXi. The network configuration that you might have defined for the VMs may not be maintained.
- After migration to AHV, NIC may not have same type of virtualized hardware device (for example VMXNET3 may be E1000 after conversion).
- Serial ports and virtual graphics processing unit (vGPU) configurations may be lost after conversion.

Virtual Machine Requirements and Limitations

- Only VMs with flat disks are supported. The delta disks are not supported.
- Only IDE and SCSI storage controllers are supported for automatic conversion. SATA and PCI disks are not supported.
- On Windows VMs, set the SAN policy to **OnlineAll** for non-boot SCSI disks so that they can be automatically brought online. For more information about setting SAN policy, see Bringing Multiple SCSI Disks Online.
- VMs that have NFS datastore folders with vSphere tagging can not be converted.
- Virtual machines with attached volume groups or shared virtual disks are not supported.
- After reverting back to ESXi from AHV, the VMs are converted to the maximum hardware version that is supported by that specific ESXi version.
- Guest OS network interfaces on Linux VMs may change to generic type during ESXi to AHV conversion (for example, in RHEL 7 network interface enoXXXX changes to eth0). You may have to reconfigure the network settings according to changes post conversion.
- Guest OS type for the Linux VMs may change to a more generic type (for example RHEL 7 may change to Other Linux 64-bit) during the conversion back from AHV to ESXi.

Supported Operating Systems

Table 78: Supported Operating Systems

Operating System	Versions	Limitations
Windows	• Windows 2008 R2 or later versions • Windows 7 or later versions	• Only 64-bit operating systems are supported.
Linux	• CentOS 6.5 and 7.0 • Red Had Enterprise Linux (RHEL) 6.5 or later and RHEL 7.0 or later. • Oracle Linux 6.5 and 7.0 • Ubuntu 14.04	SUSE Linux Enterprise Server (SLES) operating system is not supported.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2221

In-Place Hypervisor Conversion Process

ESXi to AHV

After you start the conversion process, all the nodes in the cluster are converted in a rolling manner to AHV one node at a time. During conversion, the first node is placed in the maintenance mode and all the VMs that are running on the node are migrated to other ESXi nodes in the cluster using the HA and DRS feature. After the VMs are migrated, the node is converted to AHV. After node is successfully converted, all VMs that were migrated to ESXi are migrated one at a time to AHV. Similar steps are performed for the rest of the nodes in the ESXi cluster until the last ESXi node. The VMs that are running on the last ESXi node in the cluster are converted and migrated to the AHV hosts and then the ESXi host is converted to AHV. If any error occurs during VM conversion, appropriate alerts or error messages are displayed. When converting a VM the source vdisk is not modified. Therefore, if there are any fatal errors during imaging, storing, or restoring of the configuration, the conversion is stopped and you are prompted to abort the conversion.

> **Note:** After conversion, do not remove the host from the vCenter Server until you are sure that the conversion is successful, because it may impact the reverse conversion process.

Port Groups and VLAN Transformation

Before the conversion all of the ESXi port groups, VLAN IDs, and virtual machines that belong to a particular group are captured. On AHV, a corresponding Acropolis virtual network is created for every unique ESXi port group on the cluster including any corresponding VLAN ID, and then associated with the VMs. If the ESXi host has a VLAN set on the management port group, after conversion the Acropolis management interface and the Controller VM public interface are placed in that same VLAN.

AHV to ESXi

During the reverse conversion (AHV to ESXi), the process of conversion is similar. Additionally, if the cluster does not have the ESXi ISO stored on the cluster, you need to provide the ESXi ISO image during the conversion process.

> **Note:**
>
> - The image that you provide should be of the same major ESXi version that you have used during ESXi to AHV conversion.
> - If new nodes were added to the cluster after conversion to AHV, then these nodes need to be removed before starting the reverse conversion process.

After conversion to ESXi, all the hosts are automatically registered to the vCenter Server.

Converting Cluster (ESXi to AHV)

Perform the following procedure to convert the cluster from ESXi to AHV.

Before you begin

Verify that you have met all the networking and virtual machine requirements as described in Requirements and Limitations for In-Place Hypervisor Conversion on page 369.

About this task

Procedure

1. Log into the Prism Element web console.
2. Click the gear icon in the main menu and then select **Convert Cluster** in the **Settings** page.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2222

3. From the **Available Hypervisor** drop-down menu, select **AHV**.
4. Select the state of the VMs that you want post conversion from the **VM Boot Options** drop-down menu.
   - **Preserve power state of the user VMs**: Select this option if you want to keep the original power state of the VMs. For example, if you want the VMs to be in a running state post conversion automatically, select this option.
   - **Power Off User VMs**: Select this option if you want power off all the VMs running on ESXi cluster before you start the conversion process. After conversion, these VMs will be in the powered off state.
5. Click **Validate** to enter vCenter Server credentials and to verify whether you have met all the requirements.
6. Enter the IP address of the vCenter Server in the **vCenter Sever IP Address** along with the administrator user name and password of the vCenter Server in the **Username** and **Password** fields.
7. Click **Yes**.
   A validation that you have met all the requirements is performed. Once the validation is successful the conversion process proceeds. If validation fails (for any reason), a relevant message to take appropriate action is displayed.
8. Click **Convert Cluster**.
   A confirmation message is displayed.

   Note: The cluster changes to Read Only mode. A message Oops - server Error may be displayed when the Prism node is undergoing conversion. Wait for the conversion process to complete. You can access other Controller VM for Read-Only Prism operations.

   The entire conversion process may take 3 to 4 hours depending on the nodes that are present in your cluster. However, the VM downtime will be less than 5 minutes because all the nodes in the cluster are converted in a rolling manner. You can also track the progress of the conversion by logging again into the web console.

Converting Cluster (AHV to ESXi)

Perform the following procedure to convert the cluster back to ESXi from AHV.

About this task

Perform this procedure only if you have converted your cluster from ESXi to AHV. You cannot start the conversion process on the AHV cluster.

Before you begin

Ensure that you have met all the networking and virtual machine requirements as described in Requirements and Limitations for In-Place Hypervisor Conversion on page 369 topic.

Procedure

1. Log into the Prism Element web console.
2. Click the gear icon in the main menu and then select **Convert Cluster** in the **Settings** page.
3. From the **Available Hypervisor** drop-down menu, select **ESXi**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2223

4. Select the state of the VMs that you want post conversion from the **VM Boot Options** drop-down menu.

   » **Preserve power state of the user VMs**: Select this option if you want to keep the original power state of the VMs. For example, if you want the VMs to be in a running state post conversion automatically, select this option.

   » **Power Off User VMs**: Select this option if you want power off all the VMs running on ESXi cluster before you start the conversion process. After conversion, these VMs will be in the powered off state.

5. Click **Validate** to enter vCenter Server credentials and to verify whether you have met all the requirements.

6. Enter the IP address of the vCenter Server in the **vCenter Sever IP Address** along with the administrator user name and password of the vCenter Server in the **Username** and **Password** fields.

7. Click **Yes**.

   A validation that you have met all the requirements is performed. Once the validation is successful the conversion process proceeds. If validation fails (for any reason), a relevant message to take appropriate action is displayed.

8. Click **Convert Cluster** button to start the conversion process.

9. (Optional) If you have not saved the ESXi ISOs at the foundation/isos/hypervisor/esx/ location, click **Choose File** and select the ESXi ISO.

   > **Note:** If you have different versions of ESXi running in your cluster, you have to perform this step for every version of ESXi ISO.

10. Click **Convert**.

    All cluster operations stops and you will not be able to perform any operations on the cluster while the conversion is in progress. A message to this effect is displayed.

11. Click **Yes** to proceed with the conversion.

    The conversion begins. The time taken to finish the conversion is dependent on your environment. For example, it might take between 2 to 3 hours for the conversion to finish for a 3 or 4 nodes cluster. However, the VM downtime will be less than 5 minutes.

Stopping Cluster Conversion

If any issues occur with the cluster conversion process, a message to stop the cluster conversion or to continue with the conversion process is displayed. Depending on the type of message, you can appropriate action.

Before you begin

Ensure that you have saved the ESXi ISO at the foundation/isos/hypervisor/esx/ location. This ISO image is used to bring the cluster back to its pre-conversion state if you stop the cluster conversion operation from ESXi to AHV.

About this task

Issues in the cluster conversion process might occur because of the following reasons.

- Imaging Issue: If this issue occurs, you can only stop the cluster conversion process and a relevant message is displayed. Aborting the conversion reverts the cluster back to the its original state.
- VM Conversion Issue: If this issue occurs, you can either stop the conversion or can continue with the process. If you decide to continue with the process, cluster conversion is completed keeping the current state of the VM. After conversion is completed, you must perform appropriate actions on the VMs to bring back the VMs.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2224

Procedure

Click **Abort** when a message to stop the cluster conversion is displayed.

The cluster goes back to its original state. You may need to manually power on the VMs depending on its state after you perform this operation.

Internationalization (i18n)

The following table lists all the supported and unsupported entities in UTF-8 encoding.

Table 79: Internationalization Support

Supported Entities	Unsupported Entities
Cluster name	Acropolis file server
Storage Container name	Share path
Storage pool	Internationalized domain names
VM name	E-mail IDs
Snapshot name	Hostnames
Volume group name	Integers
Protection domain name	Password fields
Remote site name	Any Hardware related names (for example, vSwitch, iSCSCI initiator, vLAN name)
User management	
Chart name	

Caution: The creation of none of the above entities are supported on Hyper-V because of the DR limitations.

Entities Support (ASCII or non-ASCII) for the Active Directory Server

- In the New Directory Configuration, **Name** field is supported in non-ASCII.
- In the New Directory Configuration, **Domain** field is not supported in non-ASCII.
- In Role mapping, **Values** field is supported in non-ASCII.
- User names and group names are supported in non-ASCII.

Localization (L10n)

Nutanix localizes the user interface in Simplified Chinese and Japanese language. All the static screens are translated to the selected locale language. All the dashboards (including tool tips) and menus of the Prism Element are localized.

You have an option to change the language settings of the cluster from English (default) to Simplified Chinese or Japanese. For more information, see Changing the Language Settings on page 376.

If the Prism Central instance is launched from the Prism Element, language settings of the Prism Central takes precedence over Prism Element.

You can also create new users with the specified language setting. For more information, see User Management.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2225

Conditions and Limitations

- Logical entities that do not have a contextual translation available in the localized language are not localized.
- The AOS generated alerts and events are not localized to the selected locale language.
- Following strings are not localized: VM, CPU, vCPU, Language Settings, licensing details page, hardware names, storage denominations (GB, TB), About Nutanix page, EULA, service names (SNMP, SMTP), hypervisor types.

Changing the Language Settings

Perform the following procedure to set the Prism language settings to a chosen language (English, simplified Chinese, or Japanese). You also have an option to set the calendar, date, and time format to a selected region.

Procedure

1. Log in to the Prism Element web console.
2. Click the gear icon in the main menu and then select **Language Settings** in the **Settings** page.
   The **Language Settings** dialog box appears.
3. To change the language, select the desired language from the **Languages** field pull-down menu.

   The **English** language is selected by default, but you can change that to either **Simplified Chinese** or **Japanese**.
4. To change the locale settings (date, time, calendar), select the appropriate region from the **Region** field drop-down menu.

   A default locale is set based on the language setting. However, you can change the region to display the date, time, and calendar in some other format. This format for date, time, and calendar is applied to the entire cluster.
5. When the settings are correct, click the **Save** button.

   The language and locale settings are changed according to the selection. For example, the language setting for a cluster can be changed to Chinese and the locale setting to Russian.

   For more information on the entities that are supported, see Internationalization (i18n) on page 375. For more information about localization, see Localization (L10n) on page 375.

Hyper-V Setup

Adding the Cluster and Hosts to a Domain

After completing foundation of the cluster, you need to add the cluster and its constituent hosts to the Active Directory (AD) domain. The adding of cluster and hosts to the domain facilitates centralized administration and security through the use of other Microsoft services such as Group Policy and enables administrators to manage the distribution of updates and hotfixes.

Before you begin

- If you have a VLAN segmented network, verify that you have assigned the VLAN tags to the Hyper-V hosts and Controller VMs. For information about how to configure VLANs for the Controller VM, see the Advanced Setup Guide.
- Ensure that you have valid credentials of the domain account that has the privileges to create a new computer account or modify an existing computer account in the Active Directory domain. An Active Directory domain created by using non-ASCII text may not be supported. For more information about usage of ASCII or non-ASCII text in Active Directory configuration, see Internationalization (i18n) in *Prism Element Web Console Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2226

Procedure

1. Log on to the Web Console by using one of the Controller VM IP address or by using cluster virtual IP address.
2. Click the gear icon in the main menu and select **Join Cluster and Hosts to the Domain** on the **Settings** page.
3. Enter the fully qualified name of the domain that you want to join the cluster and its constituent hosts to in the **Full Domain Name** field.
4. Enter the IP address of the name server in the **Name Server IP Address** field that can resolve the domain name that you have entered in the **Full Domain Name** field.
5. In the **Base OU Path** field, type the OU (organizational unit) path where the computer accounts must be stored after the host joins a domain. For example, if the organization is nutanix.com and the OU is Documentation, the Base OU Path can be specified as *OU=Documentation,DC=nutanix,DC=com*

   Specifying the Base OU Path is optional. When you specify the Base OU Path, the computer accounts are stored in the Base OU Path within the Active Directory after the hosts join a domain. If the Base OU Path is not specified, the computer accounts are stored in the default Computers OU.
6. Enter a name for the cluster in the **Nutanix Cluster Name** field.

   The maximum length of the cluster name should not be more than 15 characters and it should be a valid NetBIOS name.
7. Enter the virtual IP address of the cluster in the **Nutanix Cluster Virtual IP Address** field.

   If you have not already configured the virtual IP address of the cluster, you can configure it by using this field.
8. Enter the prefix that should be used to name the hosts (according to your convention) in the **Prefix** field.

   - The prefix name should not end with a period.
   - The maximum length of the prefix name should not be more than 11 characters.
   - Should be a valid NetBIOS name.

     For example, if you enter prefix name as Tulip, the hosts are named as Tulip-1, Tulip-2, and so on, in the increasing order of the external IP address of the hosts.

   If you do not provide any prefix, the default name of NTNX-`block-number` is used. Click **Advanced View** to see the expanded view of all the hosts in all the blocks of the cluster and to rename them individually.
9. In the **Credentials** field, enter the logon name and password of the domain account that has the privileges to create a new or modify an existing computer accounts in the Active Directory domain.

   Ensure that the logon name is in the `DOMAIN\USERNAME` format. The cluster and its constituent hosts require these credentials to join the AD domain. Nutanix does not store the credentials.
10. When all the information is correct, click **Join**.
    The cluster is added to the domain. Also, all the hosts are renamed, added to the domain, and restarted. Allow the hosts and Controller VMs a few minutes to start. After the cluster is ready, the logon page is displayed.

What to do next

Create a Microsoft failover cluster. For more information, see Creating a Failover Cluster for Hyper-V on page 377.

Creating a Failover Cluster for Hyper-V

Before you begin

Perform the following tasks before you create a failover cluster:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2227

- Join the hosts to the domain as described in Adding the Cluster and Hosts to a Domain.
- Ensure that the Windows failover cluster IP address and hypervisor or host IP address are in the same subnet.

Perform the following procedure to create a failover cluster that includes all the hosts in the cluster.

Procedure

1. Log on to the Prism Element web console by using one of the Controller VM IP addresses or by using the cluster virtual IP address.
2. Click the gear icon in the main menu and select **Configure Failover Cluster** from the **Settings** page.
3. Type the failover cluster name in the **Failover Cluster Name** field.

   The maximum length of the failover cluster name must not be more than 15 characters and must be a valid NetBIOS name.
4. Type an IP address for the Hyper-V failover cluster in the **Failover Cluster IP Address** field.

   This address is for the cluster of Hyper-V hosts that are currently being configured. It must be unique, different from the cluster virtual IP address and from all other IP addresses assigned to the hosts and Controller VMs. It must be in the same network range as the Hyper-V hosts.
5. In the **Credentials** field, type the logon name and password of the domain account that has the privileges to create a new account or modify existing accounts in the Active Directory domain.

   The logon name must be in the format `DOMAIN\USERNAME`. The credentials are required to create a failover cluster. Nutanix does not store the credentials.
6. Click **Create Cluster**.

   A failover cluster is created by the name that has been provided and it includes all the hosts in the cluster.

   For information on manually creating a failover cluster, see Manually Creating a Failover Cluster (SCVMM User Interface) on page 378.

Manually Creating a Failover Cluster (SCVMM User Interface)

About this task

Perform the following procedure to manually create a failover cluster for Hyper-V by using System Center VM Manager (SCVMM).

If you are not using SCVMM or are using Hyper-V Manager, see Creating a Failover Cluster for Hyper-V on page 377.

Before you begin

Join the hosts to the domain as described in Adding the Cluster and Hosts to a Domain in the *Hyper-V Administration for Acropolis* guide.

Procedure

1. Start the Failover Cluster Manager utility.
2. Right-click and select **Create Cluster**, and click **Next**.
3. Enter all the hosts that you want to add to the Failover cluster, and click **Next**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2228

4. Select the **No. I do not require support from Microsoft for this cluster, and therefore do not want to run the validation tests. When I click Next continue creating the cluster** option, and click **Next**.

> **Note:**
>
> If you select **Yes**, two tests fail when you run the cluster validation tests. The tests fail because the internal network adapter on each host is configured with the same IP address (192.168.5.1). The network validation tests fail with the following error message:
>
> Duplicate IP address
>
> The failures occur despite the internal network being reachable only within a host, so the internal adapter can have the same IP address on different hosts. The second test, Validate Network Communication, fails due to the presence of the internal network adapter. Both failures are benign and can be ignored.

5. Enter a name for the cluster, specify a static IP address, and click **Next**.

6. Clear the **All eligible storage to the cluster** check box, and click **Next**.

7. Wait until the cluster is created. After you receive the message that the cluster is successfully created, click **Finish** to exit the **Cluster Creation** wizard.

8. Go to **Networks** in the cluster tree and select **Cluster Network 1** and ensure it is in the internal network by verifying the IP address in the summary pane. The IP address must be 192.168.5.0/24 as shown in the following screen shot.

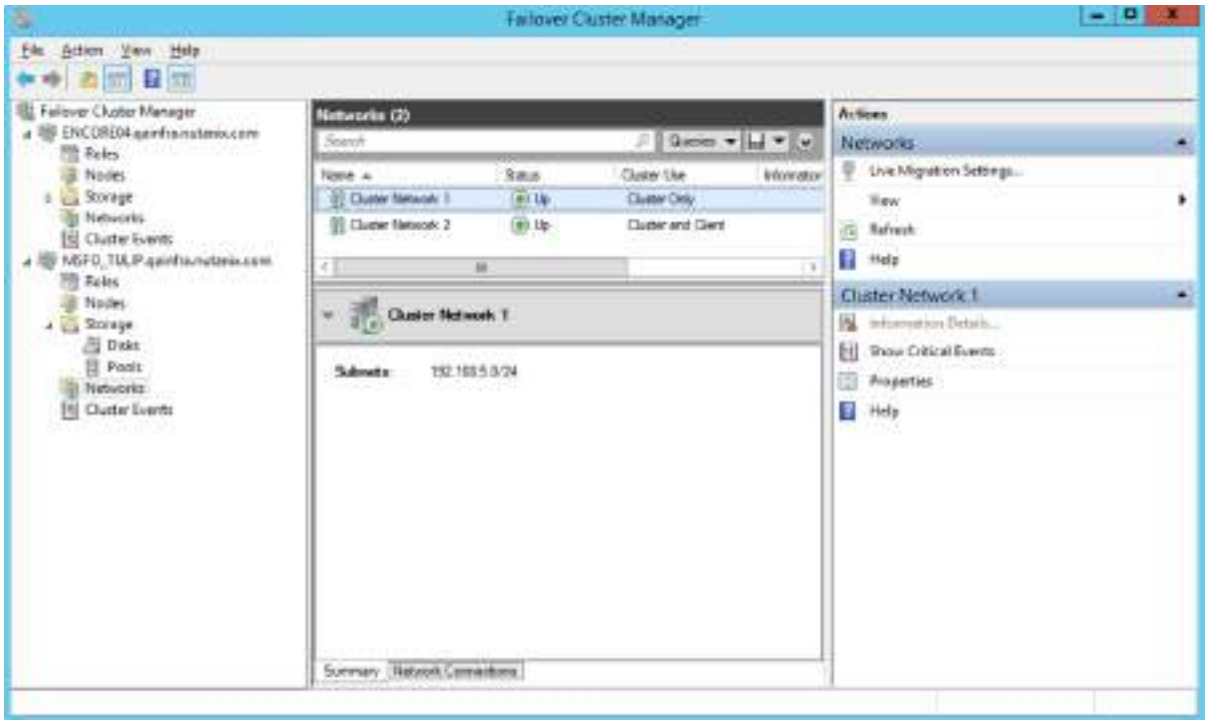


Figure 49: Failover Cluster Manager

9. Click the **Action** tab on the toolbar and select **Live Migration Settings**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2229

10. Remove **Cluster Network 1** from **Networks** for Live Migration and click **OK**.

> **Note:** If you do not perform this step, live migrations fail because the internal network is added to the live migration network lists. Log on to SCVMM, add the cluster to SCVMM, check the host migration setting, and ensure that the internal network is not listed.

Enabling Kerberos for Hyper-V

If you are running Windows Server 2012 R2, perform the following procedure to configure Kerberos to secure the storage. You do not have to perform this procedure for Windows Server 2016 because Kerberos is enabled automatically during failover cluster creation.

Before you begin

- Join the hosts to the domain as described in Adding the Cluster and Hosts to a Domain on page 376.
- Verify that you have configured a service account for delegation. For more information on enabling delegation, see the *Microsoft documentation*.

Procedure

1. Log on to the web console by using one of the Controller VM IP addresses or by using the cluster virtual IP address.
2. Click the gear icon in the main menu and select **Kerberos Management** from the **Settings** page.
3. Set the **Kerberos Required** option to enabled.
4. In the **Credentials** field, type the logon name and password of the domain account that has the privileges to create and modify the virtual computer object representing the cluster in Active Directory. The credentials are required for enabling Kerberos.

   The logon name must be in the format `DOMAIN\USERNAME`. Nutanix does not store the credentials.
5. Click **Save**.

Configuring the Hyper-V Computer Object by Using Kerberos

About this task

Perform the following procedure to complete the configuration of the Hyper-V Computer Object by using Kerberos and SMB signing (for enhanced security).

> **Note:** Nutanix recommends you to configure Kerberos during a maintenance window to ensure cluster stability and prevent loss of storage access for user VMs.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2230

Procedure

1. Log on to Domain Controller and perform the following for each Hyper-V host computer object.
   a. Right-click the host object, and go to **Properties**. In the **Delegation** tab, select the **Trust this computer for delegation to specified services only** option, and select **Use any authentication protocol**.
   b. Click **Add** to add the **cifs** of the Nutanix storage cluster object.

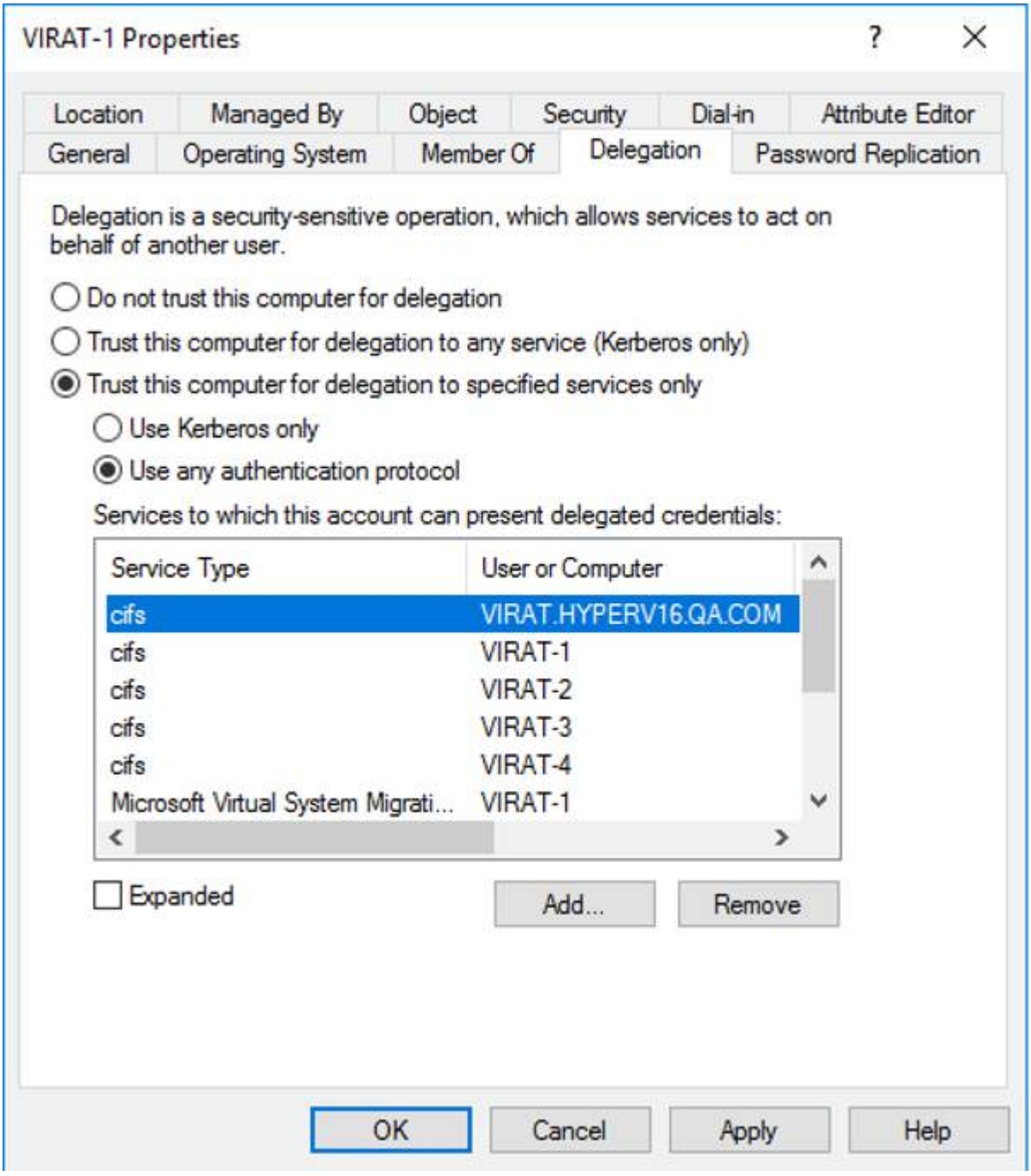


Figure 50: Adding the cifs of the Nutanix storage cluster object

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2231

2. Check the Service Principal Name (SPN) of the Nutanix storage cluster object.

```
> Setspn -l name_of_cluster_object
```

Replace *name_of_cluster_object* with the name of the Nutanix storage cluster object.

Output similar to the following is displayed.

```
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator> setspn -1 virat
Registered ServicePrincipalNames for CN=VIRAT,CN=Computers,DC-hyperv16, DC=qa,DC=com:
    cifs/VIRAT.HYPERV16.QA.COM
    cifs/VIRAT
PS C:\Users\Administrator>
```

If the SPN is not registered for the Nutanix storage cluster object, create the SPN by running the following commands.

```
> Setspn -S cifs/name_of_cluster_object name_of_cluster_object
> Setspn -S cifs/FQDN_of_the_cluster_object name_of_cluster_object
```

Replace *name_of_cluster_object* with the name of the Nutanix storage cluster object and *FQDN_of_the_cluster_object* with the domain name of the Nutanix storage cluster object.

Example

```
> Setspn -S cifs/virat virat
> Setspn -S cifs/virat.sre.local virat
```

3. [Optional] To enable SMB signing feature, log on to each Hyper-V host by using RDP and run the following PowerShell command to change the **Require Security Signature** setting to **True**.

```
> Set-SMBClientConfiguration -RequireSecuritySignature $True –Force
```

> **Caution:** The SMB server will only communicate with an SMB client that can perform SMB packet signing, therefore if you decide to enable the SMB signing feature, it must be enabled for all the Hyper-V hosts in the cluster.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2232

SECURITY AND USER MANAGEMENT

Prism provides several mechanisms to maintain security in a cluster and control user access.

- Set the user authentication method. For more information, see Configuring Authentication in the *Nutanix Security Guide*.
- Add, edit, or delete local user accounts. For more information, see User Management in the *Nutanix Security Guide*.
- Install or replace an SSL certificate. For more information, see Certificate Management in the *Nutanix Security Guide*.
- Control SSH access to the cluster. For more information, see Controlling Cluster Access in the *Nutanix Security Guide*.
- Enable data-at-rest encryption. For more information, see Data-at-Rest Encryption in the *Nutanix Security Guide*.
- Enable network segmentation. For more information, see Securing Traffic Through Network Segmentation in the *Nutanix Security Guide*.
- Review authentication best practices. For more information, seeAuthentication Best Practices in the *Nutanix Security Guide* and for firewall requirements see Firewall Requirements in the *Nutanix Security Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2233

SUPPORT SERVICES

Nutanix provides support services in several ways.

- Nutanix technical support can monitor your clusters and provide assistance when problems occur. For more information, see Controlling Remote Connections on page 393, Configuring HTTP Proxy on page 394, and Pulse Health Monitoring on page 384.
- Nutanix technical support maintains a portal that you can access to request assistance, download AOS updates, or view documentation. For more information, see Accessing the Nutanix Support Portal on page 395.
- Nutanix supports a REST API that allows you to request information or run administration scripts for a Nutanix cluster. For more information, see Accessing the REST API Explorer on page 397.

Pulse Health Monitoring

The Pulse feature provides diagnostic system data about a Prism Element cluster to Nutanix Support to help deliver proactive, context-aware support for Nutanix solutions. Pulse collects this information without affecting system performance and shares only basic system-level information necessary for monitoring the health and status of a Prism Element cluster.

This information includes the following items.

- System alerts
- Current Nutanix software version
- Nutanix processes and Controller VM information
- Hypervisor details such as type and version

Pulse frequently collects important data, like system-level statistics and configuration information, to automatically detect issues and help simplify troubleshooting. With this information, Nutanix Support can apply advanced analytics to optimize your implementation and address potential problems.

Pulse sends messages through HTTPS (port 443) using TLS 1.2. The HTTPS request uses certificate authentication to validate that Pulse has established communication with the Nutanix Remote Diagnostics service. The TLS 1.2 protocol uses public key cryptography and server authentication to provide confidentiality, message integrity, and authentication for traffic passed over the Internet. For the complete list of required ports, see Ports and Protocols.

Pulse Transport Methods

Nutanix recommends that you configure one of the following Pulse transport methods (in the order of preference):

1. Enable Pulse and use Prism Central as a proxy for the Pulse data transmitted by each node (for clusters registered with Prism Central).

   Advantages: The configuration is automatic (as described in Prism Central Proxy for Pulse Data of the *Prism Central Admin Center Guide*), and no new firewall configurations are required when you add a node to the cluster or remove a node from the cluster.
2. Enable Pulse and configure an HTTP proxy server. For information on how to configure an HTTP proxy server see Configuring HTTP Proxy on page 394.

   Advantage: No new firewall configurations are required when you add a node to the cluster or remove a node from the cluster.
3. Enable Pulse and configure your firewall. Enable Pulse by using each Controller VM IP address in each managed cluster. For more information, see Pulse Configuration on page 386 and Pulse Access Requirements.

   Disadvantage: New firewall configurations are required when you add a node to the cluster or remove a node from the cluster.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2234

Pulse Access Requirements

To successfully send Pulse-collected data from a Prism Element cluster to the Nutanix Insights endpoints, Pulse requires the following access:

- Ensure your firewall allows the IP addresses of all Controller VMs because Pulse data is sent from each controller VM of the cluster to insights.nutanix.com over port 443 using the HTTPS REST endpoint.
- Ensure your firewall allows traffic from each Controller VM to the Nutanix Insights endpoints. For more information, see Ports and Protocols.

  Note: Firewall port requirements for the Controller VMs might not be necessary if you have a Prism Central deployment. For more information, see Prism Central Proxy for Pulse Data in the *Prism Central Admin Center Guide*.

Remote Diagnostics

Remote Diagnostics enables Nutanix Support to request granular diagnostic information from Pulse-enabled clusters. Pulse streams a collection of configuration data, metrics, alerts, events, and select logs to Nutanix Insights, providing a high-level representation of the cluster state. If the Pulse data stream is not detailed enough to diagnose a specific issue, Nutanix Support might need to collect more diagnostic data from the cluster. Remote Diagnostics allows Nutanix to remotely collect the following data only.

- Logs
  - Nutanix services logs
  - Custom gflags set for any Nutanix service
  - Activity traces for Nutanix services
  - Hypervisor logs
  - Hypervisor configuration
  - Cluster configuration
  - System statistics like memory usage
- Nutanix NCC health check reports
- Nutanix log summary report (Panacea)
- A curated set of read-only commands

Each time Remote Diagnostics triggers a collection, it adds an entry to the audit trail of the cluster. There are always two entries, the start (initiation) and finish (termination) of the diagnostics collection.

By default, every Pulse-enabled cluster has Remote Diagnostics enabled. If your security policy or other consideration does not allow cluster access to Nutanix Support for remote diagnostics collection, you can disable Remote Diagnostics without disabling Pulse. Nutanix Support continues to provide seamless and proactive support based on the Pulse data.

- To check the Remote Diagnostics status, log on to a Controller VM through SSH and run the following command.

  ```
  nutanix@cvm$ zkcat /appliance/logical/nusights/collectors/kCommand/override_config
  ```

  Note: This command prints the Remote Diagnostics status only if the Remote Diagnostics status is set explicitly. The command does not print anything if the status is the default status.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2235

- To disable Remote Diagnostics, log on to a Controller VM through SSH and run the following command.

  ```
  nutanix@cvm$ /home/nutanix/ncc/bin/nusights/set_remote_diagnostics_status --
  enable=false --reason="text"
  ```

  Replace *text* with a string describing the reason for disabling Remote Diagnostics. The --reason parameter is optional.

- To enable Remote Diagnostics, log on to a Controller VM through SSH and run the following command.

  ```
  nutanix@cvm$ /home/nutanix/ncc/bin/nusights/set_remote_diagnostics_status --
  enable=true --reason="text"
  ```

  Replace *text* with a string describing the reason for disabling Remote Diagnostics. The --reason parameter is optional.

Pulse Configuration

When you log in to the Prism Element web console for the first time after an installation or an upgrade, the system checks whether Pulse is enabled. If it is not enabled, a pop-up window appears recommending that you enable Pulse.

- To enable Pulse, click **Continue** and follow the prompts.
- To continue without enabling Pulse, select the **Disable Pulse (not recommended)** checkbox and click **Continue**.

For Pulse configuration recommendations, see Pulse Transport Methods.

Enabling Pulse

About this task

Perform the following steps to enable Pulse in a cluster.

> **Note:**
>
> - For information on how to enable Pulse simultaneously in all the clusters registered to a Prism Central, see Enabling Pulse in the *Prism Central Admin Center Guide*.
> - Nutanix recommends that you enable Pulse to allow Nutanix Support to receive cluster data and deliver proactive and context-aware support.
> - Nutanix does not collect any personally identifiable information (PII) through Pulse.

Procedure

1. Log in to the Prism Element web console.
2. Go to **Settings** > **Setup** > **Pulse**.
   The **Enable Insights powered by Pulse** window appears.
3. Click **Enable Pulse**.
   Pulse is enabled in the cluster and the following message is displayed.

   ```
   Pulse has been enabled for this cluster.
   ```

Disabling Pulse

About this task

Perform the following steps to disable Pulse from a cluster.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2236

Caution: Nutanix recommends that you enable Pulse to allow Nutanix Support to receive cluster data and deliver proactive and context-aware support. If Pulse is disabled, the clusters do not send alerts to Nutanix Support when problems occur.

Procedure

1. Log in to the Prism Element web console.
2. Go to **Settings** > **Setup** > **Pulse**.
   The **Enable Insights powered by Pulse** window appears.
3. Click **Disable Pulse**.
   Pulse is disabled from the cluster and the following message is displayed.

   ```
   Pulse has been disabled for this cluster.
   ```

Mask Entity Names and IP Addresses

When you enable Pulse, Pulse periodically sends data to the Nutanix Insights tool and the Nutanix Support team for troubleshooting. Pulse is the underlying technology that securely transmits system-level diagnostic data to the Insights platform, enabling predictive health and context-aware support automation workflows. Nutanix Insights is an integrated service that utilizes this data to augment product support, reducing customer case volume and expediting issue resolution time.

Nutanix does not share any data that Pulse sends with any third parties unless permitted by your agreement with Nutanix or the Nutanix Privacy Statement. Certain Nutanix products require Pulse enablement for functionality and features. For more information, see Nutanix Privacy Statement and the applicable product documentation.

You can mask the entity names and IP addresses not masked by default. The entity names and IP addresses link to Nutanix entities, such as cluster names, and not to individuals.

To check masking settings on a specific Prism Element cluster, run these commands.

- Check if partial scrubbing is enabled.

  ```
  nutanix@cvm$ curl -H "Content-Type: application/json" -X GET -H "X-Nutanix-Preauth-User:admin" http://localhost:9080/PrismGateway/services/rest/v1/pulse
  ```

  If the output contains the string "identificationInfoScrubbingLevel":"PARTIAL" or "identificationInfoScrubbingLevel":"AUTO", partial scrubbing is enabled. By default, the scrubbing level is set to AUTO. If the output contains the string "identificationInfoScrubbingLevel":"ALL", identificationInfoScrubbingLevel is still set to ALL, and the **Open In Prism** button on the Insights Portal remains deactivated.

- Mask entity names and IP addresses, and update the PII scrub level.

  ```
  nutanix@cvm$ curl -H "Content-Type: application/json" -X PUT -H "X-Nutanix-Preauth-User:admin" --data '{"identificationInfoScrubbingLevel": "ALL"}' http://localhost:9080/PrismGateway/services/rest/v1/pulse
  ```

Pulse Health Monitoring Data Collection

The following categories serve as a general overview of the types of information that Pulse gathers from the clusters. Note that some of this information may be anonymized depending on your settings. This list is not exhaustive; for more details about the Pulse information your clusters send to Nutanix, contact Nutanix Support.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2237

Table 80: Pulse Data Collection

Entity	Data Collected
Cluster	• Cluster name (may be anonymized) • Uptime • AOS version • Cluster ID • Block serial number • HW model • Cluster IOPS • Cluster latency • Cluster memory

Entity	Data Collected
Hardware **Note:** In this context, hardware can include nodes, blocks, boards, disks, BMCs, fans, DIMMs, BIOS, CPUs, NICs, storage controllers, and power supplies.	• Model number • Serial number • Part number • Block number • Node UUID • Type • Size • Version • Name (may be anonymized) • Manufacturer • Status • Memory (size) • Hypervisor type • Hypervisor version • Firmware version • Disk type • Disk model • Disk capacity • Node temperature • Network interface model • SATADOM firmware • PSU status • Node location • IPMI version • Fan RPM • Component location • DIMM bank connection • Clock speed • DIMM temperature • BIOS release date • BIOS ROM size • CPU signature • CPU core count • CPU cores enabled • CPU thread count • CPU temperature

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2239

Entity	Data Collected
Storage Pool	• Name (may be anonymized) • Capacity (logical used capacity and total capacity) • IOPS and latency
Container	• Container name (may be anonymized) • Capacity (logical used and total) • IOPS and latency • Replication factor • Compression ratio • Deduplication ratio • Inline or post-process compression • Inline deduplication • Post-process deduplication • Space available • Space used • Erasure coding and savings
Controller VM (CVM)	• Details of logs, attributes, and configurations of services on each CVM • CVM memory • vCPU usage • Uptime • Network statistics • IP addresses (may be anonymized)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2240

Entity	Data Collected
VM	• Name (may be anonymized) • VM state • vCPU • Memory • Disk space available • Disk space used • Number of vDisks • Name of the container that contains the VM (may be anonymized) • VM operating system • IOPS • Latency • VM protection status • Management VM (yes or no) • I/O pattern (read, read/write, random, sequential) • IP address (may be anonymized)
Disk Status	• Performance stats • Usage
Hypervisor	• Hypervisor software and version • Uptime • Installed VMs • Memory usage • Attached datastore
Datastore	• Usage • Capacity • Name
Protection Domains	• Name (may be anonymized) • Count and names of VMs in each protection domain

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2241

Entity	Data Collected
Gflags	• Key and value • State (set) • Node ID • Service name • Time of modification
Feature	• Feature ID • Name • State (enabled or disabled) • Mode
License	License type (Starter, Ultimate, or Pro)
Alerts	• Alert ID • Type • Severity • Resolution status • Acknowledgement status • Impact type • Message • Creation time • Modification time
Tasks	• Task ID • Operation type • Status • Entities • Message Completion percentage • Creation time • Modification time
Logs	• Component • Timestamp • Source file name • Line number • Message

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2242

Entity	Data Collected
Nutanix Services	Service-specific metrics

Remote Support Connections

Nutanix technical support can remotely assist with problems by logging into the faulty cluster through an SSH connection.

If you encounter an issue in your Nutanix cluster and the Nutanix Support team needs access to your cluster to troubleshoot the issue, you can open a support tunnel for the Nutanix Support team to give remote access to your cluster. The Nutanix Support team ensures that the connection to your cluster through the support tunnel is secure and compliant by consolidating connectivity, authentication, authorization, audit, and recorded sessions.

You have complete control over enabling or disabling the support tunnel for a specific cluster. You can enable the support tunnel for a certain amount of time, close it at any time, or extend the duration to keep the support tunnel open. The support tunnel is automatically closed after a defined period.

Configuring Remote Connection Using CLI

You can enable a remote support connection tunnel for a maximum of 72 hours using CLI.

About this task

Use the following procedure to enable the remote support connection tunnel.

Procedure

1. SSH into CVM or PCVM .
2. Start ncli.

```
nutanix@cvm$ ncli

<ncli>
```

3. Run the cluster start-remote-support with the duration parameter set as required.
   The duration parameter must be set in minutes even if you need a duration of hours.

```
ncli> cluster start-remote-support duration=<minutes>
```

   Add duration that you want to enable the remote support connection tunnel for, in minutes. For example, if you want to keep the connection open for 24 hours, enter `duration=1440`.

> **Note:** You can keep the remote support connection tunnel between 0-72 hours.

Controlling Remote Connections

About this task

To enable (or disable) Nutanix technical support remote access to your cluster through this connection, do the following:

Procedure

1. Click the gear icon in the main menu and then select **Remote Support** in the **Settings** page.
   The **Remote Support** dialog box appears.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2243

2. Select (click the radio button for) the desired access state.

   - To allow remote access (temporarily) for Nutanix support, select **Enable for**, enter the desired number in the field provided, and select the duration (hours or minutes) from the drop-down menu.

     Note:

     - Remote Support can be enabled for any time period between 1 minute and 24 hours.
     - When you enable Remote Support, a new SSH key pair is automatically generated and pushed to the Nutanix servers. This key is used to connect to the cluster in a secure way without sharing CVM password with Nutanix Support.

   - To prevent remote access by Nutanix support, select **Disable**.

3. Click the **Save** button to save the new setting. A **Remote Support has been updated** message is displayed along with the updated connection status.

   Note: It might take a few minutes for the connection status to be updated. If the connection status is not updated, refresh the Remote Support setting screen to view the updated status.

Configuring HTTP Proxy

About this task

If the customer site cannot send traffic to a Nutanix service center directly, an HTTP proxy is required. To configure an HTTP proxy, do the following:

Procedure

1. Log in to the Prism Element web console.
2. Click the gear icon in the main menu and then select **HTTP Proxy** in the **Settings** page.
   The **HTTP Proxy** dialog box appears.
3. To add an HTTP proxy, click the **New Proxy** button and do the following in the displayed fields:

   Note: Only one HTTP proxy can be configured at a time. If one exists currently, you must first delete it before creating a new one.

   a. **Name**: Enter a proxy server name.
   b. **Address**: Enter an IP address or host name for the proxy server.
   c. **Port**: Enter the port number to use.
   d. **Username**: Enter a user name.
   e. **Password**: Enter a password.
   f. **Protocols**: Select the checkbox(es) for the protocol to proxy (HTTP, HTTPS, or both).
   g. When all the fields are correct, click the **Save** button (lower right).
      This saves the configuration and redisplays the dialog box with the new HTTP proxy entry appearing in the list.

      Note: To return to the **HTTP Proxy** window without saving, click the **Cancel** button.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2244

4. To edit an HTTP proxy entry, click the pencil icon on the line for that entry, update one or more of displayed field entries as desired, and then click the **Save** button.

   The **Update HTTP Proxy** dialog box appears with the same fields as the **Create HTTP Proxy** dialog box plus the option (below the protocol checkboxes) to add whitelist entries. To configure HTTP proxy whitelist entries, do the following:

   - To add an allowlist target, click the **+ Create** link. This opens a line to enter a target address or a network. An allowlist entry is a single host identified by an IP address or a network identified by the network address and subnet mask. Adding an allowlist entry instructs the system to ignore proxy settings for a particular address or network.
     - To allow a single IP address, enter the target IP address and then click the **Save** link in that field.
     - To allow an entire subnet, enter the network address and the subnet mask in the following format: *network_address*/*subnet_mask*, and then click the **Save** link in that field. Replace *network_address* with the network address and *subnet_mask* with the subnet mask of the network that you want to allow.
   - To edit an allowlist target, click the pencil icon for that target and update as needed.
   - To delete an allowlist target, click the X icon for that target.

5. To delete an HTTP proxy entry, click the X icon for that entry.
   A window prompt appears to verify the action; click the **OK** button. The entry is removed from the HTTP proxy list.

Accessing the Nutanix Support Portal

About this task

Nutanix provides a variety of support services and materials through its support portal.

Procedure

1. Log in to the Prism Element web console.
2. To access the Nutanix support portal, select **Support Portal** from the question mark icon dropdown menu. The login screen for the Nutanix support portal appears in a new tab or window.
3. Enter your support account user name and password.
   The Nutanix support portal home page appears.
4. Select the desired service from the screen options.

   You can select an option from one of the main menu dropdown menus or search for a topic at the top of the screen, click one of the icons (Documentation, Open Case, View Cases, Downloads) in the middle, or view one of the selections at the bottom such as an announcement or KB article. The following table lists the menu options.

   Note: Some options have restricted access and are not available to all users.

Table 81: Main Menu Options

Category	Option	Description
Documentation	Product Documentation	Displays a page from which you can view the Nutanix product manuals.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2245

Category	Option	Description
	Knowledge Base	Displays a page from which you can view the knowledge base (KB) articles.
	Solutions Documentation	Displays a page from which you can view documents that describe how to implement the Nutanix platform to solve a variety of business applications.
	EOL Information	Displays a page from which you can view the end of life policy and bulletins.
	Field Advisories	Displays a page from which you can view field advisories.
	Training	Provides a link to the separate Nutanix training portal.
	Security Advisories	Displays a page from which you can view security advisories.
	Acropolis Upgrade Paths	Displays a table of the supported AOS release upgrade paths.
	Compatibility Matrix	Displays a page from which you can view a compatibility matrix broken down (filtered) by hardware model, AOS version, hypervisor type and version, and feature version (NCC, Foundation, BMC/ BIOS).
	Webinar Recordings	Displays a page with links to a selection of Nutanix training webinars.
Support & Forums	Open Case	Displays a form to create a support case.
	View Cases	Displays a page from which you can view your current support cases.
	.NEXT Forums	Provides a link to the (separate) Nutanix Next Community forum.
	Terms & Conditions	Displays a page from which you can view various warranty and terms and conditions documents.
Downloads	AOS (NOS)	Displays a page from which you can download AOS releases.
	Hypervisor Details	Displays a page from which you can download Acropolis hypervisor versions. You can also download supporting files used when manually upgrading a hypervisor version (AHV, ESXi, or Hyper-V).
	Prism Central	Displays a page from which you can download the Prism Central installation bundle. There are separate bundles for installing on AHV, ESXi, or Hyper-V.
	Tools & Firmware	Displays a table of tools that can be downloaded, including the Nutanix Cluster Check (NCC) and Prism Central VM.
	Phoenix	Displays a page from which you can download Phoenix ISO files.
	Foundation	Displays a page from which you can download Foundation releases.
My Products	Installed Base	Displays a table of your installed Nutanix appliances, including the model type and serial number, location, and support coverage.
	Licenses	Displays a table of your product licenses along with buttons to add or upgrade licenses for your clusters.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2246

Nutanix REST API

The Nutanix REST APIs allow you to create scripts that run system administration commands against the Nutanix cluster. The API enables the use of HTTP requests to get information about the cluster as well as make changes to the configuration. Output from the commands are returned in JSON format.

There are two versions of the Nutanix REST API.

- **v1**: The original Nutanix REST API.
- **v2**: An update of the v1 API. Users of the v1 API are encouraged to migrate to v2.

A complete list of REST API functions and parameters is available in the REST API Explorer section of the Prism Element web console. In addition, the complete reference for the v2 Nutanix API, including code samples in multiple languages, and tutorials are available at http://developer.nutanix.com/.

Accessing the REST API Explorer

About this task

Nutanix provides a utility with the Prism Element web console to help you get started with the REST API. The Explorer displays the parameters and format for the API calls that can be included in scripts. Sample API calls can be made to show the type of output you should expect to receive.

You can access the REST API Explorer as an admin user or a non-admin user. The v1 and v2 APIs can both be viewed in the REST API Explorer.

Procedure

1. Open the explorer for the desired version of the API.

   » v1: Connect to the Prism Element web console, click the user icon in the upper-right corner of the Prism Element web console, and select **REST API Explorer**. In the explorer, select **Version 1** from the menu.

   » v2: Connect to the Prism Element web console, click the user icon in the upper-right corner of the web console, and select **REST API Explorer**. In the explorer, select **Version 2** from the menu.

   The REST API Explorer displays a list of the cluster objects that can be managed by the API. Each line has four options:

   - **Show/Hide**: Expand or reduce the detail shown for the object
   - **List Operations**: Show all operations that can be run on this object
   - **Expand Operations**: Show the detailed view of the operations that can be run on this object

   > **Tip:** The objects are listed by a relative path that is appended to the base URL https://*management_ip_addr*:9440/PrismGateway/services/rest/v[1,2,3]/api, where *management_ip_addr* is the IP address of any Nutanix Controller VM in the cluster.

2. Find the line for the object you want to explore and click **Expand Operations**. For this example, you will operate on a storage pool.
3. Click **GET** on the first line to show the details for this API call.

   The explorer displays the parameters that can be passed when this action is used.
4. Click **Try it out!** to test the API call when used with your cluster.

   The test displays the request URL required for scripting, as well as sample responses expected from the API call.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2247

Determining Compatibility Between Hardware and Supported Products

The Compatibility and Interoperability Matrix provides information about supported product compatibility with hardware platforms,

Supported Products Information

Nutanix provides a Compatibility and Interoperability Matrix that helps you with information about hardware and software compatibility and interoperability. This section provides information about finding compatibility of hardware platforms for software (features, components or products) such as Microsoft System Center Operations Manager (SCOM), Nutanix Mine, or Single-Node Replication Target.

To find out if the hardware you deploy supports a feature, do the following:

1. Click the Compatibility and Interoperability Matrix.
2. On the **Platform** tab, in the **Hardware Manufacturer** field, select the name of the hardware manufacturer.

   Select **Select All** in the **Hardware Manufacturer** field to check compatibility with hardware manufactured by all the listed manufacturers.
3. Turn on the **Supported Products** toggle switch.
4. In the filter field below **Hardware Model** column name, type the name of the software to filter the list of compatible platforms.

   This field supports only certain variations in the name of a feature. For example, SNRT is not a supported filter for Single Node Replication Target feature. Instead, type single or single-node.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2248

HELP RESOURCES

There are several information sources that you can access at any time when you need help:

- Context-sensitive help documentation. For more information, see Accessing Online Help on page 399.
- Health dashboard tutorial. For more information, see Health Dashboard.
- Customer support portal. For more information, see Accessing the Nutanix Support Portal on page 395.
- Nutanix community forum. For more information, see Accessing the Nutanix Next Community on page 400.
- REST API explorer. For more information, see Accessing the REST API Explorer on page 397.
- Glossary of terms. For more information, see Nutanix Glossary.

Accessing Online Help

About this task

The Prism Element web console includes online help documentation that you can access at any time.

Procedure

1. Log in to the Prism Element web console.
2. To open the online help, choose one of the following from the question mark icon drop-down list of the Main Menu:

   » Select **Help with this page** to display help documentation that describes the current screen.

   > **Note:** In a task window click the question mark icon in the upper right to display the help documentation for that window.

   » Select **General Help** to display the **Help Organization** page.

   A context-sensitive help page or the **Help Organization** page appears in a new tab or window. (These pages are located on the Nutanix support portal.) The **Help Organization** page provides descriptions of the major help topics with links to the entry page for each major topic. The display includes a breadcrumb at the top to navigate through the help pages.

3. To select a topic from the table of contents, click the click the collapse menu icon (also know as a *hamburger* button) in the upper left.

   A table of contents pane appears on the left. Click a topic in the table of contents to display that topic.

4. To display all the help contents as a single document (*Prism Element Web Console Guide*), click the **epub** or **pdf** button in the upper right corner.

   You can view the *Prism Element Web Console Guide* in either ePUB or PDF format by selecting the appropriate button. If your browser does not support the selected format, you can download the PDF or ePUB file.

5. To search for a topic, click the **Other** icon in the main menu bar and enter a search string in the field.

   This searches not only the help contents, but also all the documentation, knowledge base articles, and solution briefs. Matching results appear below the search field. Click a topic from the search results to display that topic.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2249

Accessing the Nutanix Next Community

Nutanix maintains a community forum for customers and partners to facilitate a peer-to-peer exchange of ideas, tips, and information about Nutanix technologies and the rapidly changing landscape of data center IT.

Procedure

1. Log in to the Prism Element web console.
2. To access the Nutanix next community forum, select **Nutanix Next Community** from the question mark icon dropdown menu of the Main Menu.
   The Nutanix Next Community main page appears in a new tab or window. From this page you can search existing posts, ask questions, and provide comments.

Glossary

For terms used in this guide, see Nutanix Glossary.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2250

COPYRIGHT

Copyright 2025 Nutanix, Inc.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

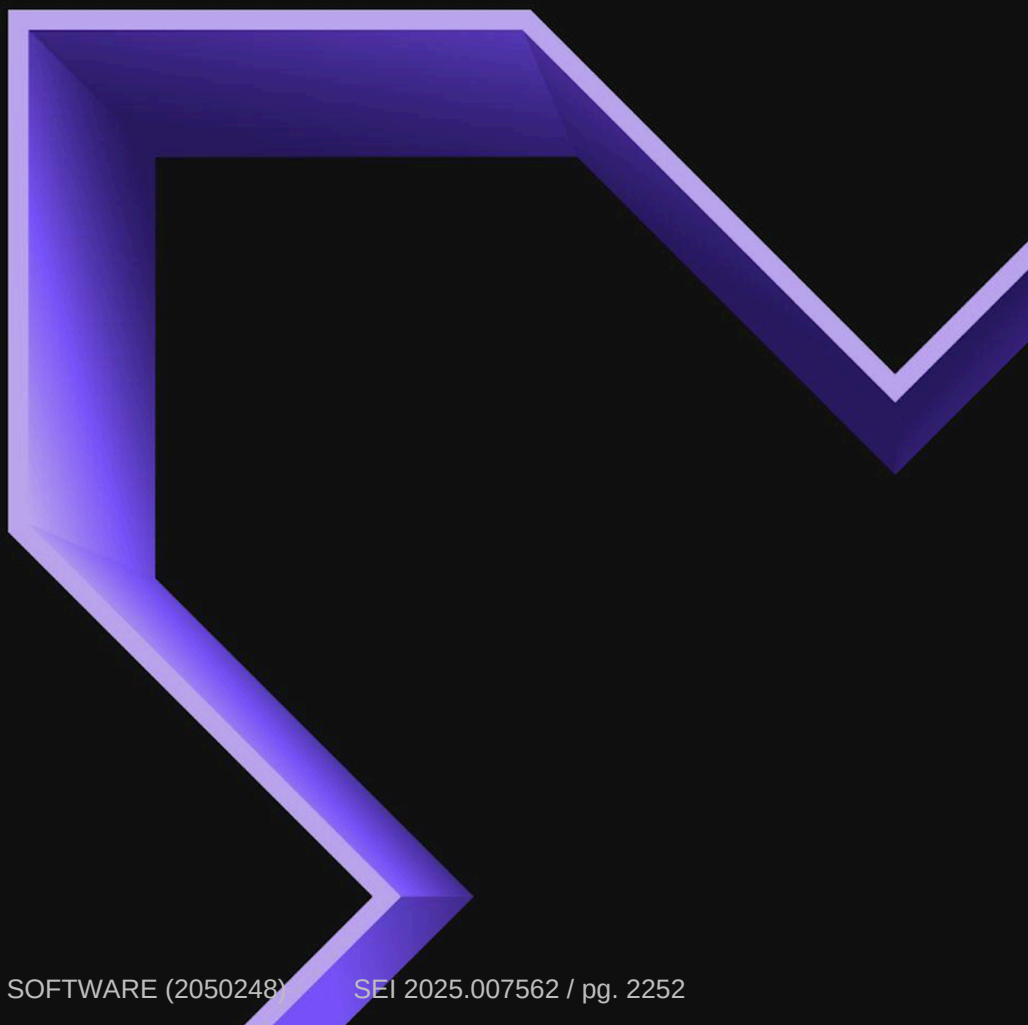
All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Nutanix and the Nutanix logo are registered trademarks of Nutanix, Inc. in the United States and/or other jurisdictions. All other brand and product names mentioned herein are for identification purposes only and may be trademarks of their respective holders.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2251

Nutanix Kubernetes Engine Guide

Nutanix Kubernetes Engine 2.10

December 10, 2024



NUTANIX

Contents

1. Nutanix Kubernetes Engine Overview 4
Kubernetes 4

2. Requirements 5

3. Resource Recommendations 8

4. Enabling Kubernetes Management from Nutanix Marketplace 12

5. Enabling Kubernetes Management 14

6. Airgap 15
Deploying Airgap 16
Disabling Airgap 18

7. Kubernetes Management Layout 20
Clusters 20
Summary 21
Node Pools 22
Storage Classes 23
Persistent Volume Claims 24
Alerts 24
Tasks 25
Logging 26
OS Images 26

8. Cluster Setup 27
Creating a Cluster 29
Creating a Cluster Using API 35
Cluster Deployment Attributes 35

9. Cluster Administration 40
Downloading the Kubeconfig 40
Logging on to the Karbonctl 41
Downloading Images 41
Creating a Storage Class 42
Deleting a Storage Class 44
Creating a Volume 44
Deleting a Volume 45
Creating a Node Pool 46
Updating the Number of Worker Nodes 47

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2253

Updating Node Pool Metadata....48
Configuring GPU....49
Configuring GPU Using Karbonctl....50
Access and Authentication....51
Accessing Locked Nodes....51
Rotating Certificates....52
Migrating DVP and CSI to Use Certificate-Based Authentication....53
Restarting the karbon_core Service....53
Impact of Restarting the karbon_core Service....53
Backing up Etcd....54
Stopping an NKE Cluster....54
Starting an NKE Cluster....56

10. Upgrades....59
NKE Upgrades....59
Upgrading a Node OS Image....60
Upgrading Kubernetes....60
Upgrading Kubernetes Using the Karbonctl....61
Upgrading Airgap using LCM....63
Updating OS Images and Kubernetes for Airgap....64

11. Options....66
Enabling Alert Forwarding....66
Disabling Alert Forwarding....67
Enabling Infra Logging....67
Disabling Infra Logging....67
Configuring a Private Registry....67
Deleting a Private Registry....69
Enabling Log Forwarding....69
Disabling Log Forwarding....70
Network Segmentation....70

12. Add-Ons....71
Logging....71
Using Logtrail Plug-in....71
Using Kibana....72
Monitoring....73

13. Onboard and View Kubernetes Clusters in Prism Central....74
Onboard the Kubernetes Clusters to Prism Central....74

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2254

1

NUTANIX KUBERNETES ENGINE OVERVIEW

Nutanix Kubernetes Engine coupled with Prism Central-based Kubernetes Management is a curated turnkey offering that provides simplified provisioning and operations of Kubernetes clusters. Kubernetes is an open source container orchestration system for deploying and managing container-based applications. You can also set up an offline NKE environment using Airgap, see Airgap on page 15.

NKE uses the CentOS Linux-based operating systems for NKE-enabled Kubernetes cluster creation. Linux containers provide the flexibility to deploy applications in different environments with consistent results.

Prism Central-based Kubernetes Management streamlines the deployment and management of Kubernetes clusters with a simple integrated GUI. Kibana, the built-in add-on, lets you filter and parse logs for systems, pods, and nodes. Prometheus, another add-on, provides a monitoring mechanism that triggers alerts on your cluster. NKE also uses Pulse, health-monitoring system of Prism, which interacts with Nutanix Support to expedite cluster issue resolutions.

To set up your NKE environment, perform the following tasks:

- Ensure that your environment meets the requirements, see Requirements on page 5.
- Enable Kubernetes Management through Prism Central (PC) and set up a cluster, see Cluster Setup on page 27.
- Download the kubeconfig, see Downloading the Kubeconfig on page 40.
- Configure access, see Access and Authentication on page 51.

Kubernetes

Prism Central-based Kubernetes Management orchestrates Kubernetes clusters to simplify the provisioning and management of containerized applications. Kubernetes packages applications in their own dedicated containers together with all of the required operational components for running the application. Containers , which run inside of pods on top of nodes, are the core building block of Kubernetes architecture.

Containerized applications are simple to manage, easy to deploy, and portable as they are abstracted from the OS of the host. Since different containers share an operational kernel, they do not require as much compute capacity as a VM, making them "lightweight".

Managing Kubernetes operations requires a basic familiarity with key Kubernetes concepts.

To gain a better understanding of containerization, cluster architecture, workloads, and storage concepts, see Kubernetes documentation.

2

REQUIREMENTS

Meet the indicated requirements prior to enabling Kubernetes Management and deploying NKE.

Cluster Requirements

- Install Prism Central (PC) on a Nutanix cluster.
- Ensure that the configuration of the Prism Element (PE) cluster meets the following specifications:
  - AHV
  - A minimum 120 MB of memory and 700 MB of disk space in PC

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2256

- Do the following before deploying NKE:
  - For Prism Central (PC) and Prism Element (PE) compatibility requirements, see *NKE Software Compatibility* in the Nutanix Kubernetes Engine Release Notes.
  - Register the PE cluster to PC.

    Caution: Do not unregister the PE cluster hosting an NKE Kubernetes cluster from PC. Unregistration of PE from PC will prevent the management of the NKE clusters.
  - Configure the cluster virtual IP address and the iSCSI data services IP address on the designated PE cluster.

    Note: NKE does not recognize changes to the iSCSI Data Service IP.
  - Configure the Network Time Protocol (NTP) and the Domain Name System (DNS) in PE and PC.
  - Synchronize the time of the cluster, PC, and the clients that use kubectl.

    Note: NKE requires using the UTC timezone.
  - Open the required ports and allowlist the required domains, see table below.
  - (Production clusters only) Configure an AHV network with IP address management (IPAM) enabled and IP pools configured.
  - (Development clusters only) Configure an AHV network with IPAM and IP address pools or with an external DHCP network.
  - (Airgap only) ensure you are using a Linux-based web server.

    Note:

    - IPAM is for Kubernetes cluster deployment.
    - The DHCP pool is for the worker nodes and the master nodes in a Virtual Router Redundancy Protocol (VRRP) environment.
    - The DNS configuration for an NKE Kubernetes cluster is obtained through the DHCP or Nutanix IPAM.
    - NKE is not supported on Nutanix Cloud Clusters (NC2).

Firewall Requirements

NKE only supports HTTP unauthenticated proxy. Use the IP or the fully qualified domain name (FQDN) format. Ensure that your firewall allows NKE VMs and CVMs to reach the below domains and sub-domains. Also, exclude the following domains from the security-sockets layer (SSL) inspection in the firewall.

- *.cloudflare.net
- *.cloudfront.net
- *.quay.io
- ntnx-portal.s3.amazonaws.com
- portal.nutanix.com
- release-api.nutanix.com
- s3*.amazonaws.com

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2257

- *.compute-1.amazonaws.com

> **Note:** NKE does not automatically recognize changes to proxy settings, which can cause cluster unavailability. To modify proxy settings, restart the `karbon_core` service on the cluster. For more information, see Restarting the karbon_core Service on page 53.

Port Requirements

The **Ports and Protocols** page on the portal provides detailed port information for Nutanix products and services, including port sources and destinations, service descriptions, directionality, and protocol requirements.

For information about port requirements for NKE, see Nutanix Kubernetes Engine in the *Ports and Protocols* page.

For information about port requirements for Airgap, see NKE (Airgap) in the *Ports and Protocols* page.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2258

3

RESOURCE RECOMMENDATIONS

Resource recommendations for Kubernetes entities and services.

Node Resource Default Settings

NKE allocates all control plane node resources to Kubernetes infrastructure services.

Table 1: Minimum Resources per Control Plane Node

Cluster Type	vCPU	Memory (GiB)	Storage (GiB)
Production	4	4	120
Development	2	4	120

> **Note:** The minimum resources are the default values allocated per Control Plane Node.

Etcd nodes use resources to store cluster configuration data and status details.

Table 2: Minimum Resources per Etcd Node

Cluster Type	vCPU	Memory (GiB)	Storage (GiB)
Production	4	8	40
Development	4	8	40

> **Note:** The minimum resources are the default values allocated per Etcd Node.

Worker nodes need enough resources to run cluster workloads on top of infrastructure services, including the kubelet. If available memory resources on a worker node fall under 400 MiB, the kubelet evicts a pod.

Table 3: Minimum Resources per Worker Node

Cluster Type	vCPU	Memory (GiB)	Storage (GiB)
Production	8	8	120
Development	8	8	120

> **Note:** The minimum resources are the default values allocated per Worker Node.

Kubernetes core consumes resources such as scheduler, DNS, etc. that are an overhead. The following table displays the minimum Kubernetes overhead required for a cluster deployed by NKE:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2259

For more details for all the processes, see the tables below.

Table 4: Minimum Resources for Infrastructure Services per Kubernetes Cluster

Cluster Type	vCPU	Memory (MiB)
Production	6.8 vCPU shared across all worker nodes in the cluster plus 1.25 vCPU for each worker node. **Note:** For example, a cluster with 3 worker nodes requires 10.55 vCPU. 6.8 vCPU + (3 workers x 1.25 vCPU)	8294 MiB shared across all worker nodes in the cluster plus 870 MiB for each worker node. **Note:** For example, a cluster with 3 worker nodes requires 10904 MiB memory. 8294 MiB + (3 workers x 870MiB)

kube-system Resource Default Settings

Nutanix recommends to adapt resources limits and requests based on your workload. By default, the kube-system pods are configured with the following request and limit configurations:

Table 5: DaemonSet

Entity	Requests	Limits	Replicas
Calico node	CPU: 250 m Memory: N/A	CPU: N/A Memory: N/A	1 per each worker and control plane node
Kube proxy	CPU:100 m Memory: 150Mi	CPU: 100m Memory: 150Mi	1 per each worker and control plane node

Table 6: Deployment

Service	Requests	Limits	Replicas
CoreDNS	CPU: 100 m Memory: 200Mi	CPU: 500 m Memory: 270Mi	2 overall
	CPU: 100 m Memory: 70Mi	CPU: 200 m Memory: 170Mi	1 overall
Calico kube-controller	CPU: N/A Memory: N/A	CPU: N/A Memory: N/A	1 overall
Calico typha	CPU: N/A Memory: N/A	CPU: N/A Memory: N/A	1 overall

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2260

ntnx-system Resource Default Settings

By default, the ntnx-system pods are configured with the following request and limits values:

Table 7: StatefulSet

Service	Requests	Limits	Replicas
Alertmanager-main	CPU: 200 m Memory: 150Mi	CPU: 300 m Memory: 250Mi	• 2 overall (for Production) • 1 overall (for Development)
Csi-provisioner	CPU: 200 m Memory: 400Mi	CPU: No limit Memory: No limit	1 overall
Elastic-logging	CPU: 500 m Memory: 2048Mi	CPU: 1000 m Memory: 2560Mi	1 overall
Prometheus-k8s	CPU: 600 m Memory: 450Mi	CPU: 1100 m Memory: 1586Mi	• 2 overall (for Production) • 1 overall (for Development)
Snapshot-controller	CPU: N/A Memory: N/A	CPU: N/A Memory: N/A	1 overall

Table 8: DaemonSet

Service	Requests	Limits	Replicas
Node-exporter	CPU: 112m Memory: 200Mi	CPU: 600 m Memory: 220Mi	1 per each worker and control plane node
Fluent-bit	CPU: 100 m Memory: 100Mi	CPU: 100 m Memory: 100Mi	1 per each worker and control plane node
Csi-node-ntnx-plugin	CPU: 200 m Memory: 400Mi	CPU: No limit Memory: No limit	1 per worker node

Table 9: Deployment

Service	Requests	Limits	Replicas
Kibana-logging	CPU: 200 m Memory: 128Mi	CPU: 500 m Memory: 512Mi	1 overall

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2261

Service	Requests	Limits	Replicas
Kube-state-metrics	CPU: 130 m Memory: 190Mi	CPU: 900 m Memory: 230Mi	1 overall
Kubernetes-events-printer	CPU: 100 m Memory: 200Mi	CPU: 100 m Memory: 200Mi	1 overall
Prometheus-operator	CPU: 110 m Memory: 120Mi	CPU: 600 m Memory: 240Mi	1 overall
snapshot-validation-deployment	No requests	No limit	2 overall

Cluster Sizing

Nutanix does not provide complete guidance on NKE Kubernetes cluster sizing. This section provides information about the minimum number of resources required for control plane nodes based on the NKE Kubernetes cluster size.

However, a control plane with sufficient compute and other resources is required. Resource consumption must be tracked precisely to prevent resource contention.

For an overview of the validated maximum number of worker nodes, see NKE Configuration Maximums on the Nutanix Support portal.

Table 10: Recommended configurations per Master Node

Worker Nodes	vCPU	Memory (GiB)
1-10	4	8
11-100	4	16

Table 11: Recommended configurations per Etcd Node

Kubernetes Nodes	vCPU	Memory (GiB)
1-100	4	8

Recommended configurations per Worker Node

> **Note:** Worker node sizing depends on the application and resource requirements for the default infrastructure services deployed by NKE. For more details, see Table 4: Minimum Resources for Infrastructure Services per Kubernetes Cluster on page 9.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2262

4

ENABLING KUBERNETES MANAGEMENT FROM NUTANIX MARKETPLACE

Enable Kubernetes Management from the Nutanix Marketplace through the new Prism Central experience. You can view and launch the Marketplace apps after you enable Marketplace in the Admin Center.
For more information about enabling Marketplace, Marketplace application category, and application deployment, see Marketplace and Deploying Kubernetes Management in the *Prism Central Admin Center Guide*.

Before you begin

Your system must meet the Requirements on page 5 prior to enabling Kubernetes.

> **Note:** Follow this procedure to deploy NKE in Prism Central 2023.1.0.1 or later versions.

Procedure

1. Log on to **Prism Central** as an administrator.
2. In the application switcher, select **Apps and Marketplace**.
3. To enable the **Kubernetes Management** chicklet, in the **Welcome to My Apps page**, click **Enable Marketplace**.
   A progress bar appears. After successfully enabling the application in the Nutanix Marketplace, the **Get** button to deploy Kubernetes Management is enabled.
4. In the left navigation pane, select **Marketplace**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2263

5. In the **Nutanix Marketplace** page, in the **Kubernetes Management** chicklet, click **Get**.

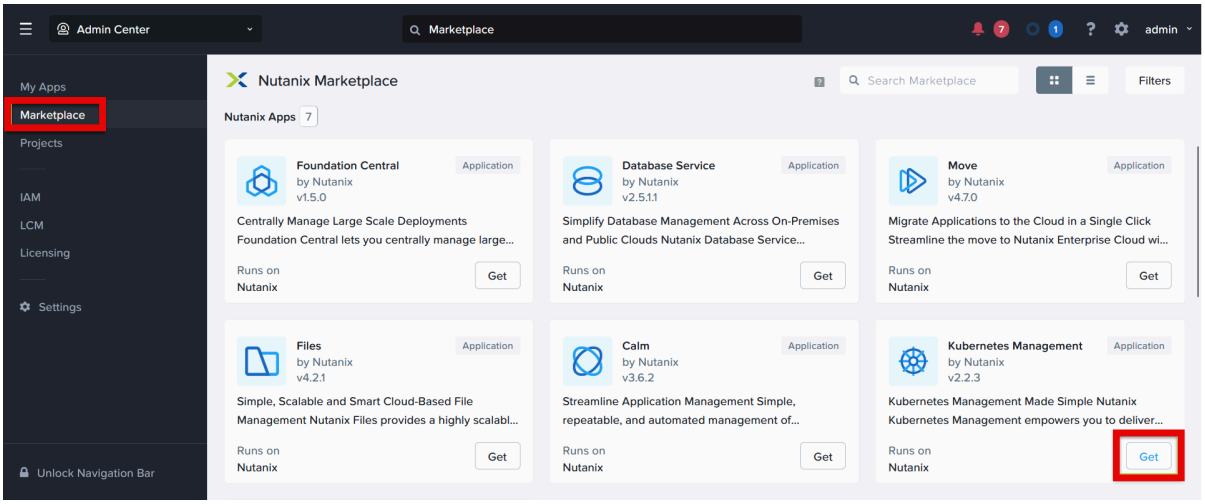


Figure 1: Kubernetes Management in Nutanix Marketplace

6. In the **Kubernetes Management** page, click **Deploy**.
   A dialog box displays the progress of the deployment.

7. After the successful deployment of **Kubernetes Management**, click **View in Admin Center**.
   The **Kubernetes Management** page displays the summary of the application.

8. In the application switcher, select **Kubernetes Management**.

9. In the Kubernetes Management console, a message directs you to download a node OS image, see Downloading Images on page 41.

What to do next

Ensure that you run the general availability (GA) version of NKE by performing an inventory check using the Life-Cycle Manager (LCM). For more information, see NKE Upgrades on page 59. If you are using LCM at a dark site, see Upgrading Airgap using LCM on page 63.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2264

5

ENABLING KUBERNETES MANAGEMENT

Enable Kubernetes Management through Prism Central.

Before you begin

Your system must meet the Requirements on page 5 prior to enabling Kubernetes.

> **Note:** Follow this procedure to deploy NKE in Prism Central 2022.9 or earlier versions.

Procedure

1. Log on to **Prism Central** as an administrator.
2. In the application switcher, select **Kubernetes Management**.
3. In the main console window, click **Enable Kubernetes**.

   > **Note:** The Kubernetes Management might take several minutes to launch.

   Once Kubernetes Management is enabled successfully, a confirmation page appears. The Kubernetes Management console window appears.
4. In the Kubernetes Management console, a message directs you to upload a node OS image, see Downloading Images on page 41.

What to do next

Ensure that you run the general availability (GA) version of NKE by performing an inventory check using the Life-Cycle Manager (LCM). For more information, see NKE Upgrades on page 59. If you are using LCM at a dark site, see Upgrading Airgap using LCM on page 63.

6

AIRGAP

This topic describes Kubernetes Management and Airgap.

Airgap eliminates the need for Internet access to manage NKE clusters by providing required services offline through a local Docker registry. However, deploying Airgap requires a device with Internet access to download the Airgap bundle and manifest files hosted online on the Nutanix Support Portal. You must host the downloaded Airgap bundle and manifest files on a Linux web server.

> **Note:** Nutanix does not create or manage the web server. Airgap mode uses it to fetch the required Airgap bundle and manifest files.

After enabling Airgap mode, you can use it to deploy and manage NKE clusters.

The required Docker registry runs on a VM that hosts the container images required for deploying NKE clusters. This VM is called the 'Airgap VM'. Kubernetes Management deploys and manages the Airgap VM on Prism Element (PE). The Airgap VM hosts the Docker registry.

> **Note:**
>
> - You cannot modify the settings of the registry VM.
> - Airgap applies to the complete Kubernetes Management environment.
> - You can deploy only one Airgap VM per Kubernetes Management installation.
> - Container images used by NKE are regularly scanned with Trivy.
> - Container images are directly provided by the owner of each upstream solutions. They are cached in a central location by Nutanix for convenience.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2266

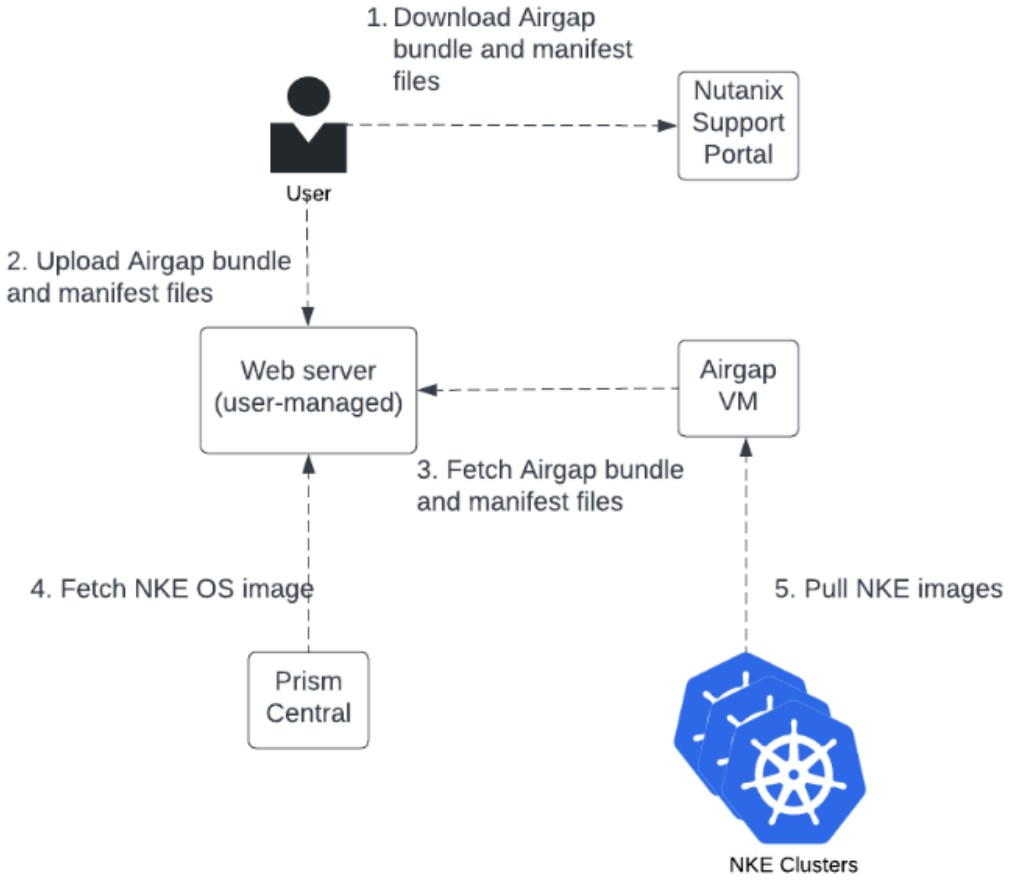


Figure 2: Airgap - Overview Diagram

For deployment step, see Deploying Airgap on page 16.

Note:

- If there are any Kubernetes clusters managed by NKE, you cannot enable or disable Airgap.
- Airgap bundle version should be the same as the NKE version running on Prism Central.
- Network segmentation is not applicable for the Airgap VM.
- After Airgap is deployed, you cannot modify the network configuration, such as the subnet or IP address. To modify the network configuration, you must disable Airgap and re-enable it. However, you cannot disable Airgap while there are existing Kubernetes clusters deployed. Therefore, you cannot modify the Airgap network configuration after enabling it initially.

Deploying Airgap

This procedure describes the steps for deploying Airgap.

About this task

Deploying Airgap requires downloading the required files from the Nutanix Support Portal and transferring them to a self-hosted web server.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2267

Before you begin

- Ensure to have a Linux-based host to extract deployment files and to transfer them to a Linux-based web server.
- Ensure that the web server is reachable through HTTP.
- Ensure that your environment meets all NKE requirements. For more information, see Requirements on page 5.
- Ensure that you do not have any Kubernetes clusters deployed.
- Ensure that you have a Prism IPAM managed subnet for the Airgap VM deployment.
- Create directory ntnx-*`version-number`* on a self-hosted web server.

  Note:

  - As a best practice, use the full Airgap version number as indicated in the Airgap download section in the Nutanix Support Portal. Example: ntnx-2.1.0.
  - Create the directory on a path that is reachable via HTTP on the web server. Example: /var/www/html/ntnx-*`version-number`*.

- Log on to Prism Element and get the following details:

  Note: The Airgap VM requires a Prism IPAM managed subnet, even when using a static IP (using a static IP address is optional).

  - Network name (in **Network** view)
  - Storage container name (in **Storage** view)
  - Prism Element cluster name (in **Home** view)

    Note: NKE creates the Airgap VM using the specified Prism Element cluster and network. The specified storage container uses a volume group (VG) to store Docker images.

- Ensure the following for the Airgap VM:

  - Node pool name = "airgap"
  - Count of nodes (VMs) = 1
  - *`num_sockets`* = 2
  - *`num_vcpu_per_socket`* = 2
  - *`mem`* = 4 GiB
  - *`boot_disk_size`* = 20 GiB
  - *`data_disk_size`* = 20 GiB

    Note: For information about port requirements for Airgap, see NKE (Airgap) in the *Ports and Protocols* page.

Procedure

1. If you have not already, enable Kubernetes Management through Prism Central (PC), see Enabling Kubernetes Management on page 14.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2268

2. In the Nutanix Support Portal, go to **collapse menu icon** > **Downloads** > **Nutanix Kubernetes Engine** to download the deployment files.

   a. To download the airgap-ntnx-*version-number*.tar.gz file, next to **NKE Airgap bundle**, click **Download**.

   b. To download the airgap-manifest.json file, click **Metadata** under the **Download** button.

   c. Transfer the airgap-ntnx-*version-number*.tar.gz and airgap-manifest.json deployment files to the *ntnx-version-number* directory on your self-hosted web server.

   d. Untar the airgap-ntnx-*version-number*.tar.gz file.

      tar -xvzf airgap-ntnx-version-number.tar.gz

      The following deployment files and directories appear: host-images, host-images.json, ntnx-k8s-releases, ntnx-k8s-releases.json.

3. Log on to karbonctl, see Logging on to the Karbonctl on page 41.

4. To deploy Airgap, replace the values as indicated and the run the following command.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl airgap enable \
--webserver-url http://webserver_url/ntnx-version-number/ \
--vlan-name network_name --static-ip static ip-address \
--storage-container storage_container_name \
--pe-cluster-name PE_cluster_name \
--pe-username user
```

   - Replace *webserver_url* with the URL of the web-server directory hosting the Airgap package.
   - Replace *version-number* with the Airgap bundle version number.
   - Replace *network_name* with the VLAN network name for the Airgap VM deployment.
   - Replace *static IP-address* with the static IP address for the Airgap VM deployment.
   - Replace *storage_container_name* with the name of the storage container that Airgap must use for volume deployment.
   - Replace *PE_cluster_name* with the name of the Prism Element (PE) cluster.
   - Replace *user* with the Prism Element (PE) user name.

     Note: It is optional to include --static-ip static ip-address in the above command.

   Airgap deployment process begins.

   You can track the deployment progress in the **Tasks** tab in PC. To track the progress using CLI, run the following command:

   nutanix@pcvm$ /home/nutanix/karbon/karbonctl airgap list

   Note: If HTTP proxy is configured in Prism Element, then add the Airgap VM IP address to the proxy allowlist.

   For information on adding an IP address to the proxy allowlist, see Configuring HTTP Proxy in the *Prism Element Web Console Guide*.

Disabling Airgap

Use the karbonctl to disable Airgap.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2269

About this task

> **Note:** If there are any Kubernetes clusters running, you cannot disable Airgap.

Procedure

1. Log on to the karbonctl, see Logging on to the Karbonctl on page 41.
2. To display the unique universal identifier (UUID) of Airgap, list all the Airgap UUIDs.

   ```
   nutanix@pcvm$ /home/nutanix/karbon/karbonctl airgap list
   ```

3. Replace *UUID* with the UUID for Airgap.

   ```
   nutanix@pcvm$ /home/nutanix/karbon/karbonctl airgap disable --airgap-uuid UUID
   ```

   > **Note:** If HTTP proxy was configured in Prism Element, then remove the Airgap VM IP address from the proxy allowlist.
   >
   > For information on removing an IP address from the proxy allowlist, see Configuring HTTP Proxy in the *Prism Element Web Console Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2270

7

KUBERNETES MANAGEMENT LAYOUT

The Kubernetes Management home page consists the **Clusters** and**OS Images** tabs. The **Clusters** tab is the main landing page and displays a list of all the Kubernetes clusters. The **OS Images** tab displays available CentOS images and the download image option.

- Clusters on page 20
- OS Images on page 26

Clusters

The **Clusters** tab includes the following sections and options:

- Create a cluster with the **Create Kubernetes Cluster** button.
- An **Actions** drop-down list with the following options:
  - Download the Kubernetes configuration file to your client by clicking **Download Kubeconfig**. The kubeconfig lets you run kubectl commands against the Kubernetes cluster, see Downloading the Kubeconfig on page 40.
  - The **SSH Access** option lets you access nodes in a Kubernetes cluster using an ephemeral certificate, which expires after 24-hours. See Accessing Locked Nodes on page 51.
  - Use the **Upgrade Node Image** option to upgrade the NKE node OS image for the cluster. See Upgrading a Node OS Image on page 60.
  - Use the **Upgrade Kubernetes** option to upgrade the Kubernetes version of the cluster. See Upgrading Kubernetes Using the Karbonctl on page 61.
  - Use the **Delete Cluster** to delete the selected cluster.

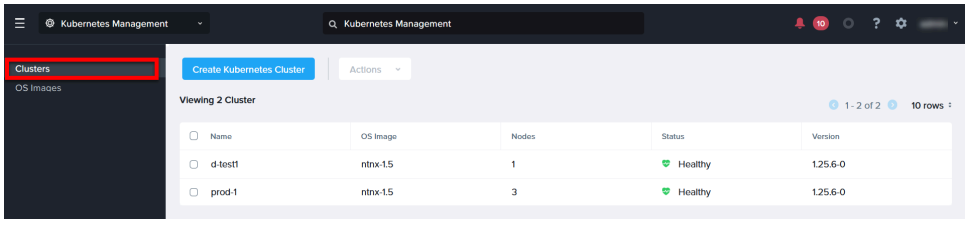


Figure 3: Kubernetes Management Clusters Table

The home page also includes a table with the following details of every cluster:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2271

Table 12: Clusters Table

Parameter	Description
Name	The name of the cluster.
OS Image	The node OS image version used for the cluster.
Nodes	The number of worker nodes on the cluster.
Status	The status field describes the health of the cluster, specifies the status of operations, and notes when there are available upgrades (**Deploying**, **Healthy**, **Upgrading**, **Failed**).
Version	Kubernetes version.

Clicking any name of a cluster on the **Clusters** page takes you to the **Summary** page of the cluster. The menu pane also includes the **Node Pools**, **Storage**, and **Activity** tabs.

Summary

Clicking the name of a cluster on the **Clusters** page takes you to the **Summary** page. The **Summary** page consists of multiple tiles that provide details on the clusters usage, alerts, tasks, and nodes.

Properties, Alerts, and Tasks

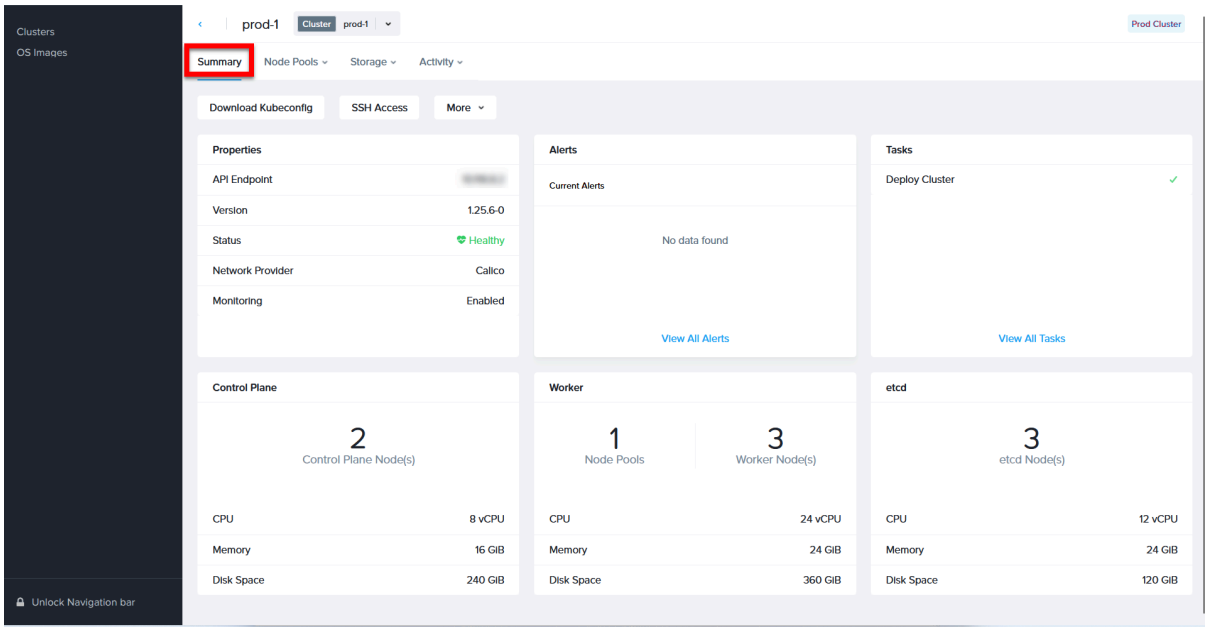


Figure 4: Summary Page

Table 13: Properties Tile

Parameter	Description
API Endpoint	Control plane server endpoint.
Version	Kubernetes version.
Status	The health status of the cluster.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2272

Parameter	Description
Network Provider	The network provider for the cluster.
Monitoring	Whether cluster monitoring is enabled or not.

Table 14: Alerts Tile

Parameter	Description
Current Alerts	Lists the number of **critical**, **warning**, and **info** alerts for the last 24 hours
Icon	An icon indicating the severity of the alert appears next to a description of the issue.
View All Alerts	Click the **View All Alerts** link to go to the **Alerts** tab.

Table 15: Tasks Tile

Parameter	Description
Task	Lists various operations on the cluster.
Icon	Indicates if the task completed successfully.
View All Tasks	Click the **View All Tasks** link to go to the **Tasks** tab.

Node Tiles

The node tiles display the following node details for each node type: etcd, control plane, and worker:

Table 16: Node Tile Parameters

Parameter	Description
Node(s)	The quantity of the specified nodes in the cluster.
vCPU	The total number of vCPUs for the specified node type.
Memory	The amount of memory currently in use out of the total configured memory.
Disk Space	The amount of disk space currently in use out of the total configured disk space.

Node Pools

The **Node Pools** tab provides three sub-tabs for each type of node in the cluster: **Control Plane**, **Worker**, and **etcd**. Each tab consists of a table with details about the indicated node type.

The **Worker** tab has a button to **Add Node Pool** and an **Actions** drop-down menu with options to **Delete**, **Resize**, and **Update** the selected node pool.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2273

Tabs for each node type provide a table with the following details:

Table 17: Control Plane and etcd Node Table Parameters

Parameter	Description
Name	The name of the node.
IP address	The IP address of the cluster.
CPU	The number of vCPUs allocated for the node.
Memory	The memory capacity for the node (GiB).
Storage	The storage capacity for the node (GiB).

Table 18: Worker Table Parameters

Parameter	Description
Name	The name of the node.
CPU	The number of vCPUs allocated per node.
Memory	The memory capacity per node (GiB).
Storage	The storage capacity per node (GiB).
Networks	The primary and additional networks configured for the node pool.
Labels (worker nodes only)	The key value pair labels of the node pool.
Number of Nodes	The number of worker nodes in the node pool. Clicking the dropdown arrow displays name and the IP address of each worker node.

Storage Classes

The **Storage** tab contains the **Storage Classes** option which includes the **Create Storage Class** and **Delete Storage Class** buttons. See Creating a Storage Class on page 42. The **Storage Classes** page also includes a table with details about each storage class. See table below for details.

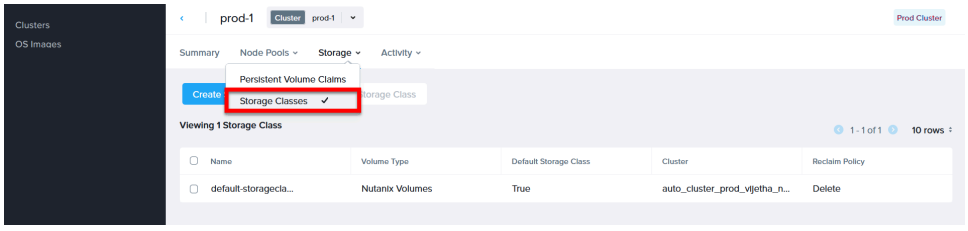


Figure 5: Storage Classes Page

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2274

Table 19: Storage Class Table Parameters

Parameter	Description
Name	The name of the storage class.
Volume Type	The type of storage used for Persistent Volumes.
Default Storage Class	Specifies if the storage class is the default (**True** or **False**).
Cluster	The name of the underlying cluster.
Reclaim Policy	The reclaim policy specifies what happens to the volume once it is not use (**delete** or **retain**).

Persistent Volume Claims

The **Storage** tab contains the **Persistent Volume Claims**option which includes the **Create Volume** and **Delete Volume** buttons. See Creating a Volume on page 44. The **Persistent Volume Claims** page also a table with details about each `PersistentVolume` (PV). See table below for details.

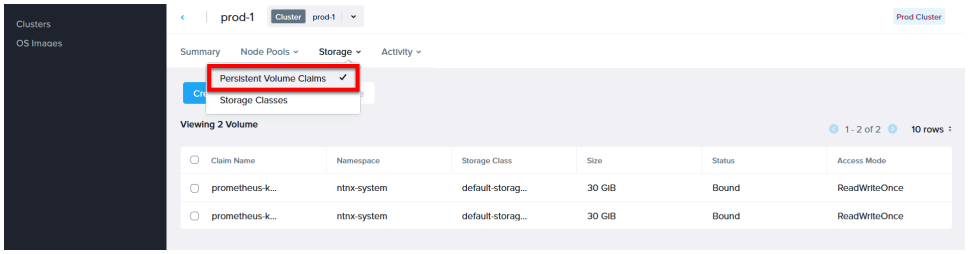


Figure 6: Persistent Volume Claims Page

Table 20: Persistent Volume Claims Table Parameters

Parameter	Description
Claim Name	Name used to attach storage to pods (maximum 253 characters). The name must start with a letter or a number. Only use lowercase alphanumeric characters, hyphens, and periods.
Namespace	Selected Kubernetes namespace (available options are displayed).
Storage Class	Storage class used by the volume.
Size	The size of the volume in GiB.
Status	Persistent volume status (**Pending**, **Available**, **Bound**, **Release**, **Failed**).
Access Mode	**ReadWriteOnce** is the only available access mode for Nutanix Volumes storage. Nutanix Files storage supports both **ReadWriteMany** and **ReadWriteOnce** access modes.

Alerts

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2275

The Alerts tab consists of a table that lists and describes recent alerts for the cluster. The Prometheus add-on powers Kubernetes Management alerts, see Monitoring on page 73.

The alerts table consists of the following parameters

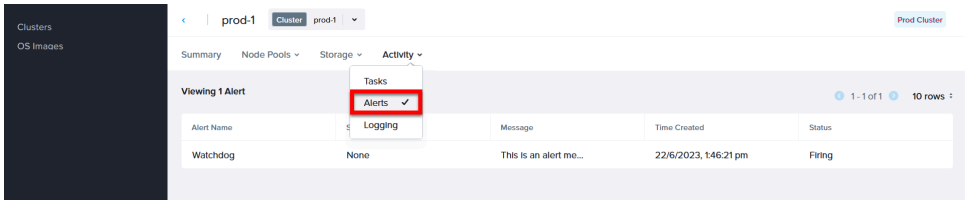


Figure 7: Alerts Page

Table 21: Alerts Table

Parameter	Description
Alert Name	The name of the alert.
Severity	The severity of the alert.
Message	A description of the alert issue.
Time Created	The date and time when the alert was created.
Status	The current status for the alert.

Tasks

The Tasks page consists of a table that lists and describes recent tasks performed on the cluster.

The tasks table consists of the following parameters.

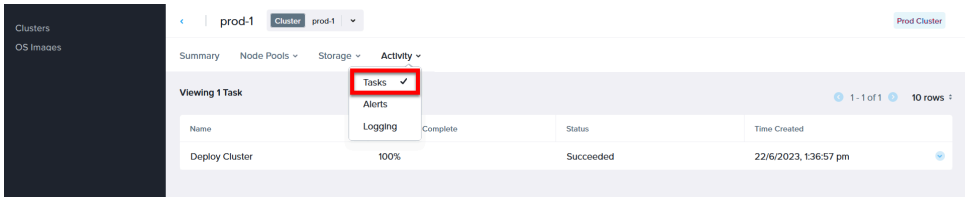


Figure 8: Tasks Page

Table 22: Tasks Table

Parameter	Description
Name	The name of the task including the entity.
Percentage Complete	The progress of the task displayed as a percentage.
Status	The status of the task.
Time Created	The date and time of task creation.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2276

Logging

The **Logging** page lists the add-ons installed on the Kubernetes cluster, see Add-Ons on page 71. For a description of the **Add-on** tab parameters for logging, see the table below.

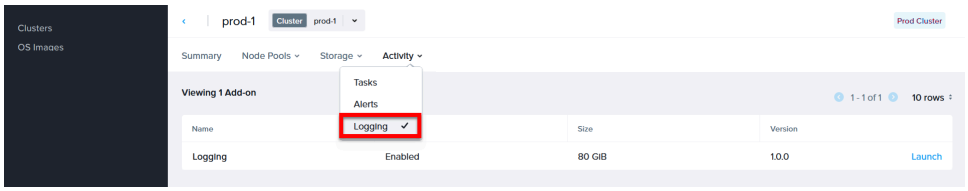


Figure 9: Add-ons Tab

Table 23: Add-On Table

Parameter	Description
Name	Name of the add-on.
State	Status of the add-on
Size	Disk space allocated to the add-on (GiB)
Version	Describes the version of the add-on, and includes a **Launch** add-on action link.

OS Images

The **OS Images** tab provides an overview of available and downloaded node OS images on your cluster. When a new version of an image is available, the tab includes options to download the new OS image. For steps to download a new image, see Downloading Images on page 41.

> **Note:** All supported OS images are provided by NKE during and after deployment. For information about image compatibility, see Nutanix Kubernetes Release Notes.

After downloading a new image from the OS images tab, upgrade cluster images through the **Clusters** tab, see Upgrading a Node OS Image on page 60.

The OS Images tab includes a table that describes the available, downloaded, and deleted images in your environment. For details, see the table below.

Table 24: OS Images Table

Parameter	Description
Image Version	The Linux distribution and image version.
Release Notes	A link to the release notes for the indicated OS image.
Size	The size of the OS image (GiB).
Download Status	The status of the image on your NKE deployment (Download, Downloading, and Downloaded).

8

CLUSTER SETUP

Creating an NKE cluster consists of setting up the following:

- Recommended configurations (optional)
- Name and environment
- Node configuration
- Network
- Storage class

For step-by-step directions for creating a Kubernetes cluster, see Creating a Cluster on page 29.

> **Caution:** Nutanix recommends adhering to the CIS Benchmark security recommendation for containers prior to deploying them on a Kubernetes cluster. For details, see the Nutanix Kubernetes Engine Release Notes.

Recommended Configurations

Before configuring your cluster, you can choose from one of the recommended configurations to streamline the deployment process. You can customize the recommended configurations during and after deployment.

The recommended configurations include two options: development cluster and production cluster. The development cluster option provides the minimum resources to launch a cluster. The production cluster configuration provides enough resources for a high-availability, production-ready cluster.

Name and Environment

To set up the Kubernetes environment, you must name the new cluster and add an optional description. The name must start with a letter or a number followed by up to 40 lowercase letters, numbers, or hyphens; (the name cannot end with a hyphen). You must specify the Prism Element (PE) cluster, the Kubernetes version, and the node operating system (OS) image. Run the Kubernetes cluster on any PE cluster that meets the requirements and has enough resources for the desired configuration.

Download a node OS image prior to deploying a cluster, see Downloading Images on page 41. NKE supports the CentOS Linux distribution. See Requirements on page 5 for a list of supported versions.

Node Configuration

> **Note:**
>
> - After the cluster configuration, the anti-affinity rules are automatically created for control planes and worker nodes between VMs.
> - Do not install Nutanix Guest Tools (NGT) or any other software onto the Kubernetes nodes.

To configure worker node, control plane, and etcd node resources, you must first specify the Kubernetes node network. The Kubernetes node network determines the network that the nodes run on. Optionally, you can also specify an additional node network to configure a dedicated network to optimize storage traffic. The additional node

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2278

network is specific to the I/O paths for the worker nodes and is responsible for any data or I/O optimization. Then, all the primary data management is handled by the primary node network while the data traffic travels through the secondary network. If the secondary network is not configured, then all the data traffic travels through the single primary node network. The purpose of the secondary network is to segment I/O traffic for optimization and security so that data travels through the secondary network interface.

Next specify the number of nodes and the virtual CPU (vCPU), memory, and size resources for each node type.

Worker nodes are responsible for services that run pods in a Kubernetes cluster. These services include Flannel for controlling traffic between nodes; Fluent Bit for system, pod, and node log collection; kubelet for running node operations; and the kube-proxy.

Etcd nodes store cluster configuration data and status details.

Control plane nodes run critical services including the API server, controller-manager, and kube-scheduler. Specify the control plane resource configuration from one of the following: single-control plane, active-passive, or external load balancer.

> **Note:** Do not use single-control plane deployments in production environments.

Single-control plane deployments have preconfigured resources. When a single-control plane node is unavailable due to upgrades, bugs, or maintenance, the scheduling service is also unavailable and NKE cannot deploy new pods. Multi-control plane deployments circumvent these issues by providing high-availability.

For multi-control plane deployments, you have the option of using an external load-balancer, which you must administer prior to deployment; or you can choose the Virtual Router Redundancy Protocol (VRRP), which NKE provides when you select the active-passive multi-control plane configuration.

Multi-control plane deployments backed by an external load balancer let nodes perform workload deployment and management at the same time, creating scalability by supporting more workloads. A load balancer requires multiple IP addresses: one external IP address and one private IP address for each control plane node. The kubectl, kubelet, and Kubernetes controllers use the public IP to communicate with the API server.

VRRP, the active-passive multi-control plane configuration, is an alternative to using a load balancer. VRRP does not provide the same scalability, but it does provide a backup control plane node for accessing the cluster if the active control plane happens to go down. Thus, when you select the active-passive configuration, the number of control plane nodes is always two.

Network

You can use Calico or Flannel as the container network interface (CNI). Flannel for NKE uses the VXLAN mode. To set up your network, you must provide classless inter-domain routing (CIDR) ranges and specify the network provider. You can leave the service CIDR and pod CIDR ranges as default, but the ranges must not overlap with each other or the existing network. The service CIDR and pod CIDR ranges do not require a VLAN. NKE does not route the ranges outside of the cluster.

For service CIDR range, there's a CIDR notation IP range from which you can assign IP addresses to service clusters. This must not overlap with any of the IP ranges assigned to nodes for pods. For pod CIDR range, Kubernetes assigns each node a range of IP addresses, so that each pod can have a unique IP address. The size of the CIDR block has an impact on the maximum number of pods and nodes.

> **Note:** The service and pod CIDR ranges once configured during NKE cluster creation cannot be modified later. If different service and pod CIDR ranges are required, create a new NKE Kubernetes cluster with different CIDR ranges and migrate your workloads.

When using Calico, all the nodes, control planes, and worker nodes (including worker node pools) have to be in the same L2 network. Only Flannel supports worker node pools in different L2 networks.

The number of required physical IP addresses varies depending on the configuration and the number of control plane, etcd, and worker nodes.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2279

For development environment configurations, NKE requires a dynamic host configuration protocol (DHCP), or a network with AHV IP address management (IPAM) enabled and IP pools setup.

For production environment configurations, IP requirements vary depending on the mode. For the active-passive mode, IPAM provides IPs for all of the nodes, and you must provide a virtual IP (VIP) for the Kubernetes API server. The VIP must be part of the same VLAN but outside of the IP pool. For an active-active mode, pre-configure the external load balancer and control plane nodes with designated IP addresses.

Storage Class

You can have multiple storage classes for your Kubernetes deployment, but once you assign a storage class to a cluster, you cannot modify it. A storage class defines the properties of a persistent volume (PV), which provides storage for the cluster. When the cluster needs more storage, a persistent volume claim (PVC) sends a request for a new PV. The PVC contains storage class details for the new PV.

Nutanix supports dynamic provisioning of PVs using the CSI Volume Driver, which runs in a Kubernetes pod. The CSI Volume Driver waits for a PVC request for a storage class and then creates a PV for that request. For more details, see CSI Volume Driver.

When deploying a cluster, NKE uses Nutanix Volumes storage. After deployment, you can add more storage classes and use either Nutanix Volumes or Nutanix Files storage.

For storage classes using Volumes, choose a Prism Element cluster. Next, select a storage container and a file system your cluster will use for allocating storage. Supported file systems include ext4 and xfs.

For Files, specify an NFS export that the cluster will use for storage.

To optimize the performance of a cluster, enable Flash Mode, which is available for both Volumes and Files. Enabling Flash Mode boosts the performance of a cluster by storing data only on the solid-state drives (SSDs) of the hot tier.

Creating a Cluster

Create an NKE cluster by configuring the cluster settings.

About this task

For details on setup options and requirements, see Cluster Setup on page 27.

Caution: Do not unregister the PE cluster hosting an NKE Kubernetes cluster from PC. Unregistration of PE from PC will prevent the management of the NKE clusters.

Note:

- Ensure that you are running a general availability (GA) version of NKE by performing an inventory check using the Life-Cycle Manager, see NKE Upgrades on page 59.
- Constrained bandwidth can lead to cluster deployment timeout.

Procedure

1. Log on to **Prism Central** as an administrator.
2. In the application switcher, select **Kubernetes Management**.
3. In the **Clusters** page, click **Create Kubernetes Cluster**.
   The **Create Cluster** page appears.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2280

4. In the **Recommended Configurations** tab, select one of the recommended configuration options.

   - **Development Cluster**: Used for development clusters only. Do not use this option for production environments. The option provides the minimum resources needed for a cluster.
   - **Production Cluster:** Used for production environments. It provides a default configuration for high-availability clusters.

5. Click **Next**.

6. In the **Name and Environment** section, do the following in the indicated fields:

   - **Kubernetes Cluster Name**: Enter a name for your cluster. The name must start with a letter or a number followed by up to 40 lowercase letters, numbers, or hyphens (cannot end with a hyphen).
   - **Nutanix Cluster**: Select the Prism Element cluster to run the Kubernetes cluster on.
   - **Kubernetes Version**: Select one of the Kubernetes versions.
   - **Host OS**: Select the version of the downloaded node OS image (**centos**), see Downloading Images on page 41.
   - **Disable Monitoring**: Select this check box to disable the monitoring stack (Prometheus) on the NKE cluster.

     Note: You can disable the monitoring stack only during cluster provisioning. Disabling the monitoring stack also disables the alerts in NKE UI. This setting cannot be modified later.

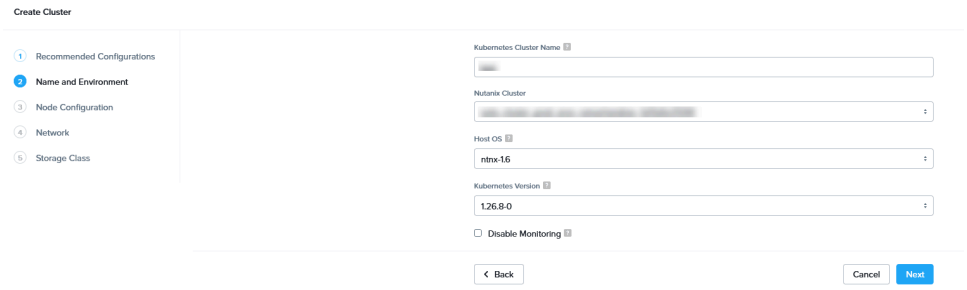


Figure 10: Name and Environment Configuration Window

7. Click **Next**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2281

8. In the **Node Configuration** tab, do the following in the indicated fields:

> **Caution:** If you exceed the available capacity on any underlying hardware when selecting memory, CPU, and disk size, the Kubernetes cluster cannot deploy.

a. Configure **Network Resources**:

- **Kubernetes Node Network**: Select one of the available networks.
- (Optional) **Additional Network**: To optimize network traffic, select another network from the PE cluster.

> **Note:** IPAM is available for production clusters. IPAM or DHCP is available for development clusters.

b. Configure **Worker Resources**:

- **Number of Workers**: Enter the number of Kubernetes worker nodes.
- (optional) Click **Edit** to customize worker resources:
  - **CPU**: Enter the number of vCPUs per worker node.
  - **Memory**: Enter the memory capacity per worker node (recommended 8 GiB per node).
  - **Size**: Enter the hard disk size (recommended 120 GiB per worker node).

c. Configure **Control Plane Resources**:

- **Select Control Plane Resource Configuration**: Select one of the following options from the dropdown:
  - 1 (suitable for non-production clusters only)
  - Multi-Control Plane: Active-Passive
  - Multi-Control Plane: External Load Balancer
- **Control Plane VIP IP Address** (active-passive only): Enter a VIP for the Kubernetes API server.

> **Caution:** Using the same managed network and IP addresses as another multi-control plane deployment results in deployment failure.

> **Note:** IPAM provides IPs for the nodes. The VIP must be part of the same VLAN but outside of the IP pool, see the "Network" section in Cluster Setup on page 27.

- **Number of Control Planes**: Enter the number of Kubernetes control plane nodes.

> **Note:** single-control plane and active-passive configurations have a set number of control plane nodes. Production deployments require at least two control plane nodes.

- (optional) Click **Edit** to customize worker resources:
  - **CPU**: Enter the number of vCPUs per node.
  - **Memory**: Enter the memory capacity per node.
  - **Size**: Enter the hard disk size (recommended 120 GiB per control plane node).
- (For external load balancer only) Enter IP addresses:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2282

> **Note:** The control plane IPs come from the non-DHCP pool of the AHV network. The IP addresses auto populate but are modifiable.

- **External Load Balancer IP**: Enter the IP address for the external load balancer.
- **Control Plane IP Addresses**: Enter an IP address for each control plane node.

> **Note:** If you use an external load balancer, it needs to be configured as an L4/TCP(443) load balancer pointing to each control plane node.

d. Configure **etcd Resources**:

- **Number of etcd nodes**: Select the number of etcd nodes.
- (optional) Click **Edit** to customize etcd resources:
  - **CPU**: Enter the number of vCPUs per node.
  - **Memory**: Enter the memory capacity per node.
  - **Size**: Enter the hard disk size (recommended 120 GiB per etcd node).

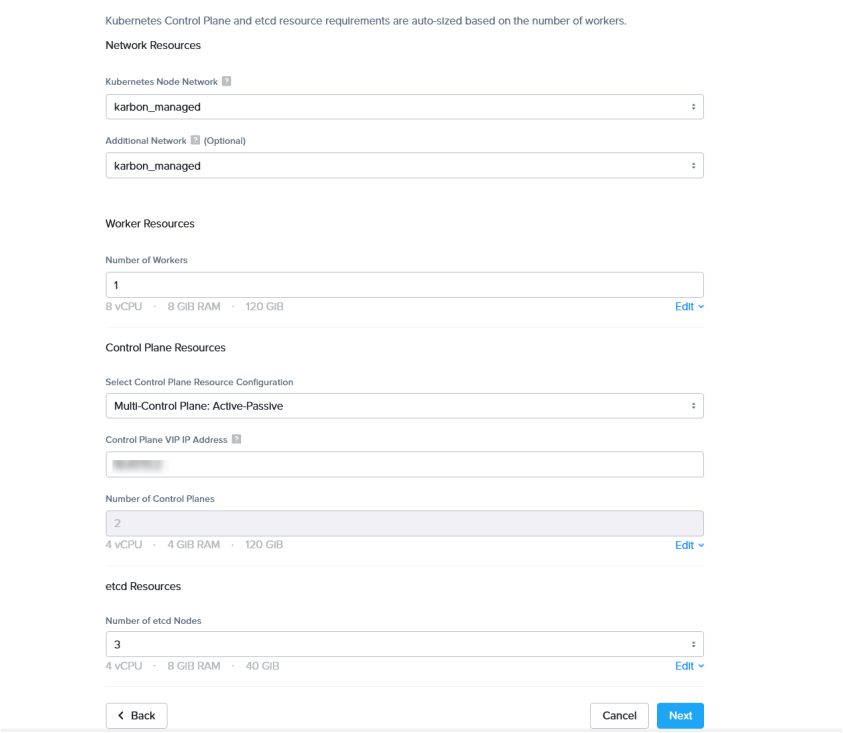


Figure 11: Network and Node Resources

9. Click **Next**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2283

10. In the **Network** tab, do the following in the indicated fields:

    For more information about Network, see Network on page 28.

    - **Network Provider**: Select the network provider from the dropdown menu.
    - **Service CIDR Range**: Enter an IP address range within your network range (RFC-1918) in CIDR notation, or use the default values. The IP range exposes services.

      Caution: The service CIDR and pod CIDR must not overlap with the Kubernetes node network IP range or with each other. Default ranges can overlap.

      Note: The service and pod CIDR ranges once configured during NKE cluster creation cannot be modified later. If different service and pod CIDR ranges are required, create a new NKE Kubernetes cluster with different CIDR ranges and migrate your workloads.

    - **Pod CIDR Range**: Enter an IP address range within your network range (RFC-1918) in CIDR notation for pod-to-pod communication. You can also use the default values. Kubernetes assigns pods in the cluster an IP address from this range.

      Note: Kubernetes configuration files refer to the pod CIDR as a "cluster IP".

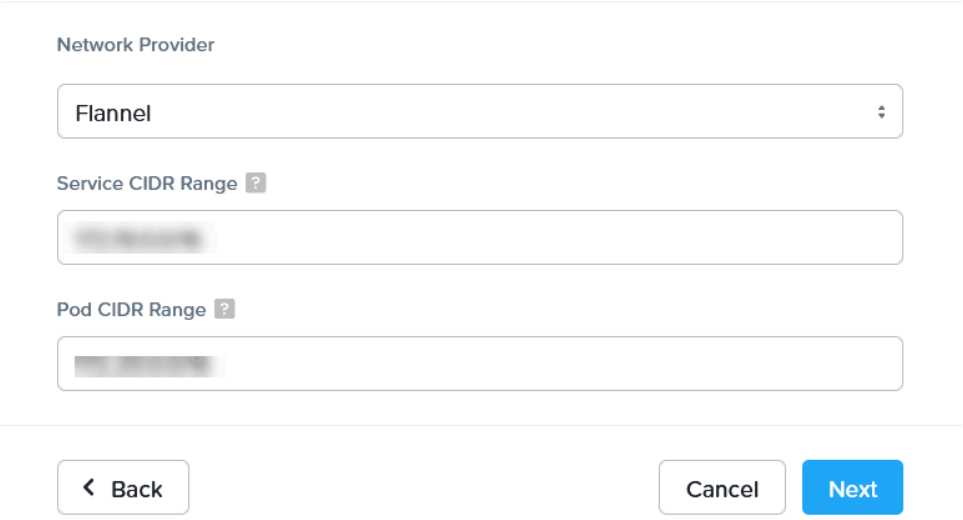


Figure 12: Network Configuration Window

11. Click **Next**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2284

12. In the **Storage Class** tab, do the following in the indicated fields:

> **Note:** You can create more storage classes once you create the cluster, see Creating a Storage Class on page 42.

> **Note:** During cluster deployment, NKE uses Nutanix Volumes storage for the storage class. After deployment, you can create a Nutanix Files storage class for the cluster.

- **Storage Class Name**: Enter the name for the storage class. The name must start with a letter or a number. Only use lowercase alphanumeric characters, hyphens, and periods (maximum 253 characters).
- **Nutanix Cluster**: Select the target cluster for allocating storage for stateful pods.
- **Storage Container Name**: Select the storage container for storage.
- **File System**: Select the file system for the storage class (xfs or ext4).
- **Reclaim Policy**: The reclaim policy specifies what the cluster does with the volume once it is not in use. Select **Delete** or **Retain**.
- **Enable Flash Mode**: Check this box to use SSDs for data storage and improved performance.

> **Note:** NKE automatically provisions some storage for node and system pod logs based on the size of the cluster.

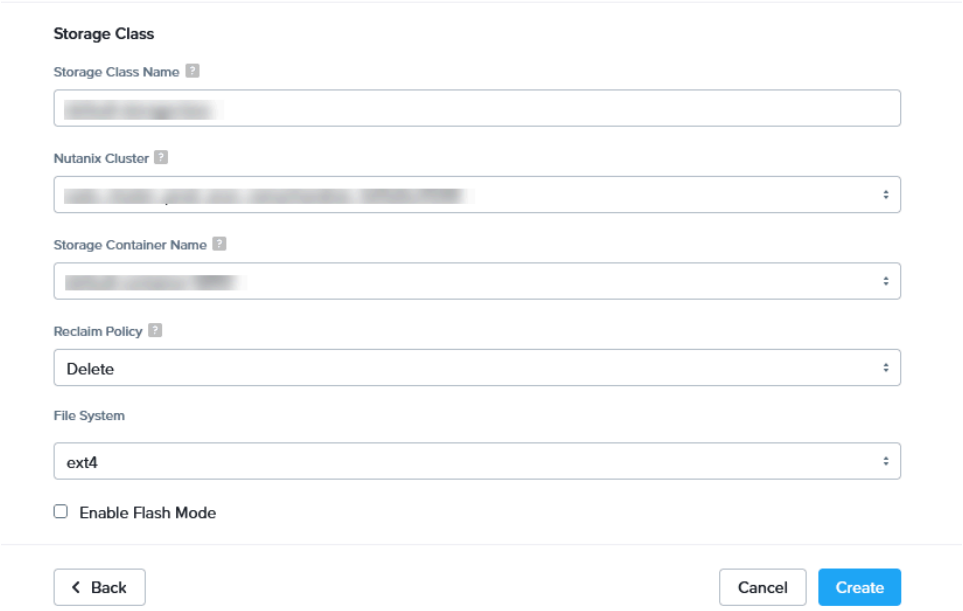


Figure 13: Storage Class Configuration Window

13. Click **Create**.
The new cluster appears on the Kubernetes Management home page. A new task for the cluster deployment displays the progress of the deployment in the **Tasks** tile on the **Summary** page.

> **Note:** After the cluster configuration, the anti-affinity rules are automatically created for control planes and worker nodes between VMs.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2285

Creating a Cluster Using API

Create a Kubernetes cluster using the karbonctl, the NKE command-line utility.

About this task

Deploying a Kubernetes cluster requires creating a JSON payload that includes the following specifications:

- Number of etcd nodes and etcd resource configuration
- Number or worker nodes and worker resource configuration
- Number of control plane nodes and control plane resource configuration
- Calico or flannel container network interface (CNI)
- Pod and service CIDR ranges for the CNI
- Kubernetes and node OS image versions

Cluster Setup on page 27 describes cluster deployment requirements and specifications in detail.

Perform the following tasks to deploy a Kubernetes cluster.

Procedure

1. Go to the Nutanix Developer Portal and create a JSON file using the POST /karbon/v1/k8s/clusters API code.
2. Update the attributes in a deployment JSON file and save the file. For information about cluster setup, see Cluster Deployment Attributes on page 35 and Cluster Setup on page 27.
3. Run the following command to deploy the cluster using the deployment JSON.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster create --filepath deployment-JSON-filepath
```

> **Note:** For additional customizations, see Nutanix Developer Portal.

Cluster Deployment Attributes

A description of API attributes for deploying a Kubernetes cluster using the karbonctl.

The following table describes the API code attributes for Kubernetes cluster deployment using the karbonctl. To deploy a cluster using the karbonctl, see Creating a Cluster Using API on page 35.

> **Tip:** You can find the required cluster and network-specific information in Prism or use the following commands.
>
> - To list the Prism Element (PE) unique universal identifier (UUID), run the following command from the PE cluster.
>
>   ```
>   nutanix@CVM:~$ ncli cluster info |grep "Cluster Uuid"
>   ```
>
> - To list the unique universal identifier (UUID) of the network, run the following command from the PE cluster.
>
>   ```
>   nutanix@CVM:~$ acli net.list
>   ```
>
> - To list the name of the container, run the following command from the PE cluster.
>
>   ```
>   nutanix@CVM:~$ ncli ctr list |grep Name|grep -v VStore
>   ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2286

Table 25: Deployment File Attributes

Object / Attribute Name	Attribute Name		Description	Value
`cni_config`	`node_cidr_mask_size`		The mask size of the node CIDR (Classless Inter-Domain Routing). The CIDR prefix.	[Integer]
	`pod_ipv4_cidr`		An IP address range within your network for pod-to-pod communication.	[An IP address range in CIDR notation. For example, 172.20.0.0/16.]
	`service_ipv4_cidr`		An IP address range within your network for service exposure.	[String in CIDR notation. For example, 172.20.0.0/16.]
`etcd_config`	`ahv_config`	`cpu`	The number of vCPUs per node.	[Integer]
		`disk_mib`	The hard disk size (recommended 130 GiB per etcd node).	[Integer] (GiB)
		`memory_mib`	The memory capacity per node.	[Integer] (MiB)
		`network_uuid`	The unique universal identifier (UUID) of the network.	[String]
		`prism_element_cluster_uuid`	The unique universal identifier (UUID) of the Prism Element (PE) cluster.	[String]
	`name`		The name of the etcd node pool.	[String]
	`node_os_version` **Note:** All node types (etcd, worker, and control plane) must use the same node OS version.		The version of the node OS image.	[String]
	`num_instances`		The number of etcd nodes.	[Integer]
`control planes_config`	`active_passive_`	`external_ipv4_address`	The IP address of the external load balancer.	[String]
	`external_lb_co`	`external_ipv4_address`	The IP address of the external load balancer.	[String]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2287

Object / Attribute Name	Attribute Name		Description	Value
		`ipv4_address`	The IP addresses of the control plane nodes. Enter an IP address for each node.	[String],
		`node_pool_name`	The name of the control plane node pool.	[String]
	`node_pools`	`cpu`	The number of vCPUs per node.	[Integer]
		`disk_mib`	The hard disk size	[Integer] (GiB)
		`memory_mib`	The memory capacity per node.	[Integer] (MiB)
		`network_uuid`	The unique universal identifier (UUID) of the network.	[String]
		`prism_element_cluster_uuid`	The unique universal identifier (UUID) of the Prism Element (PE) cluster.	[String]
		`name`	The name of the control plane node pool.	[String]
		`node_os_version` **Note:** All node types (etcd, worker, and control plane) must use the same node OS version.	The version of the node OS image.	[String]
		`num_instances`	The number of control plane nodes.	[Integer]
`metadata`	`api_version`		The API version used for cluster deployment.	v1.0.0
	`name`		The name of the Kubernetes cluster.	[String]
	`storage_class_config`	`default_storage_class`	The attribute specifies if the storage class used for the cluster is the default.	true, false
		`name`	The name of the storage class.	[String]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2288

Object / Attribute Name	Attribute Name		Description	Value
		`reclaim_policy`	The reclaim policy specifies what happens to a volume that is no longer in use.	Delete
		`volumes_config`		
		`file_system`	The file system for allocating storage.	ext4, xfs
		`flash_mode`	The flash tier provides high-performance storage when flash mode is enabled.	true. false
		`password`	Password for the PE cluster.	[String]
		`prism_element_cluster_uuid`	The unique universal identifier (UUID) for the PE cluster.	[String]
		`storage_container`	The name of the Nutanix storage container.	[String]
		`username`	The PE user name.	[String]
`version`			The Kubernetes version of the deployment. **Note:** For supported versions, see the Nutanix Kubernetes Release Notes.	[Decimal]
`workers_config`	`ahv_config`	`cpu`	The number of vCPUs per node.	[Integer]
		`disk_mib`	The hard disk size.	[Integer] (GiB)
		`memory_mib`	The memory capacity per node.	[Integer] (MiB)
		`network_uuid`	The unique universal identifier (UUID) of the network.	[String]
		`prism_element_cluster_uuid`	The unique universal identifier (UUID) of the Prism Element (PE) cluster.	[String]
	`name`	`name`	The name of the worker node pool.	[String]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2289

Object / Attribute Name	Attribute Name	Description	Value
	`node_os_version` **Note:** All node types (etcd, worker, and control plane) must use the same node OS version.	The version of the node OS image.	[String]
	`num_instances`	The number of worker nodes.	[Integer]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2290

9

CLUSTER ADMINISTRATION

Manage your Kubernetes clusters.

After deploying Kubernetes Management and creating Kubernetes clusters, you can manage the nodes, images, user access, and other aspects of your environment.

> **Note:** After the NKE cluster is deployed, there must be no manual modification of Kubernetes components (such as etcd, kubelet, API server, and so on) or add-ons (such as DNS, Prometheus, Elastic Search, and so on). The resource values for the logging and monitoring stack alone can be modified only when required.

Downloading the Kubeconfig

Before you begin

Ensure that you have downloaded kubectl to the machine from which you manage the cluster. Also, configure IAM on PC. For details, see the Prism Central Supplement.

About this task

The kubeconfig is a configuration file for running `kubectl` commands against the deployed Kubernetes cluster. The kubeconfig is signed for specific users rather than clusters. The kubeconfig token expires after 24 hours.

To deploy applications on your cluster using kubectl, download the Kubernetes cluster configuration file (*Kubeconfig*) to your host.

Procedure

1. In the Prism Central Kubernetes Management **Clusters** page, select a target cluster.
2. Click the **Actions** drop-down list.
3. Click **Download Kubeconfig**.

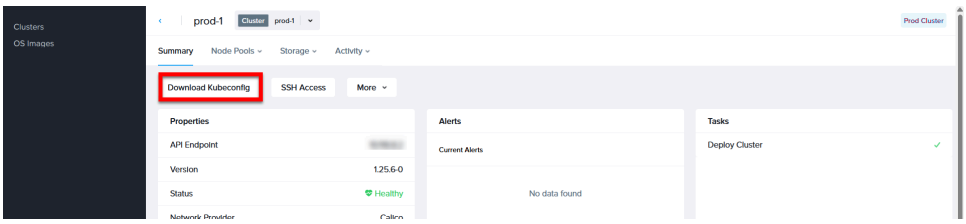


Figure 14: Download Kubeconfig Button

The **Download Kubeconfig** dialog box appears.

4. Under **Instructions**, click **Download**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2291

5. Run the kubeconfig commands by doing one of the following:

   » Click **Copy the command to clipboard** and run the command to finish the download process.

   » Manually run the required commands (continue to Step 6).

6. Replace the path to the *prod-1-kubectl.cfg* file with the file path to the downloaded file as it appears in your directory. Run the following command on your host.

   ```
   $ export KUBECONFIG=/path/to/prod-1-kubectl.cfg
   ```

   You have set the kubeconfig environment variable.

7. To test the cluster, run the following commands.

   ```
   $ kubectl cluster-info
   $ kubectl get nodes
   $ kubectl get pods --all-namespaces
   ```

Logging on to the Karbonctl

Use the indicated CLI command to log on to the karbonctl.

About this task

The karbonctl is the NKE command-line utility that you can use to manage Kubernetes.

Procedure

Log on to karbonctl from a PC VM.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl login --pc-username username \
--pc-password password
```

> **Note:** It is optional to include --pc-password password in the above command.

Downloading Images

About this task

Deploying Kubernetes clusters in NKE requires a CentOS image. You must choose from a CentOS version and download the image.

> **Caution:** You must use one of the images provided by Nutanix.

> **Note:** The Airgap package includes downloaded node OS images.

About this task

Follow these steps to download a node OS image.

Procedure

1. Log on to **Prism Central** as an administrator.
2. In the application switcher, select **Kubernetes Management**.
3. Select **OS Images** in the left navigation pane.
4. In Kubernetes Management, click the **OS Images** tab in the menu pane.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2292

5. Click **Download** to start the download process.
   The **Download Status** column will show the progress of the download.

Creating a Storage Class

About this task

After you create your first cluster and your first storage class, you can create additional storage classes through the Storage Class tab.

> **Note:** Changes to the Cluster Virtual IP or admin user name in Prism Element affect the storage class configuration. For Cluster Virtual IP and user name update assistance, contact Nutanix Support.

> **Note:** The first time you create a cluster, you also create the default storage class. For instructions about changing the default storage class, see the *Kubernetes Documentation*.

Follow these steps to create a storage class.

Procedure

1. In the Prism Central Kubernetes Management **Clusters** page, select a target cluster.
2. Click the **Storage** tab and select **Storage Classes** from the drop-down list.
3. Click **Create Storage Class**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2293

4. (For Nutanix Files, go to Step 5) For Nutanix Volumes storage, do the following in the indicated fields in the **Create Storage Class** window:

   - **Volume Type**: Select **nutanix_volumes**.
   - **Storage Class Name**: Enter the name for the storage class. The name must start with a letter or a number. Only use lowercase alphanumeric characters, hyphens, and periods (maximum 253 characters).
   - **Nutanix Cluster**: Select the target cluster for allocating storage for stateful pods.
   - **Storage Container Name**: Select the storage container to user for persistent volumes (PVs).
   - **File System**: Select the file system for the storage class (xfs or ext4).
   - **Reclaim Policy**: The Reclaim Policy specifies what the cluster should do with the volume once it is not in use. Select **Delete** or **Retain**.
   - **Enable Flash Mode**: Check this box for improved performance. With Flash Mode, NKE uses only SSDs in the hot-tier for storage.

     Note: Some storage is automatically provisioned for node and system pod logs based on the size of the cluster.

   a. Continue to Step 6.

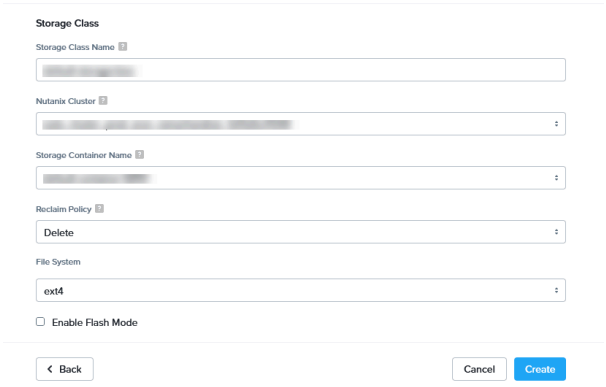


Figure 15: Nutanix Volumes - Storage Class

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2294

5. For Nutanix Files storage, do the following in the indicated fields in the **Create Storage Class** window::

   - **Volume Type**: Select **nutanix_files**.
   - **Storage Class Name**: Enter the name for the storage class. The name must start with a letter or a number. Only use lowercase alphanumeric characters, hyphens, and periods (maximum 253 characters).
   - **NFS Export Endpoint**: Enter the endpoint within the NFS export. The endpoint must be a host name or an IP address.
   - **NFS Export Path**: Enter the path to the NFS export endpoint.
   - **Reclaim Policy**: The Reclaim Policy specifies what the cluster should do with the volume once it is not in use. Select **Delete** or **Retain**.

   Note: Some storage is automatically provisioned for node and system pod logs based on the size of the cluster.

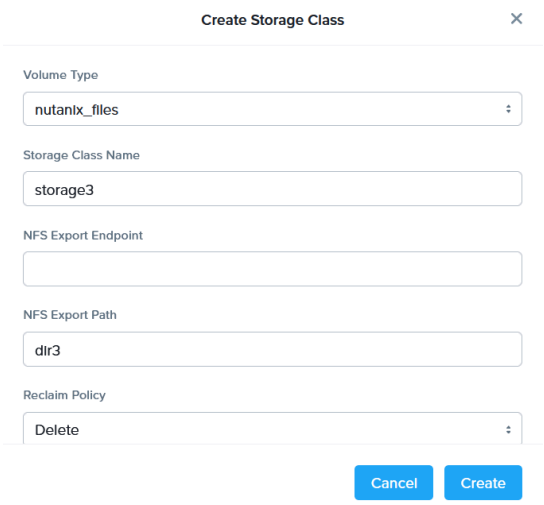


Figure 16: Nutanix Files - Storage Class

6. Click **Create**.

Deleting a Storage Class

About this task

Follow these steps to delete a storage class.

Procedure

1. In the Prism Central **Clusters** page, select a target cluster.
2. Click the **Storage** tab and select **Storage Classes** from the drop-down list.
3. Select the storage class you want to delete.
4. Click **Delete Storage Class**.

Creating a Volume

Create a Persistent Volume (PV) for your cluster.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2295

About this task

Procedure

1. In the Prism Central Kubernetes Management **Clusters** page, select a target cluster.
2. Click the **Storage** tab and select **Persistent Volume Claims** from the drop-down list.
3. Click **Create Volume**.
4. Do the following in the indicated fields:
   a. **Claim Name**: Enter a name for the Persistent Volume Claim
   b. **Storage Class**: Select a storage class.
   c. **Access Mode**: Select an access mode from **Read Write Once** or **Read Only Many**.
   d. **Volume**: Enter the size for the volume (GiB).

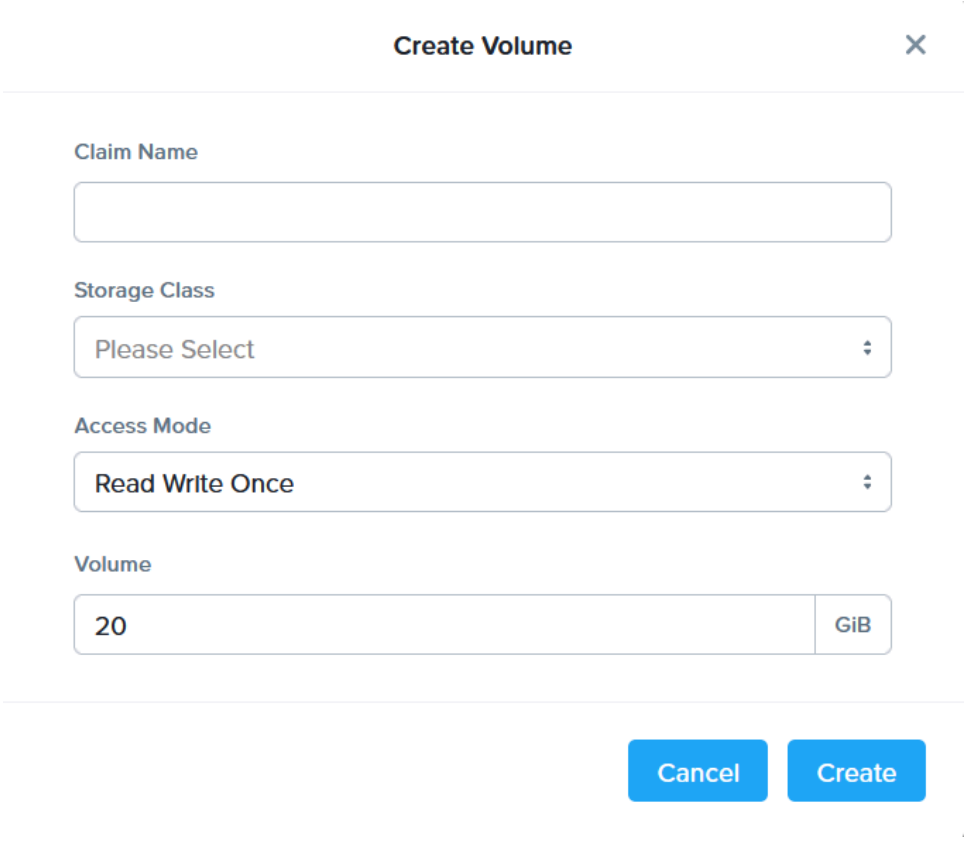


Figure 17: Create Volume Window

5. Click **Create**.

Deleting a Volume

About this task

Follow these steps to delete a volume.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2296

Procedure

1. In the Prism Central Kubernetes Management **Clusters** page, select a target cluster.
2. Click the **Storage** tab and select **Persistent Volume Claims** from the drop-down list.
3. Check the volume you want to delete.
4. Click **Delete Volume**.

Creating a Node Pool

Create one or more worker node pools on the cluster.

About this task

A node pool is a set of nodes with the same configuration. Node pools help accommodate the varying resource and scaling needs of different workflows. Follow the steps as indicated to create a node pool.

Procedure

1. In the Prism Central Kubernetes Management **Clusters** page, select a target cluster.
2. Click the **Node Pools** tab and select **Worker** from the drop-down list.
3. Click **Add Node Pool**.
4. In the **Add Node Pool** window, do the following:
   - **Name**: Enter a name for the node pool.

     Note:

     - Only use alphanumeric characters or the hyphen (-) special character.
     - The combined length of cluster name and node pool name can be a maximum of 41 characters.

       The format of a Kubernetes node object name is as follows:

       `<cluster-name>-<6-digit-random-uuid>-<node-pool-name>-worker-<index>`

       A Kubernetes node object name can have a maximum of 63 characters. For more information about the same, see the *Kubernetes Documentation*.

       Considering that `<index>` can be a maximum of three characters, the combination of cluster name and node pool name cannot exceed 41 characters.
   - **Number of Nodes**: Enter an integer for the number of worker nodes.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2297

5. Do the following in the fields under **Node Properties**:

   - **CPU**: Enter an integer for the amount of CPU allocated per node.
   - **Memory**: Enter an integer for the amount of memory allocated per node (GiB).
   - **Storage**: Enter an integer for the amount of storage allocated per node (GiB).
   - **Node Pool Network**: Choose the primary network for the nodes. Use any network of the Prism Element (PE) cluster that has connectivity with the NKE cluster.

     > **Note:** When you configure the Kubernetes cluster to use Calico, ensure that all the nodes are in the same L2 network. Only Flannel supports worker node pools in different L2 networks.
     >
     > For example, a Kubernetes cluster using Flannel CNI has four application pods deployed on different node pools. Pods 1 and 2 are deployed on node pool 1 with primary subnet and pods 3 and 4 are deployed on node pool 2 with secondary subnet. As Flannel CNI is an overlay network, pods 1 and 2 can communicate with pods 3 and 4 across different subnets.
     >
     > In a Kubernetes cluster using Calico CNI with four application pods deployed on different node pools, pods 1 and 2 that are deployed on node pool 1 with primary subnet can communicate with each other. However, pods 1 and 2 cannot communicate with pods 3 and 4 on node pool 2 with secondary subnet.

   - (optional) **Additional Network**: The iSCSI network used for I/O optimization.

6. (Optional) This step is applicable only if passthrough GPUs are available in the node pool) Do the following in the fields under **GPU**:

   » If you do not want to configure passthrough GPUs for the node pool, select **None**. This option is selected by default.

   » If you want to configure passthrough GPUs for the node pool, see Configuring GPU on page 49.

   You can also configure GPUs using Karbonctl. For details, see Configuring GPU Using Karbonctl on page 50.

7. Under **Metadata**, do the following:

   Use key and value pairs to add meaningful labels to the node pool in the **Kubernetes Labels** field.

   - **Key**: Enter a descriptive label for the key (for example, `environment`).

     > **Note:** Only use alphanumeric characters or the hyphen (`-`) special character.

   - **Value**: Enter a descriptive label for the value (for example, `dev`).
   - Click **+**.
   - (optional) To add more key value pairs, click **+**.

8. Click **Add**.

Updating the Number of Worker Nodes

To resize a node pool, add or remove the number of worker nodes.

About this task

You can't modify memory, storage, and CPU details. Perform the following steps as indicated to add or reduce the number of worker nodes in your cluster.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2298

Procedure

1. In the Prism Central Kubernetes Management **Clusters** page, select a target cluster.
2. Click the **Node Pools** tab and select **Worker** from the drop-down list.
3. Select the target node pool.
4. In the **Actions** drop-down list, select **Resize**.

   Note:

   - If you want to delete a worker node, then select the option **Actions** > **Delete**.
   - You cannot delete the default node pool or the last remaining worker node from the default node pool.
   - As you cannot delete the last worker node in the default node pool from the Kubernetes Management UI, you must not delete that worker node from Prism Element either.

5. In the **Resize Node Pool** window, under **Total Number of Nodes**, indicate the desired number of worker nodes for the node pool.

   For example, if you currently have three worker nodes in the node pool but you want to have a total of five nodes, click **+** so that the **Total Number of Nodes** is **5**.

   Note:

   - Reducing the number of nodes might delete the most recently added nodes.
   - When GPUs are assigned to nodes in a node pool, each node is assigned an equal number of GPUs. Hence, to increase the number of nodes in a node pool, ensure that sufficient number of unassigned GPUs are available in the Kubernetes cluster for the new nodes. If no unassigned GPUs are available, the UI does not allow you to increase the node count.

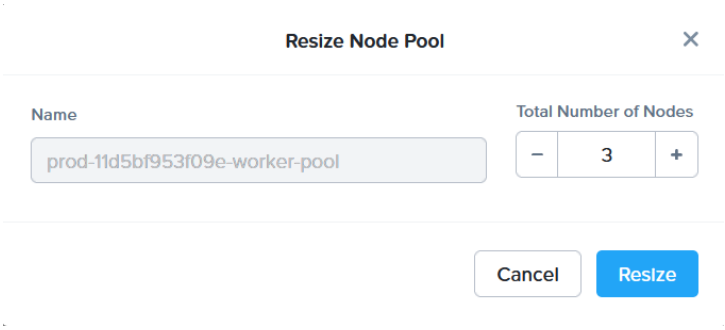


Figure 18: Resize Node Pool Window

6. Click **Resize**.

Updating Node Pool Metadata

Update the metadata of a node pool.

About this task

Follow the steps as indicated.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2299

Procedure

1. In the Prism Central Kubernetes Management **Clusters** page, select a target cluster.
2. Click the **Node Pools** tab and select **Worker** from the drop-down list.
3. Select the target node pool.
4. In the **Actions** drop-down list, select **Update**.
   The **Update Node Pool** window appears. The only fields that can be updated are those under **Metadata**. All the other fields will be greyed out and cannot be updated.
5. Under **Metadata**, do the following:

   Use key and value pairs to add meaningful labels to the node pool in the **Kubernetes Labels** field.

   - **Key**: Enter a descriptive label for the key (for example, `environment`).

     Note: Only use alphanumeric characters or the hyphen (`-`) special character.

   - **Value**: Enter a descriptive label for the value (for example, `dev`).
   - Click **+**.
   - (optional) To add more key value pairs, click **+**.
   - (optional) To delete a key value pair, click the **Delete label** icon.
6. Click **Update**.

Configuring GPU

Create a node pool configured for passthrough GPU.

Note: You can also configure GPUs using Karbonctl. For details, see Configuring GPU Using Karbonctl on page 50.

Before you begin

Meet the following requirements:

- Install the ntnx-1.2 node OS image or higher on the cluster.
- Allocate a minimum of 9 GiB of memory for the worker node pool to support installation of the NVIDIA GPU operator.
- Ensure that the host has supported GPU hardware. In the Prism Central **Infrastructure** dashboard, go to **Hardware** > **GPUs**.
- Check that AHV supports the GPU, see Supported GPUs in the *AHV Administration Guide*.
- Nutanix recommends reviewing the NVIDIA GPU compatibility and support.

  Note: GPU enablement requires installation of NVIDIA datacenter driver software governed by NVIDIA licensing terms.

- Passthrough GPUs must be in compute mode.

  For more information about passthrough GPU, see GPU Pass-Through for Guest VMs in the *AHV Administration Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2300

About this task

Follow the steps as indicated.

Procedure

1. Perform Step 1 to Step 6 from Creating a Node Pool on page 46.
2. Select **Passthrough**.
3. Click the **Configure GPU** button.
   A window that lists all the GPUs available for the Kubernetes cluster and options to configure them appears.
4. Configure the GPUs as required and click **Save**.
   A window asking to confirm the GPU configuration appears. This message appears for the first time only within an **Add Node Pool** session.
5. Click **Confirm**.
   The GPU configuration is now displayed in the **Add Node Pool** window.

What to do next

- If you want to modify the GPU configuration, click the **Configure GPU** link and make the necessary changes.
- If you want to delete a GPU configuration, click the delete icon corresponding to that configuration.
- To continue with creating a node pool, go to Step 7 in Creating a Node Pool on page 46.

Configuring GPU Using Karbonctl

The following topic details the steps to configure passthrough GPU using Karbonctl.

Before you begin

Meet the following requirements:

- Install the ntnx-1.2 node OS image or higher on the cluster.
- Allocate a minimum of 9 GiB of memory for the worker node pool to support installation of the NVIDIA GPU operator.
- Ensure that the host has supported GPU hardware. In the Prism Central **Infrastructure** dashboard, go to **Hardware** > **GPUs**.
- Check that AHV supports the GPU, see "Supported GPUs" in the *AHV Administration Guide*.
- Nutanix recommends reviewing the NVIDIA GPU compatibility and support.

  > **Note:** GPU enablement requires installation of NVIDIA datacenter driver software governed by NVIDIA licensing terms.

- Passthrough GPUs must be in compute mode.

  For more information about passthrough GPU, see GPU Pass-Through for Guest VMs in the *AHV Administration Guide*.

About this task

Follow the steps as indicated.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2301

Procedure

1. List the passthrough GPU configurations associated with the PE cluster of the NKE cluster.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster gpu list –cluster-name name-of-karbon-cluster
```

2. Add a GPU configuration to a node pool.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster node-pool  add --cluster-name name-of-cluster
 --node-pool-name name-of-node-pool --count number-of-nodes --gpu-count gpus-per-node
--gpu-name gpu-config-type --memory size-GiB
```

   Include additional parameters as needed.

   - Specify the number of CPUs (8 by default): `--cpu number-of-CPUs`.
   - Specify the size of the hard disk (120 GiB by default): `--disk-size size-GiB`
   - Add a label by specifying a key-value pair (for example, `--labels environment=dev`): `--labels key=value`.
   - Specify the name or the universally unique identifier (UUID) of the VLAN: `--vlan-name name` or `--vlan-uuid UUID`.

Access and Authentication

Prism Central (PC) users with the "User Admin" role have full access to Kubernetes Management, NKE, and its functionalities. Performing most of the karbonctl operations require admin privileges. PC users that do not have the "User Admin" role can only access Kubernetes Management to download the kubeconfig and cannot perform any other administrative tasks. Nutanix requires configuring Kubernetes Management users to a directory service in Prism. For instructions about assigning roles or configuring a directory service, see Security and User Management in the *Prism Element Web Console Guide*.

After setting up and testing your cluster, configure role-based access control (RBAC). For more information, see *Kubernetes Documentation*.

To access a node in the cluster, you must receive an ephemeral certificate, see Accessing Locked Nodes on page 51.

Accessing Locked Nodes

About this task

NKE protects all nodes in a cluster. You can access nodes in a Kubernetes cluster using an ephemeral certificate, which expires after 24-hours. Perform the following steps to get a certificate.

Procedure

1. In the Prism Central Kubernetes Management **Clusters** page, select a target cluster.
2. Click the **SSH Access** button.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2302

3. In the **Node SSH Access** window, click **Download** to download and save the SSH access script to your client.

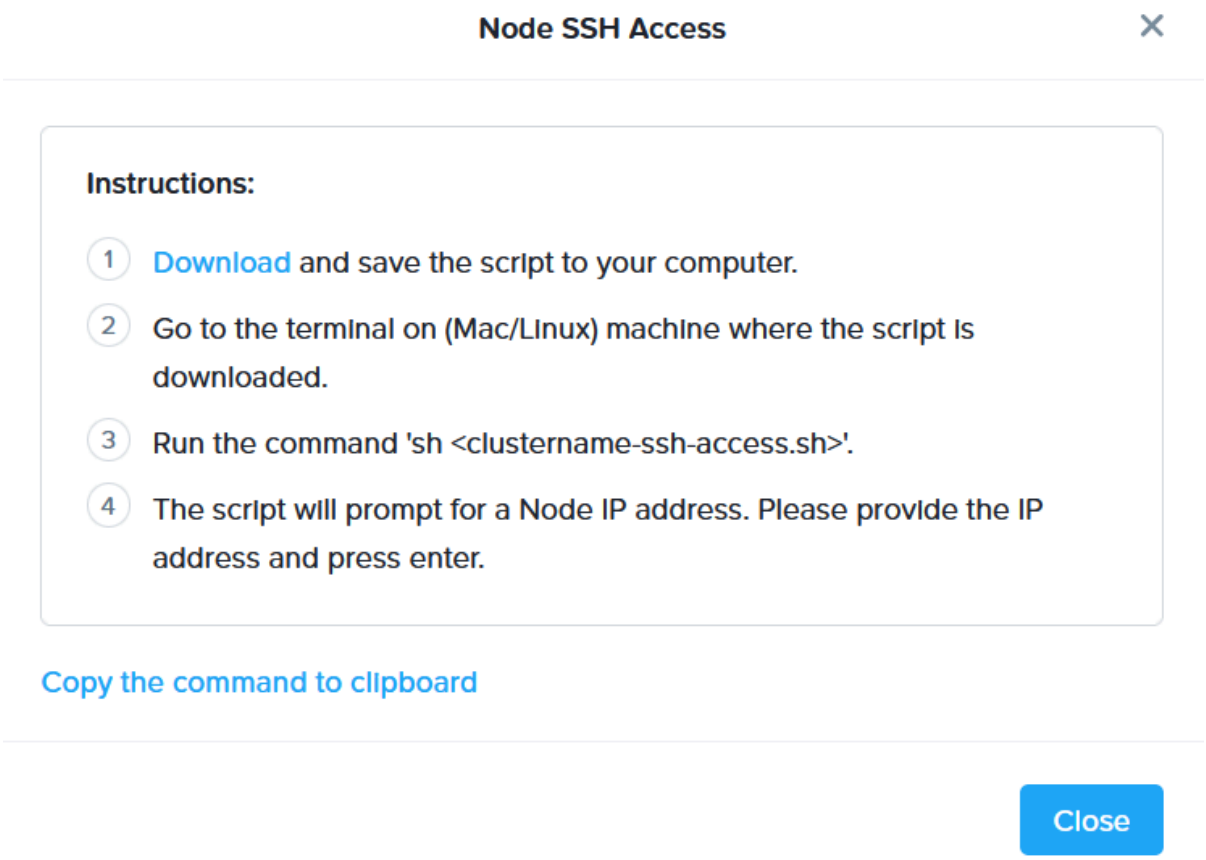


Figure 19: Node SSH Access

4. Run the following command. sh <cluster_name>-ssh-access.sh
5. When prompted, enter the IP of any node in the cluster to get access to all nodes.
   NKE grants the user a private key.
6. Log on to the target node as a Nutanix user using the command line.

Rotating Certificates

Update certificates for cluster services and add-ons.

About this task

Cluster certificates expire after two years. Once a certificate expires, the cluster becomes unhealthy, which can lead to unsuccessful operations on the cluster. Triggering a certificate rotation on a cluster restarts add-ons and node services, including the kubelet and the API server.

To trigger certificate rotation, follow the steps as indicated.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2303

Procedure

Initiate certificate rotation.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster certificates rotate-cert --
cluster-name k8-cluster-name
```

Migrating DVP and CSI to Use Certificate-Based Authentication

Migrate DVP and CSI to use certificate-based authentication.

Before you begin

Ensure that the cluster is healthy.

About this task

To migrate DVP and CSI from using user name/password-based authentication to using certificate-based authentication, certificate rotation should be initiated.

To trigger certificate rotation, follow the steps as indicated.

Procedure

Initiate certificate rotation.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster certificates rotate-cert --
cluster-name k8-cluster-name
```

Restarting the karbon_core Service

Restart the karbon_core service on a cluster.

About this task

Run the following commands from a Prism Central console.

Procedure

1. Stop the `karbon_core` service on all the PCVMs.

   ```
   nutanix@pcvm$ allssh "genesis stop karbon_core"
   ```

2. Start the `karbon_core` service.

   ```
   nutanix@pcvm$ cluster start
   ```

What to do next

To know about the impact of restarting the karbon_core service, see Impact of Restarting the karbon_core Service on page 53.

Impact of Restarting the karbon_core Service

When the NKE controller is down or unavailable, the management of the NKE clusters such as creation of new clusters and performing operations on existing clusters, is not possible. However, the applications on the clusters function without disruption.

Restarting the karbon_core service might result in a transient disruption in the management operations of the NKE clusters and workloads from the NKE UI or API. The API operations on the Kubernetes clusters with the NKE generated kubeconfig are also disrupted. However, after the karbon_core service is running, the API operations resume automatically.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2304

Upon restarting the karbon_core service, an action called scrubbing is performed on every cluster. It is meant to handle the following operations:

- Any required PC/PE proxy configuration changes.
- NKE feature enhancements such as improved kubelet garbage-collection parameter thresholds.
- NKE bugs such as misconfigured service monitor for scraping monitoring metrics.

If any of the above operations are required on the clusters, then they are performed on the nodes in sequence (that is, one node at a time). While these are being performed on a particular node, the container runtime or the kubelet of that node would be restarted. During this time, the node would be unhealthy.

Backing up Etcd

Back up your NKE cluster etcd data regularly.

About this task

> **Important:** The following procedure does not back up the application data.

Follow the steps as indicated to back up etcd data only.

Procedure

1. Collect the IP addresses of etcd nodes.
   a. In the Prism Central Kubernetes Management **Clusters** page, select a target cluster.
   b. Click the **Node Pools** tab and select **etcd** from the drop-down list.
   c. Note the IP addresses of each etcd node.
2. Back up the etcd data from only one node.
   a. Securely log on to a single etcd node using SSH (see Accessing Locked Nodes on page 51).
   b. Use sudo to become the root user.

```
$ sudo su
```

   c. Back up the etcd data.

```
# export ETCD_IP_0=<replace with etcd 0 IP address>
```

```
# export ETCDCTL_API=3
```

```
# export ETCDCTL_CACERT=/var/nutanix/etc/etcd/ssl/ca.pem;export \
ETCDCTL_CERT=/var/nutanix/etc/etcd/ssl/peer.pem;export \
ETCDCTL_KEY=/var/nutanix/etc/etcd/ssl/peer-key.pem
```

```
# etcdctl --endpoints https://$ETCD_IP_0:2379 snapshot save /root/snapshot.db
```

   d. Copy /root/snapshot.db to a safe location. For example, copy the file using SFTP (Secure File Transfer Protocol) or SCP (Secure Copy Protocol).

Stopping an NKE Cluster

Gracefully stop an NKE cluster.

Before you begin

- Stop the apps and pods in the NKE cluster. This helps reduce the possibility of data corruption.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2305

- Take a backup of the Kubernetes cluster etcd data (see Backing up Etcd on page 54).

About this task

Follow the steps as indicated to shut down an NKE cluster.

Procedure

1. Collect the cluster name and IP address of one of the control plane nodes.
   a. In Kubernetes Management, select the target cluster, expand **Nodes**, and click **Control Plane**.
   b. Note the IP address of one control plane node.
2. Use SSH to log on to one of the control plane nodes (see Accessing Locked Nodes on page 51) for shutting down the Kubernetes pods.
   a. Cordon the worker nodes to prevent the scheduler from placing new pods onto the nodes.
   ```
   $ kubectl cordon -l 'kubernetes.io/role=node'
   ```
   b. Drain the worker nodes to gracefully shutdown the pods.

      Note: This command ignores any PodDisruptionBudget.

   ```
   $ kubectl drain -l 'kubernetes.io/role=node' --disable-eviction --ignore-
   daemonsets --delete-emptydir-data --force
   ```
   c. Wait for the previous command to complete its execution.
3. Use Prism Central UI to select the worker nodes.
   a. In Prism Central, click the hamburger menu, expand **Compute & Storage**, and then click **VMs**.
   b. Click **Filters**, select the **Name** checkbox, change the option to **Starts with**, and type the following:

      karbon-*`kubernetes_cluster_name-`*

      Where, *`kubernetes_cluster_name-`* is the name of the NKE cluster.
   c. Ensure that the filter is only showing the desired Kubernetes cluster nodes.
   d. Select the virtual machines with the text **worker** in their name.
4. Soft shutdown the worker nodes.
   a. With the worker nodes selected, click **Actions** and then click **Guest Shutdown**.
   b. Click **OK** to confirm.
5. Once the worker nodes are powered off, perform Step 3 for control plane nodes.
   a. Clear the worker nodes.
   b. Select the virtual machines with the text **master** in their name.
   c. Soft shutdown the control plane (see Step 4).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2306

6. Once the control plane nodes are powered off, perform Step 3 for etcd nodes.
   a. Clear the control plane nodes.
   b. Select a single etcd node.
   c. Soft shutdown the etcd node (see Step 4).
      Repeat the steps for each etcd node on the cluster once the previous node has been powered off.

Starting an NKE Cluster

Starting an NKE cluster after shutdown.

About this task

Follow the steps as indicated to start an NKE cluster.

Procedure

1. Use Prism Central UI to select the etcd nodes.
   a. In Prism Central, click the hamburger menu, expand **Compute & Storage**, and then click **VMs**.
   b. Click **Filters**, select the **Name** checkbox, change the option to **Starts with**, and type the following:
      karbon-`kubernetes_cluster_name-`
      Where, `kubernetes_cluster_name-` is the name of the NKE cluster.
   a. Ensure that the filter is only shows the desired Kubernetes cluster nodes.
   b. Select the virtual machines with the text **etcd** in their name.
2. Start all etcd nodes.
   a. With the etcd nodes selected, click **Actions** followed by **Power On**.
   b. Click **OK** to confirm.
3. Collect the IP addresses of etcd nodes.
   a. In Kubernetes Management, select the target cluster, expand **Nodes** in the sidebar, and click **etcd**.
   b. Note the IP addresses for each etcd node.
4. Securely log on to an etcd node using SSH, see Accessing Locked Nodes on page 51.
5. Use sudo to become the root user.
   ```
   $ sudo su
   ```
6. Verify that services have started on all etcd nodes.
   ```
   # export ETCD_IP_0=<replace with etcd 0 IP address>
   # export ETCD_IP_1=<replace with etcd 1 IP address, only production clusters>
   # export ETCD_IP_2=<replace with etcd 2 IP address, only production clusters>
   # export ETCDCTL_API=3
   # export ETCDCTL_CACERT=/var/nutanix/etc/etcd/ssl/ca.pem;export \
   ETCDCTL_CERT=/var/nutanix/etc/etcd/ssl/peer.pem;export \
   ETCDCTL_KEY=/var/nutanix/etc/etcd/ssl/peer-key.pem
   # export ETCDCTL_ENDPOINTS=\
   ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2307

```
"https://$ETCD_IP_0:2379,https://$ETCD_IP_1:2379,https://$ETCD_IP_2:2379"
```

```
# etcdctl -w table endpoint status
```

The output generated should be similar to the following image, displaying three etcd nodes with one of them as the leader.

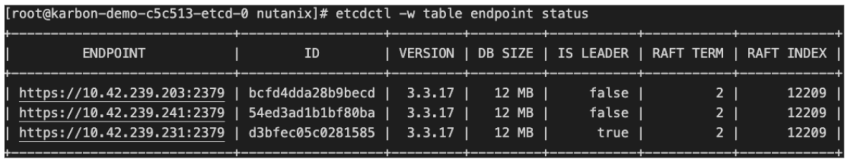


Figure 20: Starting an NKE Cluster - Verifying Services on All Etcd Nodes

7. If there are any missing etcd nodes, ensure the following:
   a. The nodes are up.
   b. The etcd service has started.
   c. There is network connectivity.
8. Start all control plane nodes.
   a. Perform Step 1 for control plane nodes.
      - Clear the etcd nodes.
      - Select the virtual machines with the text **master** in their name.
   b. Power on the control plane (see Step 2).
9. Use SSH to log on to one of the control plane nodes (see Accessing Locked Nodes on page 51) to check the control plane status.
   a. To verify that the control plane nodes are up, use the `kubectl` to check for the Ready status.
      $ watch kubectl get nodes
   b. If the control plane nodes are NotReady, then check whether there are connection issues between the control plane nodes and etcd nodes.
10. Start all the worker nodes.
    a. Perform Step 1 for worker nodes.
       - Clear the control plane nodes.
       - Select the virtual machines with the text **worker** in their name.
    b. Power on the workers (see Step 2).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2308

11. Use SSH to log on to one of the control plane nodes (see Accessing Locked Nodes on page 51) to check the cluster status and uncordon the worker nodes.

    a. To verify that all worker nodes are up, use the kubectl to check for the `Ready`, `SchedulingDisabled` status.

    ```
    $ watch kubectl get nodes
    ```

    b. Uncordon all the worker nodes to start the pods.

    ```
    $ kubectl uncordon -l 'kubernetes.io/role=node'
    ```

    c. To verify that all pods are up, use the kubectl to check for the `Running` status.

    ```
    $ watch kubectl get pods --all-namespaces
    ```

12. In the Kubernetes Management UI, verify that the cluster status is healthy.

10

UPGRADES

There are two different types of NKE upgrades:

- NKE version upgrades using the Life Cycle Management feature, see NKE Upgrades on page 59.
- Node OS image upgrade, see Upgrading a Node OS Image on page 60.

Perform LCM upgrades through Prism Central (PC). Kubernetes Management and NKE are part of the PC upgrades module in LCM. LCM upgrades the following components:

- NKE version
- Kubernetes Management UI

Perform node OS image upgrades through Kubernetes Management. When a node OS image upgrade is available, Kubernetes Management displays an option to download the new image in the **OS Images** tab, see OS Images on page 26. Kubernetes Management also displays an **Upgrade Available** icon next to the cluster in the **Clusters** view, see Upgrading a Node OS Image on page 60.

NKE Upgrades

To check the current version of NKE or to upgrade to later versions, perform the inventory check in Prism Central using LCM.

For steps about performing inventory and upgrades in LCM, see the Life Cycle Manager Guide. Ensure that you are running a compatible version of Prism Central (PC), Prism Element, and AOS. For compatibility details, see the Nutanix Kubernetes Engine Release Notes.

> **Note:**
>
> - To use the new Kubernetes versions and features, migrate NKE 2.10 to Nutanix Kubernetes® Platform (NKP).
>
>   For more information, see the Nutanix Kubernetes Engine Migration Guide.
> - After enabling PC-scale out, upgrade all PC nodes to a compatible version of NKE.
> - Before upgrading NKE to the latest version, ensure that all the deployed clusters are running the minimum supported Kubernetes minor version for the latest NKE version. If the Kubernetes minor version in the clusters is older than the minimum supported version, the LCM upgrade task for NKE_version will fail with LCM pre-check task failure.
>
>   The Kubernetes version is composed of *major.minor.patch*. The Kubernetes version required for the NKE upgrade refers to only the minor version, not the patch version.

First Time NKE Users

Perform the following tasks to install NKE in your environment.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2310

- Perform an inventory and upgrade to a compatible version of PC using the Life Cycle Management (LCM) feature in PC. For more information, see the *Life Cycle Management Guide*.
- Enable Kubernetes Management. For more information, see Enabling Kubernetes Management on page 14.
- In LCM, perform inventory and update NKE to the latest available version.

Impact of NKE Upgrade

During NKE upgrade, the `karbon_core` service is restarted.

For information about the impact of restarting the `karbon_core` service, see Impact of Restarting the karbon_core Service on page 53.

Upgrading a Node OS Image

Upgrade the node OS images for your cluster.

About this task

Caution:

- Upgrading a node OS image clears the contents of the /dev/sda boot disk. Ensure that the /dev/sda disk does not contain any persistent content or files.
- Do not use the local storage for pods. Upgrading a node OS image deletes the data in the local storage.

Note: NKE supports legacy images on existing clusters. Existing Kubernetes clusters do not require an image upgrade.

Procedure

1. In the Prism Central Kubernetes Management, **Clusters** page, select a target cluster.

   Note: Clusters that have an image eligible for an upgrade display the **Upgrade Available** icon.

2. From the **Actions** drop-down list, select **Upgrade Node Image**.

   » Download the target image.

   » Upgrade using previously downloaded image (continue to Step 6).

3. In the **Upgrade Host Image OS** window, click **Download** to download the target image. Wait for the image to download.

4. Select the target image, and click **Upgrade**.
   The status of the upgrade displays under **Status** on the **Clusters** page. More details about the upgrade display on the **Tasks** tile.

Upgrading Kubernetes

Upgrade the Kubernetes version of your cluster.

Note:

When you upgrade an older Kubernetes version to Kubernetes 1.22 or a newer version in NKE:

- The container runtime in the cluster is automatically migrated from Docker to Containerd.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2311

- Configurations made to private registries and HTTP proxy settings on this cluster are retained through the upgrade. You do not need to configure them again.
- With the container runtime changing to Containerd, Docker CLI commands will not be supported.

About this task

Perform the following steps as indicated to upgrade the Kubernetes version of your cluster.

Caution: Avoid using local storage pods. Upgrading Kubernetes deletes the data in the local storage.

Procedure

1. In the Prism Central Kubernetes Management, **Clusters** page, select a target cluster.

   Note: Clusters that have a Kubernetes version eligible for an upgrade display the **Upgrade Available** icon in the table.

2. From the **Actions** drop-down list, select **Upgrade Kubernetes**.
3. Under **List of Available Kubernetes Version for Upgrade**, select the target Kubernetes version.

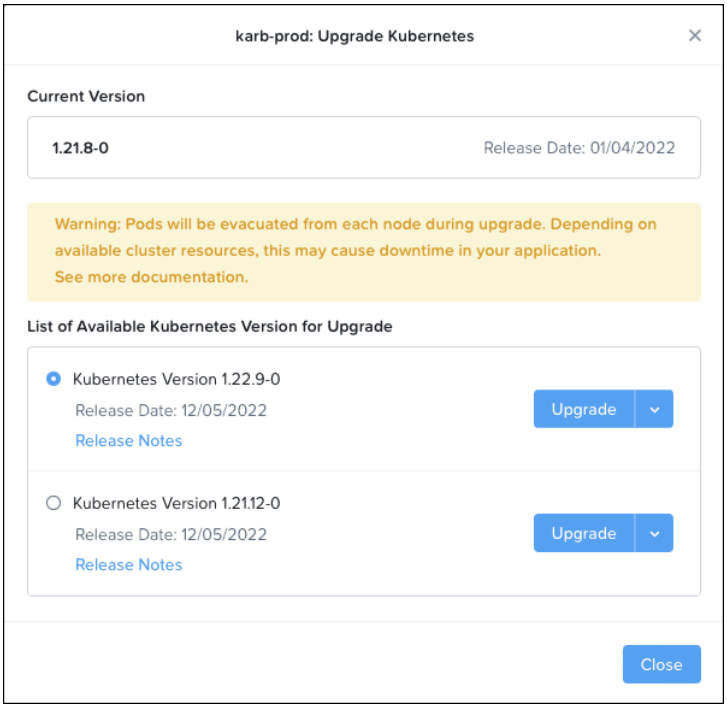


Figure 21: Upgrading Kubernetes - Versions Available for Upgrade

4. Click the dropdown arrow next to **Upgrade**.
   a. To check the health of nodes and underlying components, click **Precheck**.
   b. To upgrade to the selected Kubernetes version, click **Upgrade**.
   The upgrade task initiates. You can monitor the upgrade process in the **Tasks** view.

Upgrading Kubernetes Using the Karbonctl

Upgrade the Kubernetes version of your cluster.

About this task

You can use the karbonctl to manually perform Kubernetes upgrades instead of using the Kubernetes Management UI. For steps to log on to the karbonctl, see Logging on to the Karbonctl on page 41.

Procedure

1. List Kubernetes versions and names of existing clusters.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster list
```

2. Get the latest add-on versions.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl k8s get-from-portal
```

3. Get the list of compatible upgrade paths.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster k8s get-compatible-versions --
cluster-name cluster name
```

4. Upgrade the cluster to the specified Kubernetes version.

> **Note:** The package consists of Kubernetes and add-on versions. Currently, NKE only supports the Kubernetes version.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster k8s upgrade --cluster-
name cluster name \
--package-version package version
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2313

5. NKE allows you to modify the `drainpolicy` and `draintimeout` settings for upgrade using the following commands.

   - For the karbonctl cluster os-image upgrade:
     - `--drain-policy`: Drain policy command to perform the OS image upgrade operation. The Drain policy parameters are:
       - `kAlways` (Default): Will always perform a drain of the node.
       - `kBestEffort`: Will attempt to perform a drain of the node but in case the drain fails, an upgrade is performed and the kubelet is restarted. This behavior might be due to pod disruption budget (PDB) constraints or longer drain time and will fall back to the behaviour of `Never`.
       - `kNever`: Will not perform a drain of the node at all but just upgrade and restart the kubelet.
     - `--drain-timeout-secs`: Drain timeout (in seconds) command to drain a node. Default is 600 seconds.
   - For the karbonctl cluster Kubernetes upgrade:
     - `--drain-policy`: Drain policy command to perform the Kubernetes upgrade operation. The Drain policy parameters are:
       - `kAlways` (Default): Will always perform a drain of the node.
       - `kBestEffort`: Will attempt to perform a drain of the node but in case the drain fails, an upgrade is performed and the kubelet is restarted. This behavior might be due to pod disruption budget (PDB) constraints or longer drain time and will fall back to the behaviour of `Never`.
       - `kNever`: Will not perform a drain of the node at all but just upgrade and restart the kubelet.
     - `--drain-timeout-secs`: Drain timeout (in seconds) command to drain a node. Default is 600 seconds.

   You can use the `kAlways`, `kBestEffort`, or `kNever`custom flag parameter to invoke the kubectl drain command when the eviction or deletion of pods fail. One of the reasons for such failure is either due to strict pod disruption budget (PDB) constraints or longer drain time based on the number of pods. You can resolve this issue by increasing the `--drain-timeout-secs` value or setting the `--drain-policy` to `kBestEffort`.

What to do next

Check the upgrade status in the **Tasks** view, or using karbonctl.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster k8s upgrade status --cluster-
name cluster name
```

Upgrading Airgap using LCM

Upgrade Airgap using the Life-Cycle Manager (LCM).

Before you begin

You need a self-hosted web server reachable by your Nutanix clusters to host the LCM repository.

> **Note:** Airgap upgrades using Prism Central (PC) 5.16.1.2 cause an error. Upgrade PC 5.16.1.2 before attempting to upgrade Airgap.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2314

Procedure

1. From a device that has public Internet access, go to **Nutanix Support Portal** > **collapse menu icon** > **Downloads** > **LCM**.
   a. Next to **LCM Framework Bundle (Version)**, click **Download** to download the lcm_dark_site_bundle_*version-number*.tar.gz file.
   b. Transfer lcm_dark_site_bundle_*version-number*.tar.gz to your self-hosted web server and untar into the release directory.
2. From a device that has public Internet access, go to **Nutanix Support Portal** > **collapse menu icon** > **Downloads** > **Nutanix Kubernetes Engine**.
   a. Next to **NKE LCM Bundle (Version)**, click **Download** to download the lcm_NKE_*version-number*.tar.gz file.
   b. Transfer lcm_NKE_*version-number*.tar.gz to your self-hosted web server and untar into the release directory.
3. Log on to Prism Central.
4. Click **Home** > **LCM** > **Settings**.
   a. In the **Fetch updates from** field, enter the path to the directory where you extracted the tar file on your local server. Use the format http://webserver_IP_address/release.
   b. Click **Save**.
   You return to the Life Cycle Manager.
   c. In the LCM sidebar, click **Inventory** > **Perform Inventory**.
   d. Update the LCM framework before trying to update any other component.
   The LCM sidebar shows the LCM framework with the same version as the file you downloaded.

Updating OS Images and Kubernetes for Airgap

To upgrade OS images and the Kubernetes version on Airgap, upload Airgap bundle and manifest files to a web server.

Before you begin

- Review *Nutanix Kubernetes Engine Release Notes* for image compatibility details.
- Create directory ntnx-*version-number* on a self-hosted web server.

  Note:
  - As a best practice, use the full version number. Example: ntnx-2.0.0 or ntnx-2.0.1.
  - Create the directory on a path that is reachable via HTTP on the web server. Example: /var/www/html/ntnx-*version-number*.
- Ensure that NKE is upgraded to the required version for the new packages.

Procedure

1. From a device that has public Internet access, go to Nutanix Support Portal.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2315

2. Navigate to **collapse menu icon** > **Downloads** > **Nutanix Kubernetes Engine**.

   a. To download the airgap-ntnx-*version-number*.tar.gz file, next to **NKE Airgap bundle**, click **Download**.

   b. To download the airgap-manifest.json file, click **Metadata** under the **Download** button.

   > **Tip:** Verify that the NKE version in the airgap-manifest.json is for a version that includes new images.

3. Transfer airgap-ntnx-*version-number*.tar.gz and airgap-manifest.json files to a self-hosted web server.

   a. Transfer and untar the files in the ntnx-*version-number* directory.
   tar -xvzf airgap-ntnx-version-number.tar.gz

4. Log on to karbonctl, see Logging on to the Karbonctl on page 41.

5. Upload the new images to Airgap. Replace *airgap-UUID* with the universally unique identifier (UUID) for Airgap. Replace *webserver-directory-URL* with the URL for the directory you transferred files to in Step 3.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl airgap package-upload --airgap-
uuid airgap-UUID \
--webserver-url webserver-directory-URL
```

   > **Note:** Run the following command to find the UUID for Airgap.
   >
   > ```
   > nutanix@pcvm$ /home/nutanix/karbon/karbonctl airgap list
   > ```

6. Track the deployment progress in the **Tasks** tab in Prism Central UI.

   To track the progress using CLI, run the following command:

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl airgap list
```

7. To upgrade the Kubernetes version, follow steps in Upgrading Kubernetes Using the Karbonctl on page 61.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2316

11

OPTIONS

NKE provides multiple options to further customize your Kubernetes implementation. Starting with NKE 2.6, the ELK-based NKE logging stack is not enabled by default.

Note:

- You can deploy the ELK-based NKE logging stack to provide a simplified experience for users with environments that do not have the logging stack implementation. In environments where the logging implementation exists or where there are no explicit requirements for logging, disable the logging stack to reduce resource consumption.
- The minimum uplink speed recommended is 30 Mb/s.

Enabling Alert Forwarding

About this task

This procedure describes the steps for enabling SMTP-based alert forwarding to an e-mail address.

Procedure

1. List the names of Kubernetes clusters.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster list
```

2. Replace the variables in the command as indicated.

Note: If you have enabled transport-level security (TLS), specify the *ca-cert-path*, *client-cert-path*, and *key-path* variables.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster alerts enable-smtp  --cluster-
name="cluster-name" --from-email-address="from-email-address" \
--host="host-address" --to-email-address="to-email-address" --port=port-number --
smtp-username="smtp-username" \
 --smtp-passwd="smtp-password" --tls
```

- Replace *cluster-name* with the name of the Kubernetes cluster.
- Replace *from-email-address* with the email address to be used as Source.
- Replace *to-email-address* with comma separated email address(es) to be used as Destination.
- Replace *host-address* with the IP address or DNS name of the SMTP server.
- Replace *port-number* with the Port of the SMTP server.
- (Optional) Replace *smtp-username* with the user name for SMTP authentication.
- (Optional) Replace *smtp-password* with the password for SMTP authentication.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2317

- (Optional) Use `--tls` for TLS/STARTTLS.

Disabling Alert Forwarding

About this task

This procedure describes the steps for disabling SMTP-based alert forwarding.

Procedure

1. List the names of Kubernetes clusters.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster list
```

2. Disable alert forwarding. Replace the *cluster-name* with the name of the target cluster.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster alerts disable-smtp --cluster-
name="cluster-name"
```

Enabling Infra Logging

About this task

This procedure describes the steps for enabling infra logging stack (Elasticsearch and Kibana) on a Kubernetes cluster for system namespace.

Procedure

1. List the names of Kubernetes clusters.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster list
```

2. Enable infra logging. Replace the *cluster-name* with the name of the target cluster.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster infra-logging enable --cluster-
name="cluster-name"
```

Disabling Infra Logging

About this task

This procedure describes the steps for disabling infra logging stack (Elasticsearch and Kibana) on a Kubernetes cluster for system namespace.

Procedure

1. List the names of Kubernetes clusters.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster list
```

2. Disable infra logging. Replace the *cluster-name* with the name of the target cluster.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster infra-logging disable --cluster-
name="cluster-name"
```

Configuring a Private Registry

Configure a private registry service to your Kubernetes cluster.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2318

About this task

By default, NKE does not add additional container image registries to Kubernetes clusters. To use your own images for container deployment, add a private registry to NKE and configure private registry access for the intended Kubernetes clusters.

Follow the steps as indicated to configure a private registry for your cluster.

Procedure

1. Add the private registry to NKE.

   ```
   nutanix@pcvm$ /home/nutanix/karbon/karbonctl registry add --name registry-name \
   --url registry-url [--port registry-port] [--username username --password password] \
   [--cert-file cert-filepath]
   ```

   Replace the arguments as indicated.

   - Replace *registry-name* with name of the registry.
   - Replace *registry-url* with the URL of the registry.
   - It is optional to specify *registry-port*. It needs to be specified only if you are not using the default port (443) for your private registry.
   - To apply user name and password authentication to the registry, replace *username* and *password* with the desired authentication credentials.

     > **Note:** The `karbonctl registry add` command uses `username` and `password` only to test the registry and not to configure them in Kubernetes to allow access to the registry. Configuring the Kubernetes cluster to authenticate to the private registry using the specified `username` and `password` must be done manually after adding the registry.

   - If the registry is certificate-based, replace *cert-filepath* with the file path to the certificate.

     > **Note:**
     >
     > - Omit the *cert-filepath* parameter for HTTP-based registries. The Docker configuration supports insecure registries.
     > - To configure a private registry that use token authentication instead of certificates, contact Nutanix support.

2. Check for custom registries known to NKE.

   ```
   nutanix@pcvm$ /home/nutanix/karbon/karbonctl registry list
   ```

3. Add the private registry to a Kubernetes cluster. Replace *cluster-name* with the name of the Kubernetes cluster. Replace *registry-name* with the name of the registry (as in Step 1).

   ```
   nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster registry add --cluster-name \
   cluster-name --registry-name registry-name
   ```

4. Confirm that the NKE and the Kubernetes clusters have access to the custom registry. Replace *cluster-name* with the name of the Kubernetes cluster.

   ```
   nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster registry list --cluster-
   name cluster-name
   ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2319

Deleting a Private Registry

Delete a private registry from your NKE environment.

About this task

Delete access to a private registry before removing the registry from NKE. Follow the steps as indicated:

Procedure

1. Delete access to a private registry from your Kubernetes cluster. Replace *cluster-name* with the name of the Kubernetes cluster, and replace the *registry-name* with the name of the target registry.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster registry delete --cluster-
name cluster-name \
--registry-name registry-name
```

2. **Note:** Before deleting the registry, revoke registry access from all clusters.

   Delete a private registry from NKE. Replace the *registry-name* with the name of the target registry.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl registry delete --registry-
name registry-name
```

Enabling Log Forwarding

Steps to enable log forwarding to an external endpoint (Syslog or Elasticsearch).

About this task

The logs forwarded to the endpoints are:

- Fluent Bit logs of all the pods and containers
- Kubelet logs
- Container logs and Journald logs of the etcd nodes

Procedure

1. List the names of Kubernetes clusters.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster list
```

2. Replace the variables in the command as indicated.

   Note: If you have enabled transport-level security (TLS), specify the *ca-cert-path*, *client-cert-path*, and *key-path* variables.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster log-forward enable  --cluster-
name="cluster-name" --endpoint_type endpoint-type \
--host="host-IP-address" --port=port-number --http_username="http-username" \
 --http_passwd="http-password" --ca_cert ca-cert-path --cert client-cert-path \
--key key-path
```

   - Replace *cluster-name* with the name of the Kubernetes cluster.
   - Replace *endpoint-type* with type of external logging endpoint, this can be elasticsearch or syslog.
   - Replace *host-IP-address* with the name of the external endpoint.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2320

- Replace *port-number* with the external endpoint port.
- (Optional) Replace *http-username* with the HTTP user name for Elasticsearch authentication.
- (Optional) Replace *http-password* with the HTTP password for Elasticsearch authentication.
- (Optional) Replace *ca-cert-path* with the absolute path to the certificate authority (CA) file. Use the privacy enhanced mail (PEM) format.
- (Optional) Replace *client-cert-path* with the absolute path to the client certificate signed by the CA. Use the PEM format.
- (Optional) Replace *key-path* with the absolute path to the client key.

You can also configure the following parameters if you have enabled transport-level security (TLS):

- *enable-tls*: To enable or disable TLS support for the external elasticsearch endpoint. The default value is `false`.
- *enable-tls-verify*: To enable or disable TLS force certificate validation for the external elasticsearch endpoint. The default value is `false`.

Disabling Log Forwarding

Disable log forwarding to an external endpoint.

About this task

Procedure

1. List the names of Kubernetes clusters.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster list
```

2. Disable log forwarding. Replace the *cluster-name* with the name of the target cluster.

```
nutanix@pcvm$ /home/nutanix/karbon/karbonctl cluster log-forward disable --cluster-name=cluster-name
```

Network Segmentation

Segregate Nutanix Volumes iSCSI traffic from other traffic.

> **Important:** Before using network segmentation with NKE, enable network segmentation for Nutanix Volumes, see Service-Specific Traffic Isolation in the *Security Guide*.

Configure network segmentation on a cluster by specifying the segmented network as an additional network during cluster creation, see Creating a Cluster on page 29. It is recommended that the additional worker node pools are created with the same segmented network that is configured during the initial deployment.

> **Important:** NKE only supports using network segmentation for container workloads with Nutanix Volumes. See the *isSegmentedIscsiNetwork* parameter in Creating a Storage Class (Nutanix Volumes) in the *CSI Volume Driver Guide*. Configuring network segmentation on a cluster that uses both Nutanix Files and Nutanix Volumes storage provides a dedicated network to Nutanix Volumes traffic only.

12

ADD-ONS

NKE add-ons are open source software extensions that provide additional features to your deployment.

NKE includes the following add-ons:

- A logging add-on powered by Kibana, see Logging on page 71.
- A monitoring add-on powered by Prometheus, see Monitoring on page 73.

Logging

The NKE logging add-on is powered by Kibana. It provides a centralized interface with several features such as:

- View, analyze, and search log events.
- Tail log events in near real-time.
- Filter aggregated logs.
- Highlight search matches.

For Kubernetes 1.19.13 and older versions: the Logtrail plug-in within Kibana is used for logging. For details, refer Using Logtrail Plug-in on page 71.

For Kubernetes 1.19.16 and newer versions: Kibana is used for logging. The newer Kibana versions do not support the Logtrail plug-in. For details, refer Using Kibana on page 72.

Using Logtrail Plug-in

The Kibana data-visualization plug-in is the NKE logging add-on.

The Kibana dashboard has a custom tab for the Logtrail plug-in (not available on Kubernetes version 1.19.16 and above), which displays data for the selected namespaces. By default, Logtrail is configured to display logs for the system namespaces of the Kubernetes cluster: kube-system and ntnx-logging.

Access the add-on through the Kubernetes Management UI, as access to pods is restricted.

> **Note:** Do not delete or modify the supporting namespaces.

Settings

The **Settings** filter displays logs for the selected entity. Kibana displays the host name in orange and the pod name in blue. Click the colored text to filter by pod or host name.

You can select the following logging options from the **Settings** tab:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2322

Table 26: Logging Settings

Setting	Description
kubernetes-* (default)	Displays logs for pods running in the **kube-system** and **ntnx-logging** namespaces.
systemd-*	Displays logs for the kubelet control plane and worker services of every node.
etcd-*	Displays logs from etcd services running on etcd VMs.

All Systems

By default, the **All Systems** tab displays logs from all nodes. You can also use it to filter the display to only show logs for specific nodes.

Using Kibana

Kibana, which supports live logging, is the NKE logging add-on.

About this task

This procedure details the steps to use the NKE logging add-on. As these steps are required for the initial setup of the logging add-on, they need to be carried out only once.

Before you begin

At least one Kubernetes cluster is available.

Procedure

1. Log on to Prism Central.
2. Click the collapsed menu icon on the top-left corner.
3. In the **Services** option, click **Kubernetes**.
   The existing Kubernetes clusters are displayed.
4. Click an existing Kubernetes cluster.
   The **Summary** page opens.
5. Select the **Activity** tab and click **Logging**.
   A table appears which lists the **Logging** add-on and its details.
6. To launch the add-on, click **Logging** or **Launch**. A warning about security certificate appears in your browser. Accept the certificate warning and proceed.
   Elastic welcome page appears.
7. Click **Explore on my own**.
8. Click the collapsed menu icon and then click **Discover** under **Analytics** in the left pane.
   A screen appears prompting to create an index pattern.
9. Click **Create index pattern**.
   A screen appears with the options to define for creating an index pattern.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2323

10. Do the following in the fields in **Create index pattern** screen:

    a. **Name**: Enter a name for the index pattern. The name should match one or more sources listed on the right.

    An asterisk (*) is used to match multiple characters. To match the index pattern name with all the sources, enter only an asterisk (*).

    b. **Timestamp field**: Select a time stamp from the dropdown options.

11. Click **Create index pattern**.
    The newly created index pattern is saved.

12. Click the collapsed menu icon and then click **Discover** under **Analytics** in the left pane.
    The logging information is displayed in charts.

Monitoring

The built-in Prometheus add-on provides monitoring for Kubernetes clusters. Prometheus scans clusters for health and consumption, provides data for metrics, and triggers alerts and notifications that appear in the Kubernetes Management Console.

Prometheus feeds data to the **Alerts** tab in the Kubernetes Management user interface (UI).

> **Note:** Do not delete or modify the supporting namespaces.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2324

13

ONBOARD AND VIEW KUBERNETES CLUSTERS IN PRISM CENTRAL

Onboard the Kubernetes Clusters to Prism Central

To view the Kubernetes clusters in the **Kubernetes Clusters** dashboard in Prism Central, onboard the Kubernetes clusters to Prism Central.

For information on onboarding and viewing the Kubernetes clusters in Prism Central, see Kubernetes Clusters Management in the *Prism Central Infrastructure Guide*.

v2.2 | June 2025 | NVD-2115

NUTANIX VALIDATED DESIGN

Nutanix GPT-in-a-Box with Nutanix Kubernetes® Platform Design

NUTANIX

Legal

© 2025 Nutanix, Inc. All rights reserved. Nutanix, the Nutanix logo and all Nutanix product and service names mentioned are registered trademarks or trademarks of Nutanix, Inc. in the United States and other countries. Kubernetes is a registered trademark of The Linux Foundation in the United States and other countries. All other brand names mentioned are for identification purposes only and may be the trademarks of their respective holder(s).

Certain information contained in this content may link or refer to, or be based on, studies, publications, surveys, and other data obtained from third-party sources and our own internal estimates and research. While we believe these third-party studies, publications, surveys, and other data are reliable as of the date of publication, they have not independently verified unless specifically stated, and we make no representation as to the adequacy, fairness, accuracy, or completeness of any information obtained from a third-party. Our decision to publish, link to or reference third-party data should not be considered an endorsement of any such content.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

Contents

1. Executive Summary.....4
Software Versions.....8

2. Core Infrastructure Design.....9
Core Infrastructure Conceptual Design.....12
Scalability.....12
Resilience.....13
Nutanix Cluster Design.....14
Storage Design.....16
Network Design.....18
Nutanix Files and Nutanix Objects Design.....21
Nutanix Database Services Design.....24
Management Components.....25
Monitoring.....27
Security and Compliance.....31
Datacenter Infrastructure.....34

3. Application Cluster Designs.....37
Kubernetes Conceptual Design.....37
Large Language Model Reference Application Design.....44

4. Backup and Disaster Recovery.....50

5. Ordering.....51
Substitutions.....51
Sizing Considerations.....52
Bill of Materials.....52

6. References.....56

About Nutanix.....57

List of Figures.....58

1. Executive Summary

Nutanix continues to innovate and engineer solutions that are simple to deploy and operate. To further improve customer experience and add value for customers, Nutanix uses robust validation to simplify the process of designing and deploying solutions. This document describes the design that supports the deployment of an innovative, flexible, and secure generative pretrained transformer (GPT) solution for artificial intelligence (AI) to privately run and manage your choice of AI large language models (LLMs) and workloads on the Nutanix Cloud Platform across private and public clouds and the enterprise edge.

Nutanix can deliver this Nutanix Validated Design (NVD) as a bundled solution for scoping, designing, installing, and testing generative AI (GenAI) and machine learning (ML) solutions. This NVD provides a bill of materials that includes hardware, software, and services to accelerate and simplify the deployment and implementation process.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2329

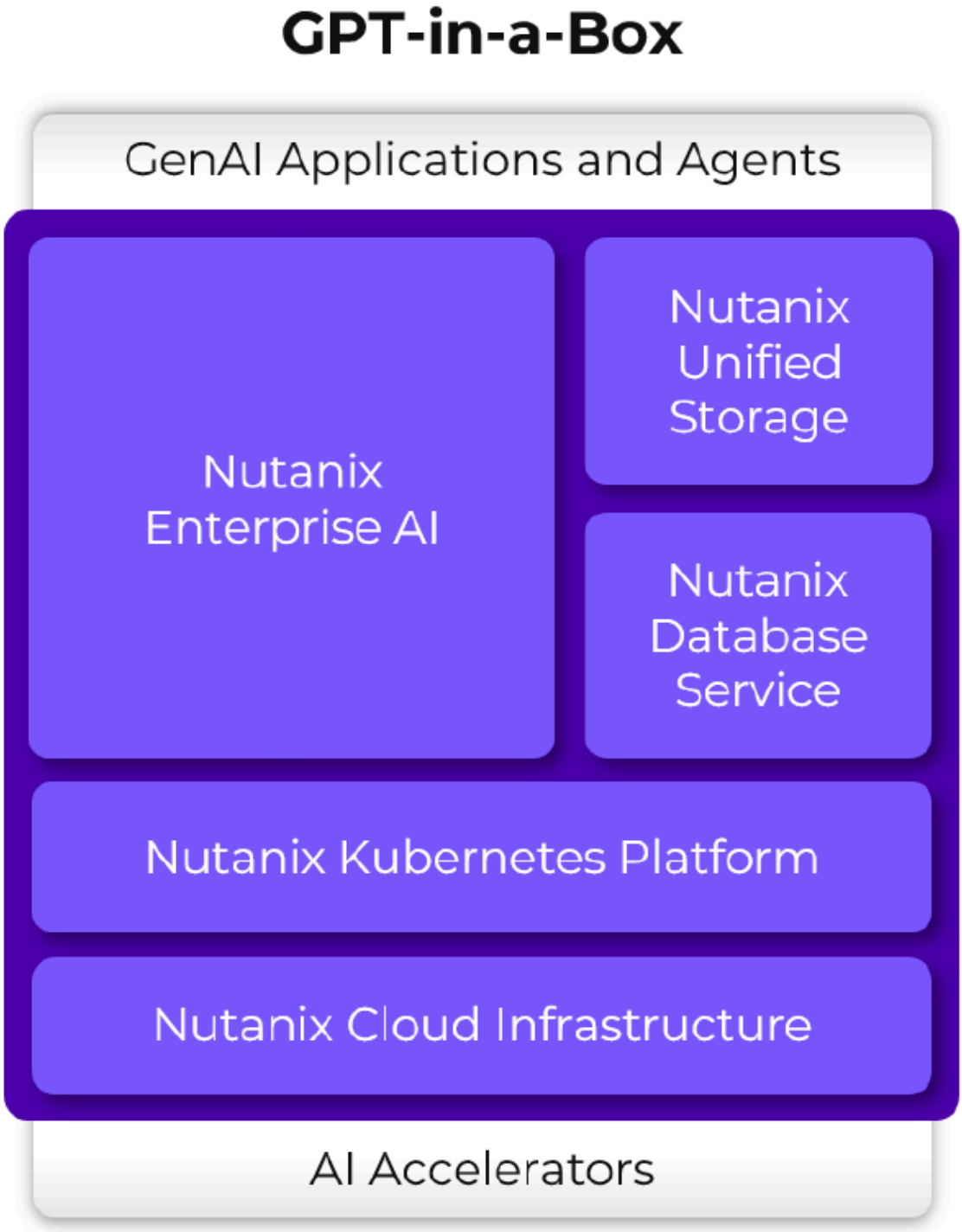


Figure 1: Architectural Layers of the Nutanix Validated Design for GPT-in-a-Box 2.0

© 2025 Nutanix, Inc. All rights reserved

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2330

Some highlights of the GPT-in-a-Box NVD include the following:

- A single-cloud operating model using Nutanix Cloud Platform hyperconverged infrastructure with graphic processing units (GPUs)
- Nutanix Unified Storage for total data management, security, privacy, and resilience
- An enterprise-grade inference endpoint from Nutanix Enterprise AI that provides an easy way to deploy your choice of LLMs from leading providers and create and manage secure APIs to connect your GenAI applications
- An enterprise-grade Kubernetes solution Nutanix Kubernetes Platform (NKP) that simplifies the processes for deploying, scaling, and managing containerized applications across hybrid and multicloud environments
- A Professional Services engagement that includes a planning workshop and a full-stack design workshop dedicated to your environment
- A full-stack focus with integrated data privacy installed using opinionated software

This NVD also incorporates Nutanix Database Service (NDB) to manage stateful PostgreSQL workloads through the NDB Operator for Kubernetes. NDB provisions two independent PostgreSQL database workflows: one for the Nutanix Enterprise AI (NAI) back end and another for user applications that require pgvector for semantic search and retrieval-augmented generation (RAG) pipelines.

This validated design is just one example of a supported GPT configuration. You can design and build a GPT solution on Nutanix in many ways, and you can deviate from this specific configuration while still following Nutanix best practices.

You can have this validated solution up and running in weeks with minimal burden on your internal teams, so that you can realize the full value of your infrastructure quickly. After you place your order, Nutanix takes care of the rest.

This guide is part of the Nutanix Solutions Library and is intended for architects and engineers responsible for scoping, designing, installing, and testing generative AI and ML solutions. You should already be familiar with the Nutanix Hybrid Cloud Reference Architecture and Nutanix products.

This document describes the components, integration, and configuration for the NVD packaged GPT-in-a-Box solution and covers the following topics:

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2331

- Core Nutanix infrastructure and related technology
- Management plane
- Nutanix Unified Storage
- Kubernetes cluster design
- Reference architecture for LLM applications
- Bill of materials

Table: Document Version History

Version Number	Published	Notes
1.0	May 2024	Original publication.
1.1	June 2024	Updated the Rack Layout image, the Scalability Design Decisions, GPT-in-a-Box Cluster: Hardware, and GPT-in-a-Box Cluster: Per-Node Hardware Configuration tables, and the Core Infrastructure Design, Scalability, and Rack Design sections.
1.2	September 2024	Updated the Ordering section.
2.0	January 2025	Significant updates throughout for GPT-in-a-Box 2.0, NKP, AMX support for embedding, and NX-9151-G9.
2.1	March 2025	Added the Nutanix Enterprise AI version, Lenovo GPU sizing, and GPT-in-a-Box Cluster: Professional Services SKUs table.
2.2	June 2025	Added NDB to the design. Updated NKP to Version 2.14.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2332

Software Versions

Table: Software Versions Used in Validation Testing

Component	Software Version
Prism Central	2024.3.0.1
Nutanix AOS	7.0
Nutanix AHV	10.0
Nutanix Foundation	5.7
Nutanix Life Cycle Manager (LCM)	3.1
Nutanix Cluster Check (NCC)	5.1
NVIDIA	nvidia_aie_10.0.0.1-11_535.216.01
Nutanix Kubernetes Platform (NKP)	2.14
Nutanix Enterprise AI	2.0
Nutanix Files	5.1
Nutanix Objects	5.1
Nutanix Database Services	2.8.0
Nutanix Database Service Operator for Kubernetes	0.5.1

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2333

2. Core Infrastructure Design

The following lists provide core infrastructure design requirements, assumptions, risks, and constraints.

Core infrastructure design requirements by component:

- Management:
  - Provide a unified management and control plane to VMs and Kubernetes runtimes.
  - Configure the management plane to integrate with Active Directory for authentication.
  - Use Active Directory–based groups for access control.
  - Provide automated infrastructure and application deployment.
  - Provision PostgreSQL databases for application back ends and vector search.
  - Provide Kubernetes-based automated database provisioning and life cycle management of PostgreSQL instances.
- Business continuity and disaster recovery (BCDR): Ensure persistent inference availability.
- Performance:
  - Support GPU passthrough for VMs and Kubernetes workloads.
  - Provide high-bandwidth, low-latency shared storage for the AI application's data.
- Environment: Optimize hardware and software to provide maximum performance.
- Scale: Support a single Nutanix GPT-in-a-Box cluster that can scale up to 16 nodes with a minimum of eight GPUs in the cluster.
- Resilience: Provide enough GPU resources to run GPU-enabled workloads in a failure scenario.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2334

- Hardware:
  - Provide hardware with GPU support using NVIDIA L40S.
  - Use hardware that supports up to four GPU cards per node.
  - Use servers with 100 Gbps network uplinks.
  - Use NVMe disks for optimal performance.
- Monitoring:
  - Monitor performance metrics and store historical data for the past 12 months.
  - Monitor resources that are critical to Nutanix AOS operations (for example, CPU, memory, storage, and network resources); resource usage that exceeds configured limits generates an alert.
  - For resources that have high availability reservations, measure the resource utilization threshold against the usable capacity after subtracting the capacity reserved for high availability.
  - Use email as the primary channel for event monitoring alerts.
  - Ensure that event monitoring is resilient.

    For example, when the management plane is the primary source of alerts, use a secondary method to monitor the management plane itself. If the management plane fails, an alert from the secondary source can trigger the action to recover the management plane.
  - Use consolidated monitoring for all deployed NKP clusters.
- Security and compliance:
  - Use role-based access control (RBAC) to follow the least-privilege rule.
  - Support network microsegmentation.
- Networking: Use Link Aggregation Control Protocol (LACP) to optimize networking traffic.

Core infrastructure design assumptions by component:

- Networking: Top-of-rack switches provide a 100 Gbps connection.

© 2025 Nutanix, Inc. All rights reserved

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2335

- Monitoring:
  - IT operations teams can continuously staff the mailbox that receives monitoring alerts to address critical issues in a timely manner.
  - IT operations teams can provide email infrastructure with sufficient resilience to send, receive, and access emails even during critical outages.
- Infrastructure: You have existing infrastructure components like Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), and Active Directory available.
- BCDR:
  - A single Nutanix cluster hosts the infrastructure.
  - Replication isn't configured.
  - Velero explicitly backs up stateful workloads in the Kubernetes cluster occasionally with the BackupStorageLocation pointing to a bucket in Nutanix Objects to save the backups external to the NKP cluster. In the event of a failure, you can restore the workload from the backup by pointing to the same backup location.
  - Nutanix Objects buckets are replicated to external destinations.

Core infrastructure design risks by component:

- Availability: A cluster-wide outage (power outage, PDU failure, availability zone (AZ) failure, software stack failure) causes services to be unavailable.
- Monitoring:
  - If Prism Central becomes unavailable for any reason, the platform can no longer send alerts. To mitigate this risk, configure each Prism Element instance to send alerts as well. As this approach results in duplicate alerts during normal operations, send Prism Element alerts to a different mailbox that you can monitor when Prism Central is unavailable.
  - If the Kubernetes management cluster becomes unavailable, the platform can no longer send Kubernetes-related alerts or record Kubernetes performance metrics.

Core infrastructure design constraints by component:

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2336

- Scalability:
  - The number of inference endpoints and models is limited to the number of GPUs available in a single node.
  - The maximum number of nodes in the GPT clusters is 16, and the maximum number of GPUs depends on the hardware you choose.
- Budget: Budget is limited.
- Hardware: The solution uses NVIDIA GPUs.
- Application: AI applications can't use vGPU.

Core Infrastructure Conceptual Design

The conceptual pod design has the following features:

- Single AZs in a single region in an on-premises datacenter
- A single Nutanix cluster that hosts the following services, among others:
  - Nutanix management components, including Prism Central
  - Nutanix Unified Storage to provide Network File System (NFS) storage and S3-compatible storage capabilities
  - NKP workload clusters used for Nutanix Enterprise AI and GenAI workload-stack
  - NKP management cluster used for deployments and observability

---

Scalability

Scalability is one of the core concepts of the Nutanix platform and refers to the ability to increase storage and compute capacity to meet both current and future workload demands. A well-designed cluster meets current requirements while providing a path to support future growth.

Scalability Conceptual Design

This NVD permits horizontal and vertical scaling within the boundaries of maximum cluster size. For more information on Nutanix scalability concepts, see the Hybrid

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2337

Cloud: AOS 6.5 with AHV On-Premises Design and the Enterprise Edge with Artificial Intelligence: AOS 6.5 with AHV Design.

This NVD supports a single GPT-in-a-Box cluster with a defined GPU capacity of eight GPU cards using a standardized node's hardware configuration. This approach provides maximum flexibility and ease of management. If the GPU, memory, or CPU pressure increases, add more nodes to the cluster. If storage demand grows, add more drives to the existing nodes or add more nodes to the cluster. This design uses all-flash storage to accommodate peak workload demands.

When using the Nutanix NX-Platform, you can scale compute and storage by adding NX-8155-G9 nodes. You can scale GPU resources independently by adding additional NX-9151-G9 nodes.

Table: Scalability Design Decisions

Design Option	Validated Selection
Node memory population	Ensure that node memory is evenly distributed.
Node drive type	Use all-flash NVMe drives.
Drive bays	Partially populate the drive bays.
Rack availability	Don't use rack availability.
Available cluster sizes	Use a single GPT-in-a-Box cluster with a starting size of four nodes on Lenovo or HPE or six nodes on NX (four HCI nodes and two GPU nodes).

Resilience

Nutanix provides many resilience features, including storage replication, snapshots, block awareness, degraded node detection, and self-healing. These capabilities increase the resilience of all workloads, even if the application itself has limited resilience options. Nutanix layers these software features on hardware designed with resilience in mind (for example, with redundant physical components and power supplies, many of which are hot-swappable or otherwise easily serviceable). Running workloads in a virtualized environment adds another kind of resilience, because you can perform many maintenance operations without application downtime. A resilient network fabric that can

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2338

sustain individual link, node, or block failures without significant impact completes the architecture.

Resilience Conceptual Design

Many components are physically redundant. The physical components include the top-of-rack switches, the nodes and their internal parts, and the datacenter itself in case of a disaster.

For more information on how to protect workloads and meet or exceed service-level agreements (SLAs), see the Hybrid Cloud: AOS 6.5 with AHV On-Premises Design and Enterprise Edge with Artificial Intelligence: AOS 6.5 with AHV Design.

Table: Resilience Design Decisions

Design Option	Validated Selection
Full redundancy of all components	Ensure the full redundancy of all components in the datacenter.
Storage replication factor	Use storage replication factor 2.
Compute fault tolerance	Use fault tolerance of 1 (n + 1).
Availability zone	Use a single availability zone with no replication.

Nutanix Cluster Design

The design incorporates a single GPU-enabled Nutanix cluster dedicated to GPT-in-a-Box workloads that offers access to LLMs. Supporting management applications like Prism Central and file and object storage are hosted on this cluster.

Size the Nutanix GPT-in-a-Box cluster Controller VM (CVM) with 16 vCPUs and 64 GB of memory.

Use the following cluster naming convention: **<cluster_type><cluster_instance_number><hypervisor><cluster_suffix_number>**. For example, **gpt01ahv01** is the name of the first GPT cluster on AHV.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2339

Cluster Conceptual Design

This NVD uses one region with a single AZ that hosts the GPT-in-a-Box cluster. This NVD doesn't use any replication targets to protect the workloads because the focus is to host the GPT workloads in a single cluster.

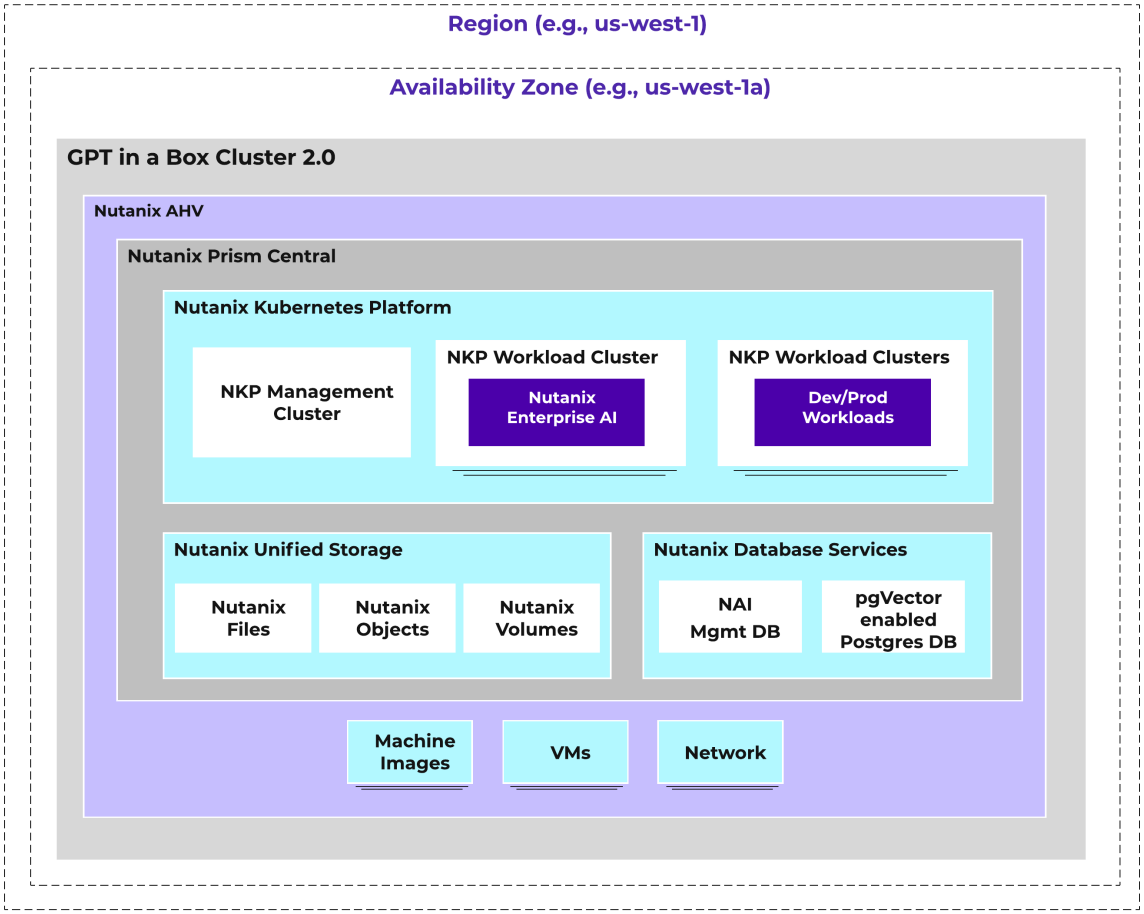


Figure 2: GPT-in-a-Box Nutanix Cluster Conceptual Architecture

Table: Cluster Design Decisions

Design Option	Validated Selection
Cluster size	Ensure the full redundancy of all components in the datacenter.
CPU	Use at least 24 cores and a high clock rate.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2340

Design Option	Validated Selection
Minimum cluster size	Use at least four nodes.
Cluster expansion	Expand in increments of 1.
Maximum cluster size	Use at most 16 nodes.
Networking	Use 100 GbE networking.
Cluster replication factor	Use storage replication factor 2.
Cluster high availability configuration	Guarantee high availability.
VM high availability	Enable high availability reservation on the clusters.

For platform details, see the Bill of Materials section of this document.

Cluster Resilience

VM high availability ensures that VMs restart on another AHV host in the AHV cluster when a host becomes unavailable, either because the original AHV host has a complete failure or becomes network partitioned or because of an AHV host management process failure. When the AHV host where a VM is running becomes unavailable, the VM turns off; therefore, from the perspective of the VM operating system, VM high availability involves a full VM start cycle.

Table: High Availability Configuration

Feature	Description	Setting
High availability reservation	Guarantee compute failover capacity within cluster for application	Enabled
Rebuild capacity reservation	Guarantee storage rebuild capacity within cluster	Enabled

Storage Design

Nutanix uses a distributed, shared-nothing architecture for storage. For information on node types, counts, and physical configurations, see the Cluster Design section in this document.

Creating a cluster automatically creates the following storage containers:

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2341

- NutanixManagementShare: Used for Nutanix features like Nutanix Files and Nutanix Objects and other internal storage needs; doesn't store workload vDisks
- SelfServiceContainer: Used by the NCM Self-Service Portal to provision VMs
- Default-Container-XXXX: Used by VMs to store vDisks for user VMs and applications

In addition to the automatically created storage containers, the following additional storage containers are created during the Nutanix Files and Nutanix Objects deployment:

- NTNX_<fileserver_name>_ctr: Provides storage for the file server instances, which provide NFS storage for the application tier
- objectsd<uniqueidentifier>: Data container for Nutanix Objects
- objectsm<uniqueidentifier>: Metadata container for Nutanix Objects

The Default-Container stores VMs and their vDisks. The additional containers for Nutanix Files and Objects are created throughout the deployment process of the respective components.

Data Reduction and Resilience Options

To increase the effective capacity of the cluster, the design enables inline compression on all storage containers. It doesn't use additional functionalities such as deduplication or erasure coding. Replication factor 2 protects against the loss of a single component in case of failure or maintenance.

Table: Data Reduction Settings

Container	Compression	Deduplication	Erasure Coding	Replication Factor
Default-Container-XXXX	On	Off	Off	2
Nutanix ManagementShare	On	Off	Off	2
SelfService Container	On	Off	Off	2
NTNX_files_ctr	On (60 min.)	Off	Off	2
Objects containers	On	Off	Off	2

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2342

The following table provides information about the storage decisions made for this design.

Table: Storage Design Decisions

Design Option	Validated Selection
Sizing a cluster	Use an all-flash cluster to provide low-latency, high-throughput storage to support the application's active data set.
Node type vendors	Don't mix node types from different vendors in the same cluster.
Node and disk types	Use similar node types that have similar disks. Don't mix nodes that contain NVMe SSDs in the same cluster with hybrid SSD or HDD nodes.
Sizing for node redundancy for storage and compute	Size all clusters for n + 1 failover capacity.
Fault tolerance and replication factor settings	Configure the cluster for fault tolerance 1 and configure the container for replication factor 2.
Inline compression	Enable inline compression.
Deduplication	Don't enable deduplication.
Erasure coding	Don't enable erasure coding.
Availability domain for cluster	Use node awareness.
Storage containers in cluster	The cluster has the following storage containers: NutanixManagementShare, SelfServiceContainer, Default-Container, NTNX_files_ctr, and the two objects storage containers.
Reserve rebuild capacity	Enable reserve rebuild capacity.

Network Design

A Nutanix cluster can tolerate multiple simultaneous failures because it maintains a set redundancy factor and offers features such as block awareness and rack awareness. However, this level of resilience requires a highly available network connecting a cluster's nodes.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2343

Nutanix clusters send each write to another node in the cluster. As a result, a fully populated cluster sends storage replication traffic in a full mesh, using network bandwidth between all Nutanix nodes. Because storage write latency directly correlates to the network latency between Nutanix nodes, any increase in network latency adds to storage write latency. Protecting the cluster's read and write storage capabilities requires highly available connectivity between nodes. Even with intelligent data placement, if network connectivity between multiple nodes is interrupted or becomes unstable, VMs on the cluster can experience write failures and enter read-only mode.

Use datacenter-grade switches designed to handle high-bandwidth server and storage traffic at low latency. This NVD uses a leaf-spine network topology, which requires at least two spine switches and two leaf switches, and LACP at the switch end. Every leaf connects to every spine using 100 GbE uplink ports and connects to every node using a 100 GbE virtual switch. For more information, see Physical Networking Best Practices.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2344

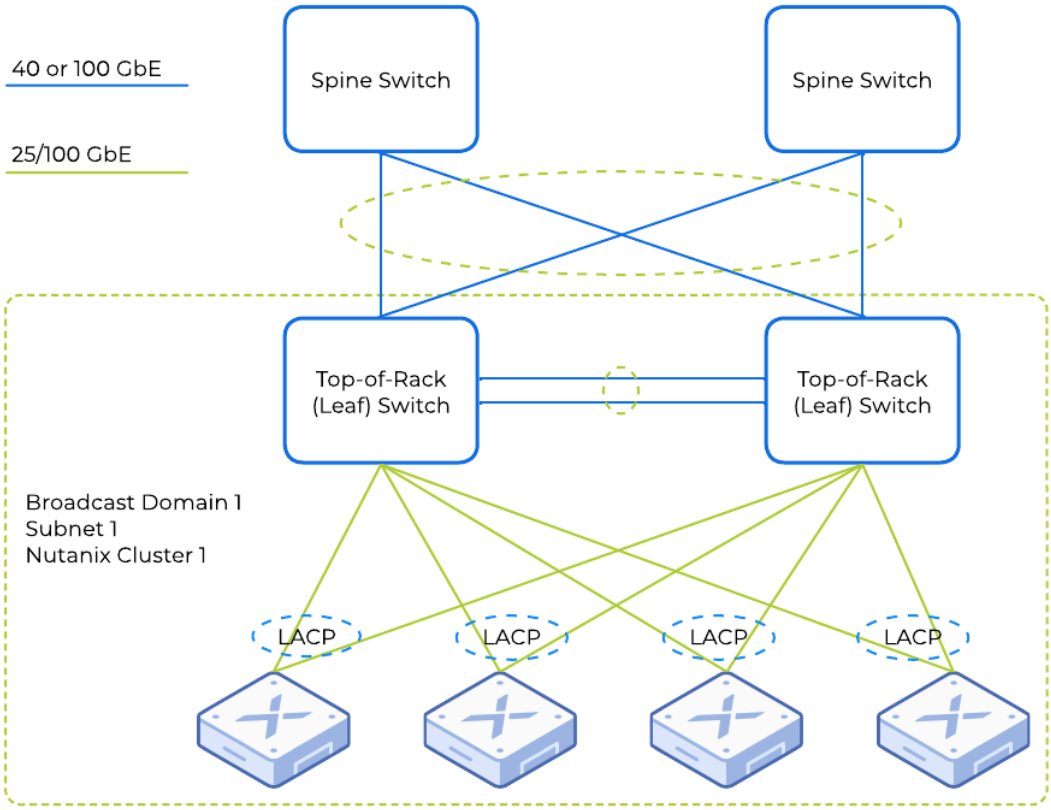


Figure 3: GPT-in-a-Box Physical Network Architecture

For more information on deploying a network to achieve the necessary resilience levels, see the Hybrid Cloud: AOS 6.5 with AHV On-Premises Design and the Enterprise Edge with Artificial Intelligence: AOS 6.5 with AHV Design.

Table: Network Design Decisions

Design Option	Validated Selection
Datacenter switch	Use large-buffer nonblocking switches.
Network topology	Use the highly available leaf-spine network topology.
Top-of-rack switches	Populate each rack with 2 × 100 GbE top-of-rack switches.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2345

Design Option	Validated Selection
CVM and hypervisor VLAN	Configure the CVM and hypervisor VLAN as native, or untagged, on server-facing switch ports.
Switch ports for guest workloads	Use tagged VLANs on the switch ports for all guest workloads.
Virtual switches	Use one vs0 virtual switch with two of the fastest uplinks of the same speed.
Logical network separation	Use VLANs to separate logical networks.
Number of required VLANs and subnets	The design requires four VLANs and subnets: one for CVM and hypervisor management, one for Integrated Lights-Out out-of-band management, one for the management network, and one for the client front-end network.

Nutanix Files and Nutanix Objects Design

For this NVD, Nutanix Files provides high-performance, shared storage to NKP using Nutanix CSI. Nutanix Enterprise AI stores the LLMs in ReadWriteMany (RWX) PersistentVolumeClaims (PVCs) to make them available to multiple endpoints. Use an additional NFS share to provide custom models that you can import into Nutanix Enterprise AI.

Nutanix Objects provides S3-compatible storage capabilities to the application and also enables you to upload new data models for import into Nutanix Enterprise AI.

Nutanix Files and Objects run on the same Nutanix cluster as the GPT-in-a-Box workloads. If you plan to expand the environment, you can also run Nutanix Files and Nutanix Objects in a dedicated cluster.

Use Prism Central to manage all the components.

Nutanix Files, Nutanix Objects, and Nutanix Kubernetes Platform Network Design

Nutanix Files and Nutanix Objects have the following network requirements:

- For maximum performance, the storage network for Nutanix Files uses the same subnet as the CVMs.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2346

- To maximize security, the client network connects to a separate subnet.
- The GPT-in-a-Box cluster that provides a single file server instance requires four storage network IP addresses and three client network IP addresses for its three file server VMs (FSVMs).

Nutanix Objects runs as a containerized service on a Kubernetes microservices platform, which provides benefits such as increased velocity of new features. Several of the required storage IP addresses are for functions related to the underlying microservices platform. You must also manage these networks. Nutanix Objects with three worker nodes requires seven storage network IP addresses and two client network IP addresses.

Each cluster provisioned by NKP has minimum IP address requirements. A Kubernetes cluster in a production-level layout with three worker nodes requires one static IP address for the control plane, six or more IPAM addresses for VMs, and a range of four or more IP addresses for the Kubernetes LoadBalancer Services.

The client network provides all IP addresses. You might need additional IPAM addresses for additional worker nodes.

Nutanix Files and Nutanix Objects Design Decisions

The following table provides information about the Nutanix Files and Nutanix Objects decisions made for this design.

Table: Nutanix Files Design Decisions

Design Option	Validated Selection
FSVM cluster size	Use three FSVMs.
vCPU and memory for FSVM	Use 12 vCPUs and 64 GB of memory for each FSVM.
Storage networking	Keep the storage network in the same subnet as the CVMs and AHV.
Client networking	Use a separate subnet to provide client access to storage.
Fault tolerance and replication factor settings	Configure the cluster for fault tolerance 1 and configure the container for replication factor 2.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2347

Design Option	Validated Selection
Storage containers	Use a separate storage container to host Nutanix Unified Storage files.
Erasure coding	Don't enable erasure coding.
Compression	Enable compression.
Deduplication	Don't enable deduplication.
Protocols for shares	Use NFS for shares.
Nutanix CSI	Use dynamic provisioning.

Table: Nutanix Objects Design Decisions

Design Option	Validated Selection
Nutanix Objects cluster size	Use three worker nodes and two load balancer nodes.
Worker node size	Use 10 vCPUs and 32 GB of memory for each worker node.
Load balancer node size	Use 2 vCPUs and 4 GB of memory for each load balancer node.
Storage networking	Keep the storage network in the same subnet as the CVMs and AHV.
Client networking	Use a separate subnet to provide client access to storage.
Fault tolerance and replication factor settings	Configure the cluster for fault tolerance 1, and configure the container for replication factor 2.
Storage containers	Use a separate storage container to host Nutanix Unified Storage Objects.
Erasure coding	Don't enable erasure coding.
Compression	Enable compression.
Deduplication	Don't enable deduplication.
Buckets to create	Create two buckets: user_upload (for end-user access), and backup (backup target).

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2348

Nutanix Database Services Design

NDB provides automated provisioning, scaling, patching, and management of databases on Nutanix infrastructure. This validated design includes NDB to provision and manage PostgreSQL databases used by GenAI workloads.

NDB provisions two independent workflows:

NAI back-end database

A transactional PostgreSQL database backing the NAI services

Vector store with pgvector

A PostgreSQL instance with pgvector extension enabled, acting as a vector store for user applications using semantic search or retrieval-augmented generation (RAG)

The NDB Operator for Kubernetes integrated with NKP workload clusters provisions and manages these databases. Database life cycle management (provisioning, patching, backup) is declarative, consistent with GitOps practices used for other NKP-managed workloads.

Metrics for the provisioned PostgreSQL instances are available through Prometheus as part of the logging stack observability in NKP. Metrics include CPU and memory usage, connection count, query duration, and IOPS.

Table: Nutanix Database Service Design Decisions

Design Option	Validated Selection
NDB version	2.8.0
Number of cores for NDB instance	16
NDB instance size	32 GB
Database deployment method	NDB Operator for Kubernetes
Database engine	PostgreSQL
Vector store extension	pgvector
Number of PostgreSQL instances	2 (NAI back end, pgvector store)
Resource separation	Each database provisioned into dedicated database VMs

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2349

Design Option	Validated Selection
Backup	Managed through NDB backup policy
Monitoring	Integrated with NKP observability stack

Management Components

Management components such as Prism Central, Active Directory, DNS, and NTP are critical services that must be highly available. Prism Central is the global control plane for Nutanix, responsible for VM management, application orchestration, microsegmentation, and other monitoring and analytics functions. You can deploy Prism Central in a single-VM or scale-out (three-VM) configuration. This NVD doesn't use all of these management features.

Management Conceptual Design

In this NVD, the management components run on the same physical cluster as the applications.

Infrastructure

The infrastructure management plane for this validated design is Prism Central, which manages and controls the following components:

- Nutanix Files and Nutanix Objects
- VMs
- RBAC
- Monitoring, observability, and auditing for the core infrastructure

Kubernetes

NKP provides its own independent management plane for Kubernetes workloads that includes the following:

- Workload cluster deployment and management using workspace profiles
- Application catalog
- Application deployment using workspace profiles and projects

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2350

Nutanix Enterprise AI

You can perform the following actions from the administrator interface in the Nutanix Enterprise AI workload cluster:

- Manage LLM.
- Manage inference endpoints.
- Manage RBAC.

DNS Management

Name resolution and SSL certificate management are critical to deploying and managing Kubernetes clusters. In this NVD, Microsoft DNS manages the DNS root domain. Subdomains map the DNS and route the traffic to the Kubernetes clusters. The core infrastructure components use DNS forwards to redirect the traffic for a particular subdomain to the local domain controller.

You can substitute your own DNS solution but you might need to make changes to certificate management.

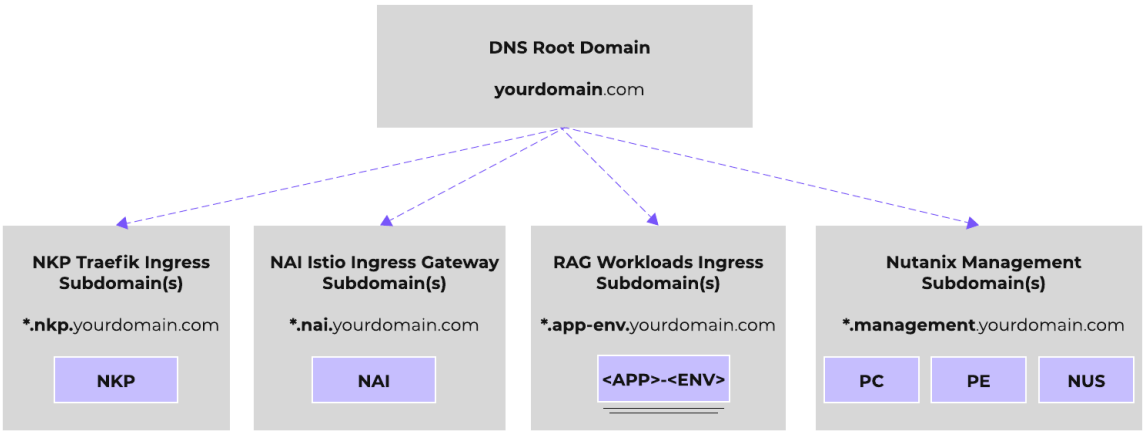


Figure 4: DNS Management

Management Detailed Design

In this NVD, the cluster runs Nutanix AOS with AHV hosting Prism Central. Prism Central is deployed in a scaled-out architecture (three-node cluster) to provide the desired uptime and performance for the management plane.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2351

The following table lists the design decisions for the Nutanix management components.

Table: Management Component Design Decisions

Design Option	Validated Selection
Cluster placement	Deploy the management components on the same cluster as the applications.
Prism Central deployment	Deploy scaled-out Prism Central (three VMs).
Prism Central deployment size	Use a small deployment size of three VMs, each with six vCPUs, 26 GB of memory, and 800 GiB of storage.
Prism Central container name	Use the default container name.
Active Directory authentication	Use Active Directory authentication.
Connection to Active Directory	Use SSL or TLS for Active Directory.
Certificates	Replace self-signed certificates with certificate authority–signed certificates.

Monitoring

Monitoring in the NVD falls into two categories: event monitoring and performance monitoring. Each category addresses different needs and issues.

In a highly available environment, you must monitor events to maintain high service levels. When faults occur, the system must raise alerts on time so that administrators can take remediation actions as soon as possible. This NVD configures the Nutanix platform's built-in ability to generate alerts in case of failure.

In addition to keeping the platform healthy, maintaining a healthy level of resource usage is also essential to the delivery of a high-performing environment. Performance monitoring continuously captures and stores metrics that are essential when you need to troubleshoot application performance. A comprehensive monitoring approach tracks the following areas:

- Application and database metrics
- Operating system metrics
- Hyperconverged platform metrics

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2352

- Network environment metrics
- Physical environment metrics

By tracking a variety of metrics in these areas, the Nutanix platform can also provide capacity monitoring across the stack. Most enterprise environments inevitably grow, so you need to understand resource usage and the rate of expansion to anticipate changing capacity demands and avoid any business impact caused by a lack of resources.

Monitoring Conceptual Design

In this NVD, Prism Central performs event monitoring for the Nutanix core infrastructure. This NVD uses syslog for log collection; for more information, see the Security and Compliance section. SMTP-based email alerts serve as the channel for notifications in this design. To cover situations where Prism Central might be unavailable, each Nutanix cluster in this NVD sends out notifications using SMTP as well. The individual Nutanix clusters send alerts to a different receiving mailbox that's only monitored when Prism Central isn't available.

Prism Element transmits the data to Prism Central using an API. Prism Central then transmits the log to Nutanix Pulse (using the Secure Sockets Layer) and the syslog server using the User Datagram Protocol (UDP). All components (Prism Central, Nutanix Unified Storage, and NKP) send the alerts to the monitoring system using SMTP.

For more information on monitoring in NKP, see the Kubernetes Conceptual Design section in this document.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2353

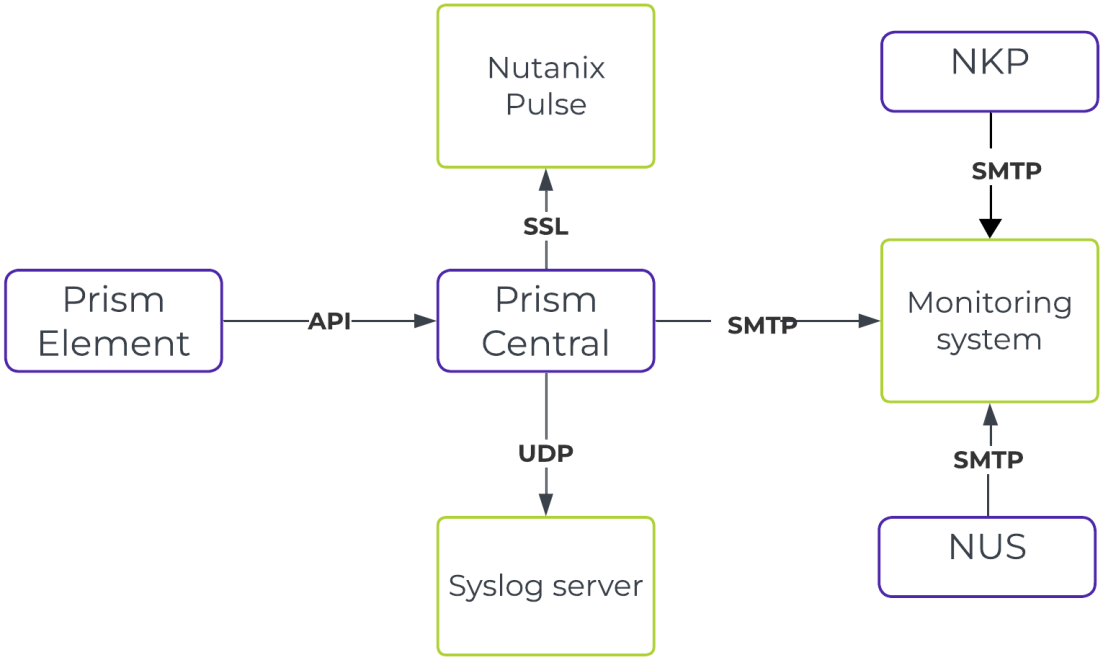


Figure 5: GPT-in-a-Box Monitoring Conceptual Design

Prism Central monitors cluster performance in key areas such as CPU, memory, network, and storage usage and captures these metrics by default. When a Prism Central instance manages a cluster, Prism Central transmits all Nutanix Pulse data, so it doesn't originate from individual clusters. When you enable Nutanix Pulse, it detects known issues affecting cluster stability and automatically opens support cases.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2354

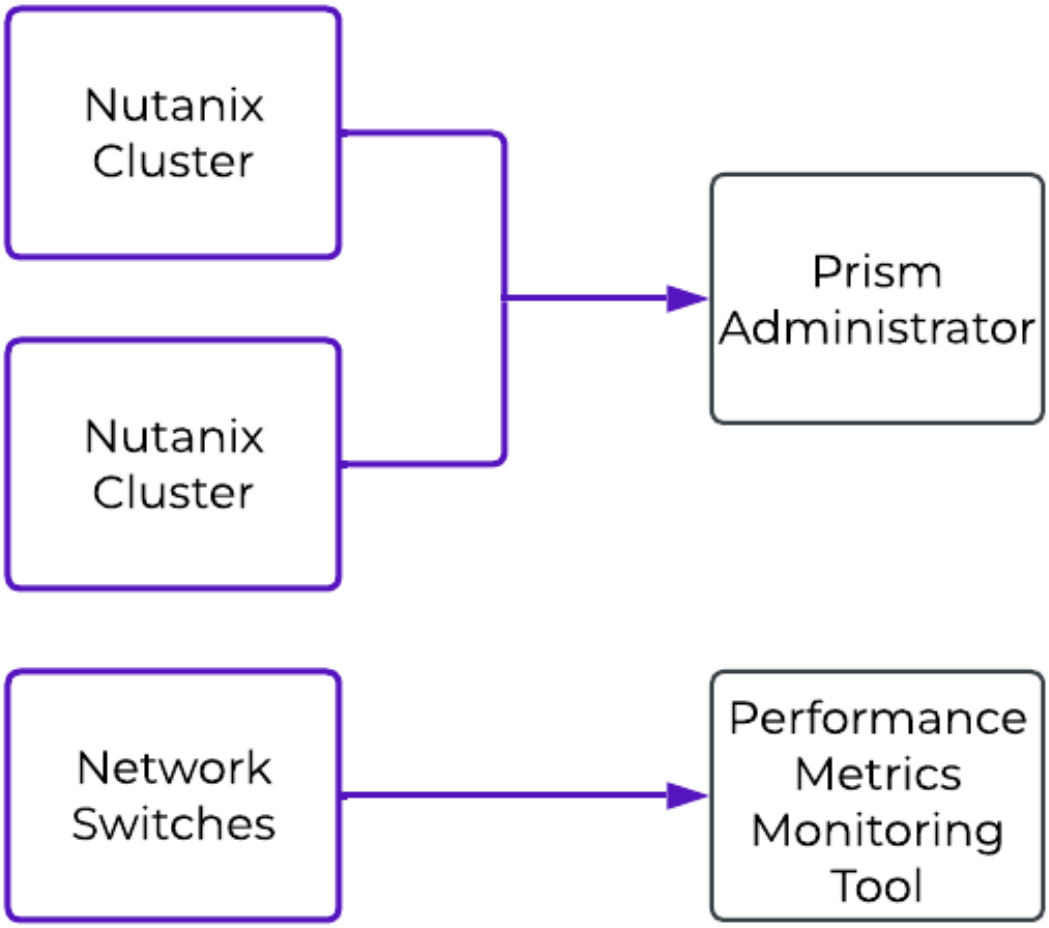


Figure 6: Hybrid Cloud Performance Metrics Systems

The network switches that connect the cluster also play an important role in cluster performance. A separate monitoring tool that's compatible with the deployed switches can capture switch performance metrics. For example, an SNMP-based tool can regularly poll counters from the switches.

The following table provides descriptions of the monitoring design decisions.

Table: Monitoring Design Decisions

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2355

Design Option	Validated Selection
Platform performance monitoring	Prism Central monitors Nutanix platform performance.
Network switch performance monitoring	A separate tool that performs SNMP polling to the switches monitors network switch performance.
SMTP alerting	Use SMTP alerting; use an enterprise SMTP service as the primary SMTP gateway for Prism Element and Prism Central.
SMTP alerting source email address	Configure the source email address to be **clustername@<yourdomain>.com** to uniquely identify the source of email messages. For Prism Central, use the Prism Central host name in place of cluster name.
SMTP alerting Prism Central recipient email address	Configure the Prism Central recipient email address to be **primaryalerts@<yourdomain>.com**.
SMTP alerting Prism Element recipient email address	Configure the Prism Element recipient email address to be **secondaryalerts@<yourdomain>.com**.
NCC reports	Configure daily NCC reports to run at 6:00 AM local time and send them by email to the primary alerting mailbox.
Nutanix Pulse	Configure Nutanix Pulse to monitor the Nutanix cluster and send telemetry data to Nutanix.

Application-specific monitoring is described in the Kubernetes Monitoring section.

Security and Compliance

Nutanix recommends a defense-in-depth strategy for layering security throughout any enterprise datacenter solution. This design section focuses on validating the layers that Nutanix can directly oversee at the control and data-plane levels. For more information, see the Security and Compliance section of the Nutanix for Enterprise Edge Computing reference architecture.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2356

Security Domains

Isolate Nutanix cluster management and out-of-band interfaces from the rest of the network using firewalls, and only allow direct access to them from the management security domain. In addition, Nutanix recommends separating out-of-band management and cluster management interfaces onto a dedicated VLAN away from the application traffic.

Authentication and Authorization

All Nutanix control plane endpoints use Active Directory–hosted LDAP over SSL (LDAPS). Active Directory itself is highly available and redundant in the existing customer landscape. Only administrative accounts are mapped to admin roles, which are controlled through a named Active Directory group.

This NVD rotates all default passwords for all accounts that aren't integrated with Active Directory, such as emergency accounts or local accounts for out-of-band interfaces. Because clusters don't have lockdown mode enabled, password SSH is enabled by default.

AOS Hardening

This NVD enables additional non-default hardening options in each AOS cluster:

- Advanced Intrusion Detection Environment (AIDE)
- Hourly security configuration management automation (SCMA)

Both features are trivial to enable, introduce little to no discernible system overhead, and help detect and prevent internal system configuration changes that could otherwise compromise service availability. These features add to the intrinsic hardening built into AOS.

Syslog

For each control plane endpoint (Prism Central), system-level internal logging goes to a centralized third-party syslog server that runs in the existing customer landscape. The system is configured to send logs for all available modules when they reach the syslog Error severity level.

This NVD assumes that the centralized syslog servers are highly available and redundant, so you can inspect the log files in case the primary log system is unavailable.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2357

Certificates

SSL endpoints serve all Nutanix control plane web pages. This NVD replaces the default self-signed certificates with certificates signed by an internal certificate authority in your environment. Any client endpoints that interact with the control plane must have the trusted certificate authority chain preloaded to prevent browser security errors.

> **Note:** Certificate management is an ongoing activity, and you must rotate certificates periodically. This NVD signs all certificates for one year of validity.

Table: Security Design Decisions

Design Option	Validated Selection
Data-at-rest encryption (DaRE)	Don't use DaRE.
SSL endpoints	Sign control plane SSL endpoints with an internal trusted certificate authority.
Certificates	Provision certificates with a yearly expiration date and rotate accordingly.
Authentication	Use Active Directory LDAPS authentication.
Control plane endpoint administration	Use a common administrative Active Directory group for all control plane endpoints.
Cluster lockdown mode	Don't enable cluster lockdown mode (allow password-driven SSH).
Non-default hardening options	Enable AIDE and hourly SCMA.
System-level internal logging	Enable error-level logging to an external syslog server for all available modules.
Syslog delivery	Use UDP transport for syslog delivery.

Table: Security Configuration References

Configuration Target	Key:Value
Active Directory	AD-admin-group:ntnx-ctrl-admins
Syslog Server	infra-az[1..2]-syslog:6514 (udp)

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2358

Datacenter Infrastructure

This design assumes that the datacenter in the hosting region sustains a single AZ. To ensure high availability at the physical cluster level, this NVD addresses the connection between the hardware running Nutanix software and the datacenter's power and networking components.

Rack Design

This NVD recommends dedicating one rack to the GPT-in-a-Box workload. Rack 1 has the following requirements:

- Two top-of-rack switches
- One management switch
- GPT-in-a-Box cluster (four 2 RU HCI nodes based on the bill of materials; for Nutanix NX, add two 2 RU GPU compute-only nodes)

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2359

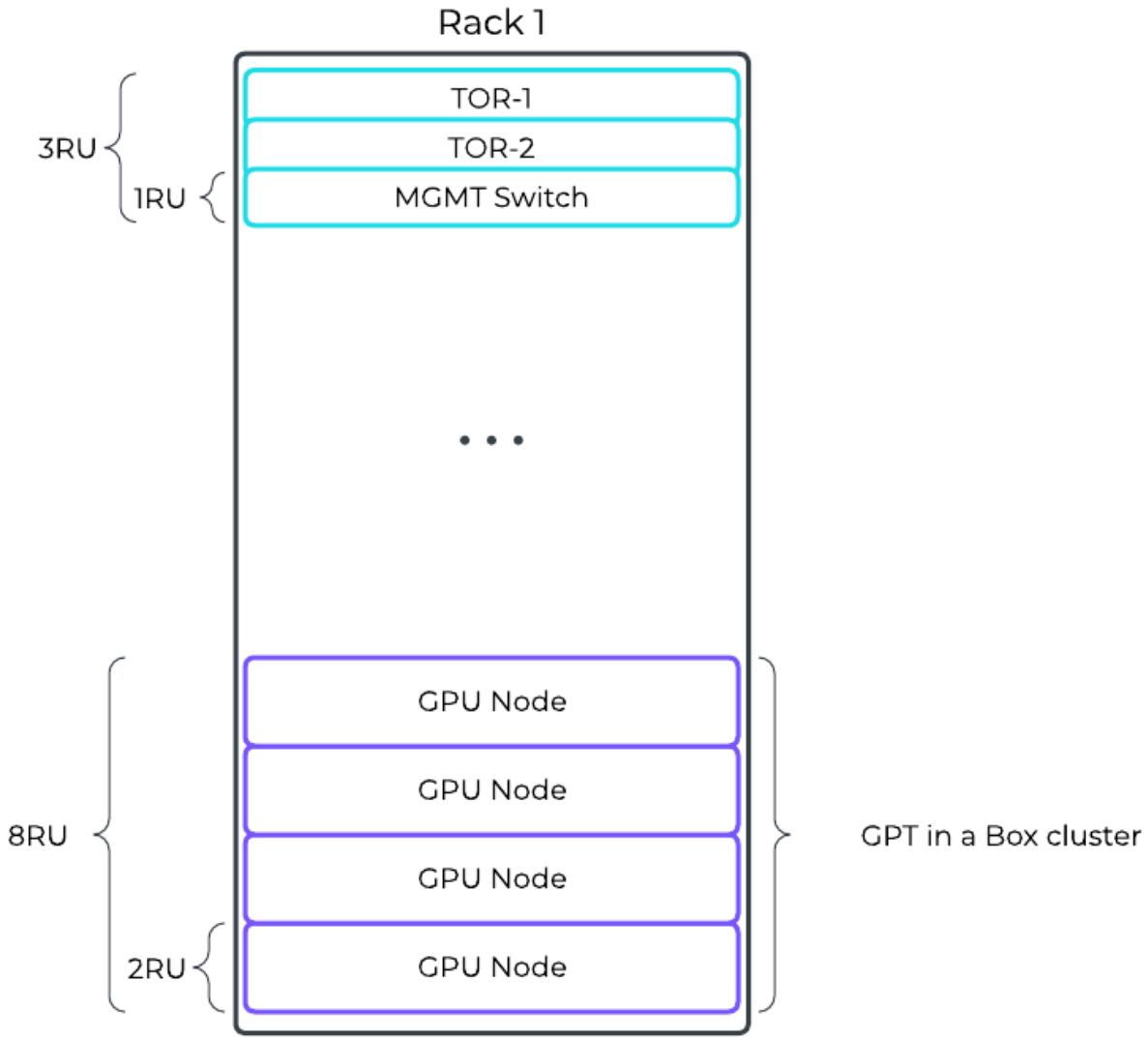


Figure 7: Rack Layout

In this design's physical rack space, one generic 42 RU rack contains 8 RU of systems with 3 RU reserved for two data switches and one out-of-band switch.

The four nodes consume four network ports on each of the two data switches. In addition, each node has a dedicated out-of-band management network interface, consuming four ports on the management switch.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2360

When scaling the environment, consider physical rack space (including floor weight capacity), network port availability, and the datacenter's power and cooling capacity.

© 2025 Nutanix, Inc. All rights reserved |

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2361

3. Application Cluster Designs

The following sections describe the designs for the Kubernetes and LLM clusters.

Kubernetes Conceptual Design

This conceptual design outlines a robust, highly available Kubernetes environment on the Nutanix platform, using NKP and integrating with essential Kubernetes tools (many of which come with NKP) and practices for efficient and secure operations.

You must purchase the NKP Ultimate license for your GPT-in-a-Box cluster because it requires the following features:

- Application catalogs and GitOps with built-in Flux CD to push workloads to multiple clusters
- Workspaces and projects to provide isolation (in terms of access)
- Cluster profile definition (in terms of applications deployed to the cluster)
- Segregation (in terms of cluster-wide and namespace-specific workloads)

In this design, we use a single NKP Ultimate management cluster to manage workloads and configurations and push them to multiple workload clusters. The NKP management cluster is used for management only. Nutanix Enterprise AI and its supporting components run on one NKP workload cluster with GPU node pools. GenAI apps and supporting components run on another workload clusters. The data resides locally in these clusters or in an S3 bucket (Nutanix Objects) or NFS share (Nutanix Files).

All production Kubernetes clusters are set up as production-level clusters using multiple control plane and worker nodes distributed across different physical hosts to ensure high availability.

When you build an NKP cluster, the process automatically deploys the following preconfigured cloud-native tools for NKP's internal use:

- Certificate management: Cert-Manager

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2362

- Ingress controller: Traefik
- Authentication: Dex
- Continuous delivery: Flux CD
- Kubernetes dashboard
- Policy admission webhook: Gatekeeper
- Cost management: Kubecost

Note: Although these tools are for internal use, workloads running on the cluster can also use them.

This NVD uses the following design decisions for NKP workspace and projects:

- Workspaces: Because the solution's two cluster categories (Nutanix Enterprise AI clusters and GenAI clusters) require different resources (Nutanix Enterprise AI requires GPU and GenAI doesn't), run different workloads, and are likely managed by different teams, create two workspaces (Nutanix Enterprise AI and GenAI).
- Projects: To allow multiple application teams to share clusters, create a project for each GenAI application in the GenAI workspace. This process also creates a namespace in the associated clusters.

    The continuous delivery mechanism makes it easy to deploy apps across all clusters associated with the project.

The following NKP workspace applications are often explicitly enabled from the NKP application catalog in both workspaces:

- Logging: Logging Operator, Grafana Logging, Grafana Loki, Fluent Bit
- Monitoring: Prometheus Monitoring, Prometheus Adpater
- Backup and recovery: Velero with Nutanix Objects as the S3-compatible object store used for storage
- Object storage: Rook Ceph, Rook Ceph Cluster

The following NKP workspace applications are explicitly enabled only on the Nutanix Entperise AI workspace:

- Istio Service Mesh

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2363

- NVIDIA GPU Operator
- Knative
- Nutanix Enterprise AI

> **Note:** To enable Nutanix Enterprise AI, add the `https://github.com/nutanix-cloud-native/nkp-nutanix-product-catalog` repo to the Nutanix Enterprise AI workspace as a Flux CD GitRepository resource in the management cluster.

The NDB Operator for Kubernetes is currently not part of the NKP catalog and must be installed separately in both workspaces. Define manifests for each PostgreSQL instance (NAI back end, vectorstore); enable the pgvector extension through an additional Kubernetes job after you deploy the underlying database.

Create the GenAI app project in the GenAI workspace and use its continuous delivery mechanism to deploy the GenAI app. The clusters in the GenAI workspace are explicitly attached to this project. You can add more projects to this workspace to allow more than one app team to share clusters in the GenAI workspace.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2364

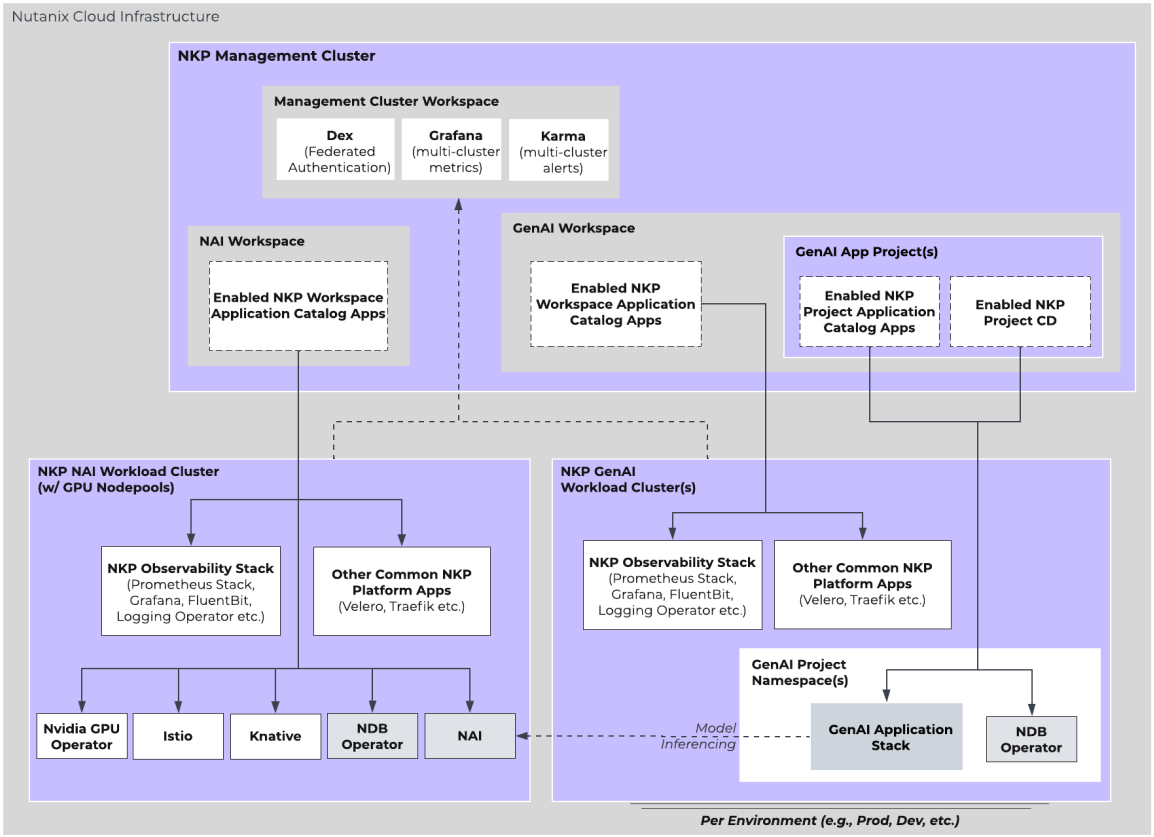


Figure 8: Nutanix GPT-in-a-Box Kubernetes Conceptual Design

Table: GPT-in-a-Box Cluster with NKP Scalability Design Decisions

Design Option	Validated Selection
NKP cluster type	Use the NKP Ultimate license.
Control plane size	Size the control plane with 4 CPUs, 16 GB of memory, and 80 GB of storage.
Initial workload size	Start with four worker nodes with 8 CPUs, 32 GB of memory, and 100 GB of storage.
GPU pool size (Nutanix Enterprise AI cluster only)	Use two worker nodes with 12 CPUs, 40 GB of memory, and 100 GB of storage.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2365

The workloads are divided into NKP management, GPT-in-a-Box Nutanix Enterprise AI, and production or development environments. The single NKP management cluster is named `<custom-prefix>-nkp-mgmt`, Nutanix Enterprise AI runs on a dedicated cluster in the Nutanix Enterprise AI workspace named `<custom-prefix>-nai`, and the workload clusters use the following naming convention: `<custom-prefix>-<cluster_type>-<environment_id>-wl-<app_id>-<optional_app_index_number>`.

NKP cluster names use a maximum of 63 characters and have the same restriction as any Kubernetes resource (the cluster name must be a valid DNS-1035 label), which means that cluster names can only contain lowercase alphanumeric characters and hyphens and must start and end with an alphanumeric character.

You can scale the NKP management and workload cluster worker nodes to accommodate different workload sizes. Nutanix recommends scaling out. The total number of workers in the GPU node pools is constrained by the number of physically installed GPUs.

All GPUs are licensed to run Nutanix Enterprise AI, but this design keeps some spare GPU dev and experimental workloads:

- NKP management cluster: acme-nkp-mgmt
- GPT-in-a-Box Nutanix Enterprise AI environment: acme-nai (two GPU nodes with two L40S each)
- Prod environment: acme-gpt-p-wl-genai-01
- Dev environment:
  - acme-gpt-d-wl-nai (two GPU nodes with one L40S each)
  - acme-gpt-d-wl-genai-01
  - acme-gpt-d-wl-genai-02
  - acme-gpt-d-wl-genai-03
  - acme-gpt-d-wl-genai-04

You can use other layouts based on your development requirements.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2366

Kubernetes Resilience

NKP clusters are production-level clusters that provide a resilient control plane by running multiple nodes for the control plane and etcd. To ensure high availability, Kubernetes deployments use multiple replica pods and implement pod antiaffinity rules. This approach helps maintain service availability, even in the event of a worker node update or failure.

Kubernetes services and ingress controllers perform the essential service of load balancing by evenly distributing network traffic across all available pods, enhancing service reliability and system performance.

Kubernetes Networking

NKP uses the following for network and communication:

- Cilium as the Container Network Interface
- Kube-VIP for network connectivity to load balance the Kubernetes API server
- MetalLB for network connectivity to load balance the Kubernetes LoadBalancer Services
- Traefik as the default ingress controller for NKP's dashboards and other internal tools
- Istio Mesh as the ingress for the Nutanix Enterprise AI
- Cert-Manager to automate the management and issuance of TLS certificates

Each deployed cluster uses a base configuration for networking.

Kubernetes Monitoring

NKP comes with a fully integrated observability stack out of the box. The logging stack is turned off by default; you must enable it explicitly.

The monitoring stack uses the following:

- Prometheus to collect metrics and generate alerts

  It uses Prometheus Operator, which allows you to modify the configuration using custom resource definitions such as PrometheusRules and ServiceMonitors.

- Prometheus Adapter to serve Kubernetes metric API

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2367

- AlertManager for alerting
- Grafana to visualize metrics with a rich set of precreated custom dashboards

For centralized monitoring, the NKP management cluster also runs Thanos for metric aggregation from all attached clusters. A centralized Grafana instance hosts dashboards to convert these metrics to meaningful information. Similarly, Karma provides a multicluster dashboard for alerts.

The logging stack uses the following:

- Fluentbit to collect host, host_kernel, and audit logs
- Logging-Operator to collect and forward container logs
- Loki to index and store logs

  By default, logs are stored in a locally deployed rook-ceph object store.
- Grafana Logging to visualize logs and the audit dashboard

All clusters run their local logging and monitoring stack. A Thanos instance running on the management cluster aggregates metrics from all Prometheus instances across NKP clusters. The management cluster runs an instance of Karma that pulls alerts from workload clusters and shows them in its dashboard.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2368

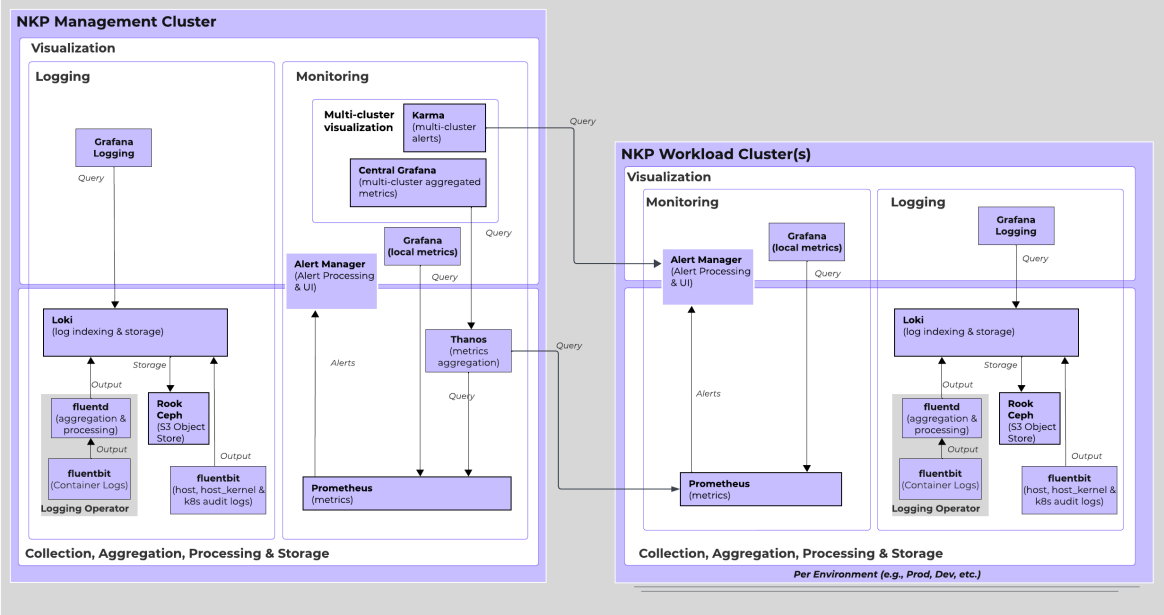


Figure 9: Kubernetes Monitoring Conceptual Design

Kubernetes Backup

The default storage class installed by NKP during deployment provides persistent storage for the management and workload clusters. The persistent volumes and application data in the all clusters can be protected by a Velero backup schedule and stored in a S3 bucket provided by Nutanix Objects (or optionally a local object store provided by a rook-ceph that runs locally on the NKP cluster). A bucket in the local Nutanix Object store can be configured as the Backup Storage Location and replicated to an external location.

> **Note:** Because NKP application catalogs or GitOps Flux CD manages application deployment, only back up stateful workloads.

NDB time machine snapshots protect the content of the vector store provided by NDB.

Large Language Model Reference Application Design

Fine-tuning an LLM on specific documents and using RAG pipelines are two distinct approaches to enhancing language models. Fine-tuning involves directly adjusting the model's parameters based on a specific set of documents. This process customizes the

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2369

model to better reflect the style, terminology, and content of the input material, making it more effective at generating or interpreting text consistent with the training data.

In contrast, a RAG pipeline doesn't alter the underlying model; instead, it augments the LLM’s capabilities by integrating a retrieval component. This component dynamically fetches relevant information from external sources (such as a database or a set of documents) in real time during the generation process. The LLM uses this retrieved information to inform its responses, making it more accurate and contextually rich without changing the model's fundamental structure.

Fine-tuning can sometimes lead to overfitting, where the model becomes overly specialized to the training data and might not perform well on general or varied inputs. In contrast, RAG preserves the generalization capabilities of the original LLM while enhancing its outputs with information retrieved dynamically from external sources. This approach is particularly important for applications where the reliability and predictiveness of the base model are crucial.

Fine-tuning an LLM can be resource-intensive, requiring substantial computational resources and data for retraining. In contrast, RAG uses the existing model by integrating external data dynamically during the inference stage, which is generally less demanding in terms of computational resources.

For these reasons, this NVD uses a RAG pipeline instead of fine-tuning. A RAG pipeline is particularly useful for applications that require up-to-date information or handle vast, ever-changing data sets.

Large Language Model Conceptual Design

This design introduces a robust architecture to support GenAI applications using a wide range of open-source LLM models. The Nutanix Enterprise AI platform can host these models as OpenAI-compatible LLM inferencing endpoints, providing flexibility and compatibility for diverse use cases.

While the Nutanix Enterprise AI platform operates on any Kubernetes infrastructure, this specific design uses NKP as the container orchestration platform to streamline operations and enhance efficiency. The design offers a comprehensive, scalable, and efficient framework tailored specifically for building RAG pipeline applications.

By incorporating the latest LLM technologies and supporting tools, this framework ensures ease of development, seamless deployment, and effective monitoring. It

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2370

provides a reliable and adaptable solution for modern AI workflows. Using Intel AMX–enabled CPUs and optimized OpenVINO libraries speeds up document embedding by a factor of 2.

Large Language Model Logical Design

LLM inference endpoints, provided through the Nutanix Enterprise AI platform, form the foundation of this architecture. These essential components plays a critical role in deploying and managing machine learning models, particularly for addressing real-time inference requirements. The integration with the Nutanix GPT-in-a-Box 2.0 design guarantees scalability, reliable accessibility, and consistent performance.

With this modular architecture, you can independently scale and update each component, providing flexibility for system optimization. Its compatibility with the RAG framework allows the LLM to query and retrieve data from the vector database, significantly improving the accuracy and relevance of generated outputs.

The data ingestion process supports both batch processing and event-driven workflows through Kafka. With this dual approach, the system can seamlessly handle large-scale periodic batch uploads and continuous real-time data streams. Serverless functions built on Knative and triggered by Nutanix Objects event notifications relayed through Kafka process events. The embedding function automatically discovers Intel AMX features to optimize data processing. This architecture ensures efficient, scalable, and highly responsive handling of incoming data streams.

After the embedding function vectorizes the data using the LangChain toolset, it stores the vectors in a pgVector-enabled Postgres database, managed by NDB, to provide the robust back-end storage necessary to meet its large-scale data demands.

During the inference process, integration with the RAG pipeline architecture allows the LLMs running on Nutanix Enterprise AI to dynamically query and retrieve relevant information from the vector database, significantly improving the accuracy and relevance of generated outputs. This approach enhances the system's ability to provide accurate, domain-specific answers by reducing reliance on the LLM's internal knowledge, which might be insufficient. Instead, the RAG workflow ensures that responses are informed by up-to-date and highly relevant data, improving both accuracy and contextual relevance for user queries.

In this architecture, Nutanix Enterprise AI uses NKP’s observability stack to enable seamless monitoring and logging for LLM workloads and GPU performance. After you

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2371

deploy the NVIDIA GPU Operator from the NKP catalog, it automatically configures NVIDIA Data Center GPU Manager metrics for Prometheus, along with default Grafana dashboards that detail GPU utilization, memory bandwidth, and thermal performance. Thanos aggregates metrics and Grafana visualizes them, while Fluentbit and Loki handle log collection and indexing, resulting in an advanced monitoring solution that goes beyond conventional GPU observability.

Large Language Model Research Workflow

The LLM uses the following research workflow:

1. Ask a question: The interaction begins when the user poses a question through the UI or chatbot interface.
2. Create a query embedding: The embedding model transforms the user's query into a vector representation.

   This process is known as vectorization.
3. Search and retrieve similar context: The vector database, which is specifically designed for similarity searches, stores the document embeddings generated by the model. It can efficiently search for and retrieve items based on these embeddings, which encapsulate the semantic meaning of the texts.
4. Send the prompt: The workflow augments the user's query with relevant contextual information retrieved from the database, then sends this enriched query as a prompt to the LLM endpoint running on Nutanix Enterprise AI. The LLM processes the enriched query and generates a response.
5. Get an answer: The UI or chatbot interface presents the LLM's response as the answer to the user's query.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2372

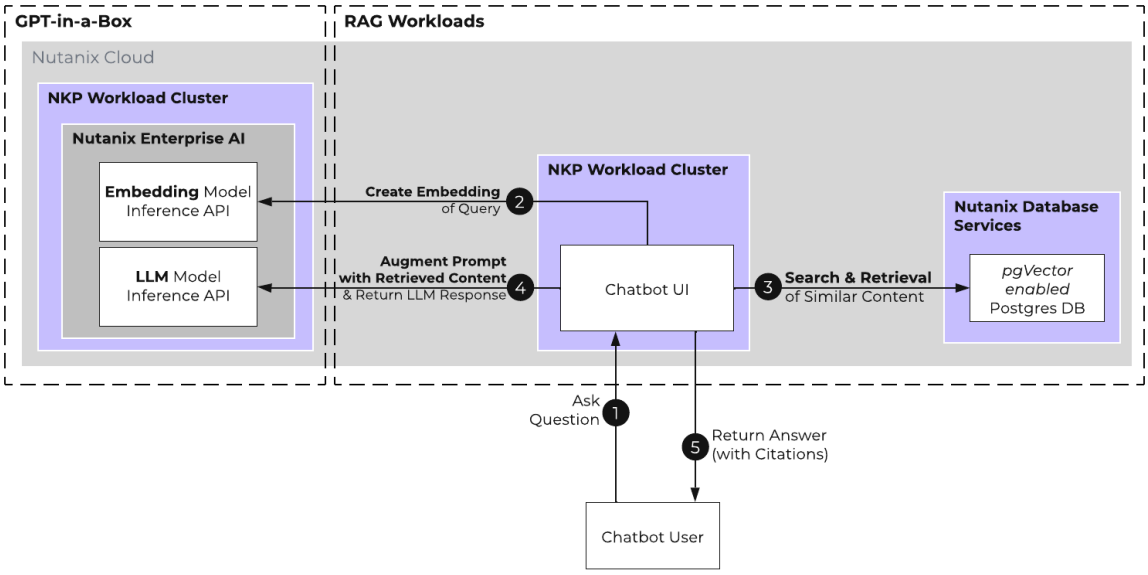


Figure 10: LLM Research Workflow

Document Ingestion Workflow

The design uses the following workflow for document ingestion:

1. Uploading the document: Each time a new document is added to the bucket, an event notification is sent through Kafka.
2. Processing the Kafka event: The notification triggers the document ingestion service to generate a new embedding for that specific document.
3. Ingesting the batch: The document ingest function downloads the document.
4. Embedding the document: Embedding involves splitting the document into smaller segments and using an embedding model to create a vector representation of each segment.
5. Storing the embeddings: The generated vectors are stored in a vector database for future retrieval and searches.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2373

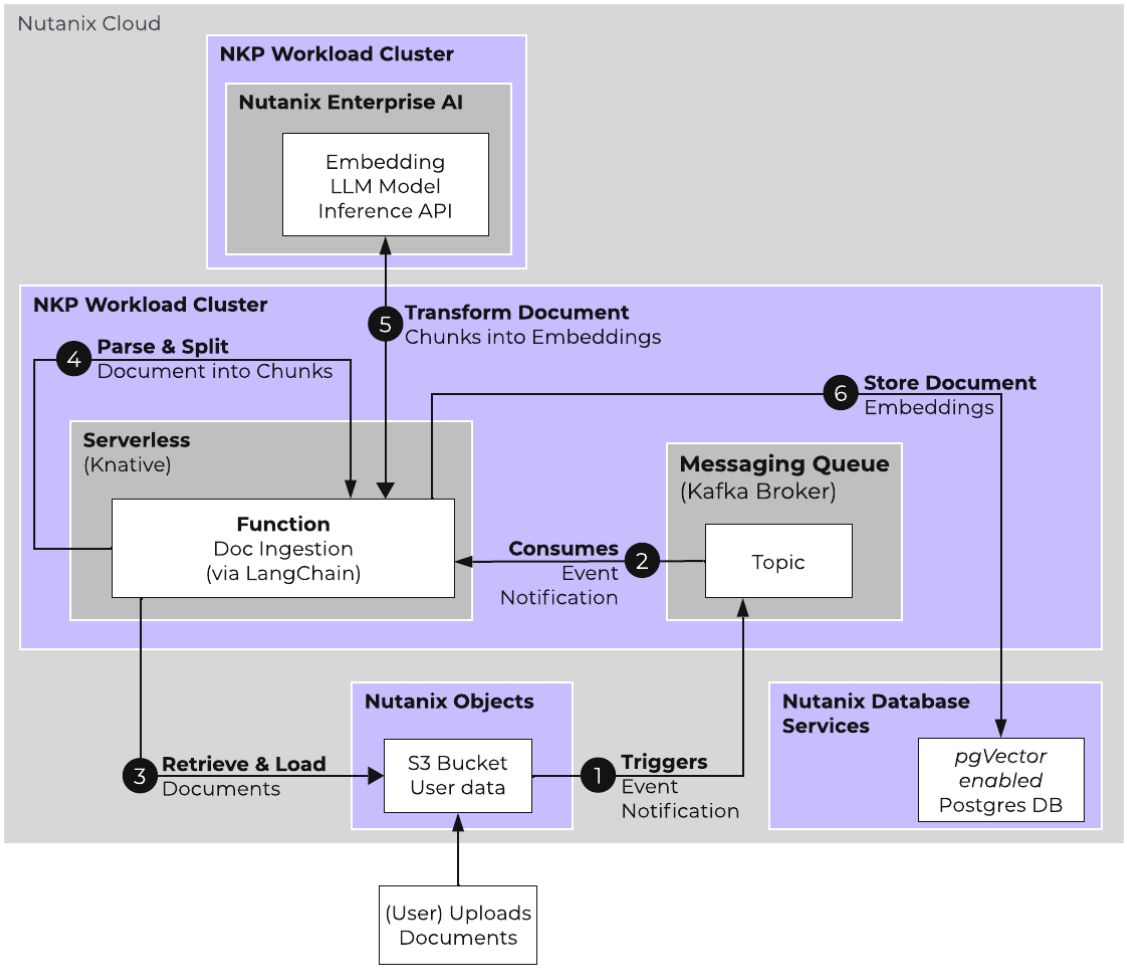


Figure 11: Document Ingestion Workflow

© 2025 Nutanix, Inc. All rights reserved

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2374

4. Backup and Disaster Recovery

Because the scope for this NVD is a single standalone GPT-in-a-Box cluster, you must back up the application data on the S3 buckets in the Nutanix Objects store to an external environment. You don't need to back up Kubernetes application resources deployed by the NKP application catalog or GitOps because Flux CD handles the deployment and stores the configuration data in an external Git repository. However, if these applications use any stateful data, you must back that up. NKP provides Velero as a tool to back up Kubernetes resources and stateful data.

You can use the streaming replication mechanism built into Nutanix Objects to replicate the data at the bucket level to a different S3 object store outside the GPT-in-a-Box cluster. You can also use the existing backup solution to back up the persistent application data and store it outside the GPT-in-a-Box cluster.

For more information on protecting workloads and meeting or exceeding SLAs, see the Hybrid Cloud: AOS 6.5 with AHV On-Premises Design and Enterprise Edge with Artificial Intelligence: AOS 6.5 with AHV Design.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2375

5. Ordering

This bill of materials reflects the validated and tested hardware and services that Nutanix recommends to achieve the outcomes described in this document. Consider the following points when you build your orders:

- All software is based on core licensing whenever possible.
- Nutanix Professional Services or an affiliated partner selected by Nutanix provides all services.

Note: Because available hardware, software, and services can change without notice, contact Nutanix Sales when ordering to ensure that you have the correct product codes.

Substitutions

Nutanix recommends purchasing the exact hardware configuration reflected in the bill of materials whenever possible. If a specific hardware configuration is unavailable, choose a similar option that meets or exceeds the recommended specification. To allow the greatest possible flexibility, you can choose between Intel and AMD.

- You can make hardware substitutions to suit your preferences; however, such changes might result in a solution that doesn't follow the recommended Nutanix configuration.
- Avoid software product code substitutions except when:
  - You need different quantities to maintain software licensing compliance.
  - You prefer a higher license tier or support level for the same software product code.
- Adding any software or workloads not specified in this design (including additional Nutanix products) might affect the validated density calculations and result in a solution that doesn't follow the recommended Nutanix configuration.
- Nutanix Professional Services substitutions to accommodate customer preferences aren't possible.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2376

Sizing Considerations

This NVD describes the design for a single GPT-in-a-Box cluster with four or more nodes. If one of the scaling factors (such as the total number of VMs, Kubernetes applications, or GPU workloads) exceeds the maximum specified for the solution, extend the cluster with the required capacity (CPU, memory, storage, GPU). After reaching the maximum cluster size, consider building a new cluster to support the demand for further growth.

Bill of Materials

The following sections show the bill of materials for the Nutanix GPT-in-a-Box cluster.

GPT-in-a-Box Cluster

Table: GPT-in-a-Box Cluster: Hardware

Item	Specification
Platform (HCI, Intel-based)	Lenovo HX650V3, HPE DX380a, or Nutanix NX-8155-G9
Platform (Compute-only, Intel-based)	Nutanix NX-9151-G9
Platform (HCI, AMD-based)	Lenovo HX665V3 or HPE DX385
Configuration	1-node
Type	All-flash NVMe
Support level	Production
NRDK support	No
NR node support	No

Note: We used the Lenovo HX665V3, HPE DX380a, and NX-8155-G9 and NX-9151-G9 models for validation.

Table: GPT-in-a-Box Cluster: Per-Node Hardware Configuration HPE or Lenovo

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2377

Component	Description	Quantity
Processor	Intel Xeon-Gold 6442Y (2.6 GHz, 24 cores) or AMD EPYC 9254 (2.9 GHz, 24 cores)	2
Memory	64 GB, 4,800 MHz DDR5 RDIMM	24
SSD	3.2 TB NVMe	6
Network adapter	100 GbE, 2-port Mellanox ConnectX-6 (QSFP56)	1
Network adapter	10 or 25 GbE, 2-port Mellanox ConnectX-6 (SFP28)	1
GPU (Lenovo)	NVIDIA L40S 48 GB PCIe	3
GPU (HPE)	NVIDIA L40S 48 GB PCIe	2

Note: We validated HPE with two GPUs, but you can order up to four GPUs. We validated Lenovo with three GPUs; you must use a minimum of two GPUs.

Table: GPT-in-a-Box Cluster: Per-Node Hardware Configuration Nutanix NX-8155-G9

Component	Description	Quantity
Processor	Intel Xeon-Gold 6442Y (2.6 GHz, 24 cores)	2
Memory	32 GB, 5,600 MHz DDR5 RDIMM	32
SSD	3.84 TB NVMe	6
Network adapter	Mellanox 100, 40, or 25 GbE, 2-port NIC (CX6 100 GbE)	2
Network adapter	SMC 10 GbE, 2-port Base-T, 2-port SFP+ NIC (X710)	1

Table: GPT-in-a-Box Cluster: Per-Node Hardware Configuration Nutanix NX-9151-G9

Component	Description	Quantity
Processor	Intel Xeon-Platinum 8462Y+ (2.8 GHz, 32 cores)	2

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2378

Component	Description	Quantity
Memory	64 GB, 4,800 MHz DDR5 RDIMM	16
Network adapter	Mellanox 100, 40, or 25 GbE, 2-port NIC (CX6 100 GbE)	3
Network adapter	SMC 10 GbE, 2-port Base-T, 2-port SFP+ NIC (X710)	1
GPU	NVIDIA L40S 48 GB PCIe	4

Use the software in the following table for the GPT-in-a-Box cluster.

Table: GPT-in-a-Box Cluster: Licensing SKUs

SKU	Description	Quantity
SW-NAI-GPT-ULT-C-PR	GPT-in-a-Box Full Stack Ultimate	HPE or Lenovo: 192; Nutanix NX: 320
SW-NAI-PRO-GB-PR	Nutanix Enterprise AI GPU memory (8 × 48 GB)	384

The GPT-in-a-Box Full Stack Ultimate License contains the following:

- NKP Ultimate
- NCI Ultimate
- NCM Starter
- NDK
- 50 Tib NUS Pro
- 20 vCPU NDB

Nutanix Professional Services

With the following Nutanix Professional Services, Nutanix can implement this NVD as designed, built, and tested.

Table: GPT-in-a-Box Cluster: Professional Services SKUs

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2379

SKU	Description	Quantity
CNS-CLDN-A-WRK-DSGN-ADV-SD	NKP Design Workshop - Adv Ed - Std Doc	1
CNS-INF-A-WRK-DES-GPT	AI/ML Design Workshop	1
CNS-CLDN-A-SVC-DEP-ADV	NKP Deployment - Adv Ed	1
CNS-INF-A-SVC-DEP-GPT	Nutanix Enterprise AI Deployment	1
CNS-INF-A-SVC-DEP-ONP-AHV	Infrastructure Deploy - On-Prem NCI Cluster - AHV	4 (NX: 6)
CNS-DBM-A-SVC-EDP-STD	NDB Deployment	1

Note: These services are based on the GPT-in-a-Box offering and don't include the reference sample application.

These services are outcome-based, with fixed prices for the scope. For more information, see the Nutanix Professional Services information available on Nutanix.com.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2380

6. References

1. Hybrid Cloud: AOS 6.5 with AHV On-Premises Design
2. Enterprise Edge with Artificial Intelligence: AOS 6.5 with AHV Design
3. Nutanix for Enterprise Edge Computing Reference Architecture
4. Nutanix Files User Guide
5. Nutanix Objects User Guide
6. Physical Networking Best Practice Guide

© 2025 Nutanix, Inc. All rights reserved

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2381

About Nutanix

Nutanix offers a single platform to run all your apps and data across multiple clouds while simplifying operations and reducing complexity. Trusted by companies worldwide, Nutanix powers hybrid multicloud environments efficiently and cost effectively. This enables companies to focus on successful business outcomes and new innovations. Learn more at Nutanix.com.

© 2025 Nutanix, Inc. All rights reserved

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2382

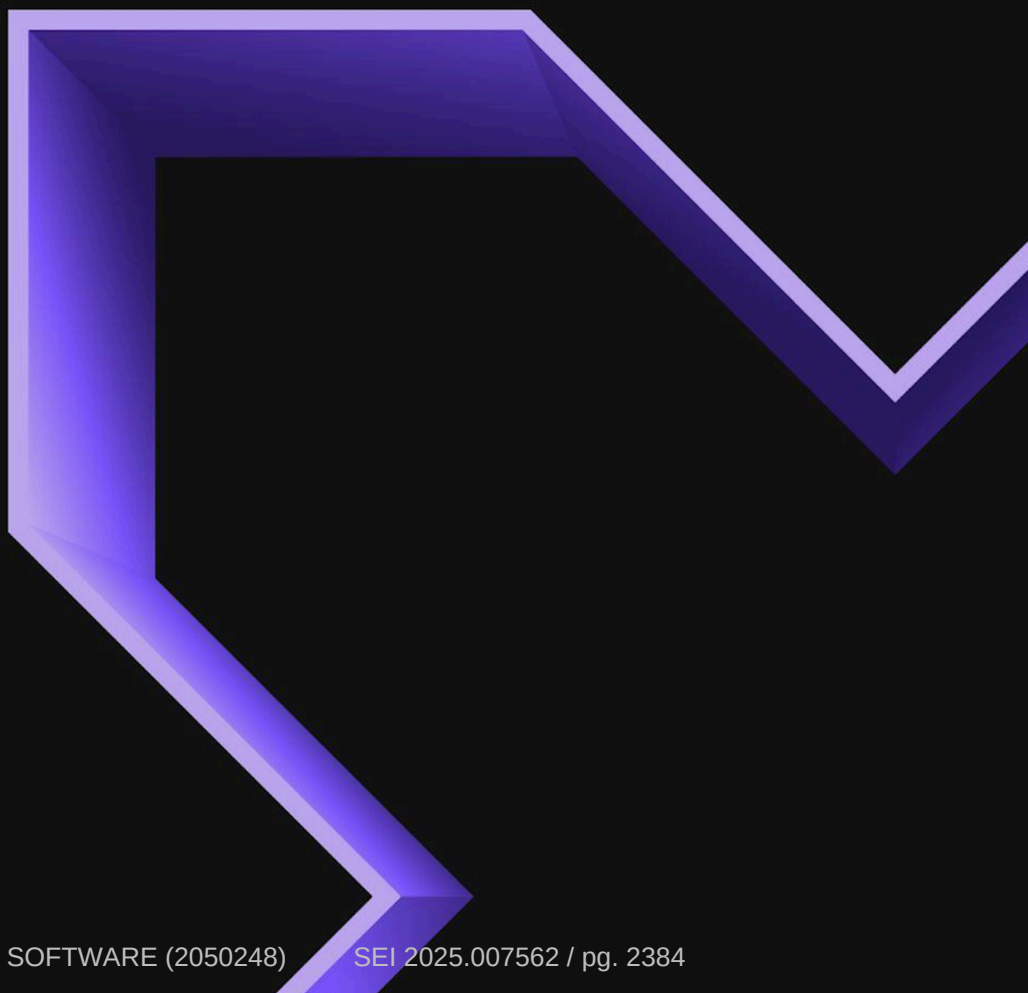
List of Figures

Figure 1: Architectural Layers of the Nutanix Validated Design for GPT-in-a-Box 2.0.....5
Figure 2: GPT-in-a-Box Nutanix Cluster Conceptual Architecture.....15
Figure 3: GPT-in-a-Box Physical Network Architecture.....20
Figure 4: DNS Management.....26
Figure 5: GPT-in-a-Box Monitoring Conceptual Design.....29
Figure 6: Hybrid Cloud Performance Metrics Systems.....30
Figure 7: Rack Layout.....35
Figure 8: Nutanix GPT-in-a-Box Kubernetes Conceptual Design.....40
Figure 9: Kubernetes Monitoring Conceptual Design.....44
Figure 10: LLM Research Workflow.....48
Figure 11: Document Ingestion Workflow.....49

v4.0 | May 2025 | NVD-2155

NUTANIX VALIDATED DESIGN

Databases: AOS 6.10 and Nutanix Database Service 2.8 Design



NUTANIX

Legal

© 2025 Nutanix, Inc. All rights reserved. Nutanix, the Nutanix logo and all Nutanix product and service names mentioned are registered trademarks or trademarks of Nutanix, Inc. in the United States and other countries. All other brand names mentioned are for identification purposes only and may be the trademarks of their respective holder(s).

Certain information contained in this content may link or refer to, or be based on, studies, publications, surveys, and other data obtained from third-party sources and our own internal estimates and research. While we believe these third-party studies, publications, surveys, and other data are reliable as of the date of publication, they have not independently verified unless specifically stated, and we make no representation as to the adequacy, fairness, accuracy, or completeness of any information obtained from a third-party. Our decision to publish, link to or reference third-party data should not be considered an endorsement of any such content.

Code samples and snippets that appear in this content are unofficial, are unsupported, and will require extensive modification before use in a production environment. As such, the code samples and snippets are provided AS IS and are not guaranteed to be complete, accurate, or up-to-date. Nutanix makes no representations or warranties of any kind, express or implied, as to the operation or content of the code samples or snippet. Nutanix expressly disclaims all other guarantees, warranties, conditions and representations of any kind, either express or implied, and whether arising under any statute, law, commercial use or otherwise, including implied warranties of merchantability, fitness for a particular purpose, title and non-infringement therein.

This content reflects an experiment in a test environment. Results, benefits, savings, or other outcomes described depend on a variety of factors including use case, individual requirements, and operating environments, and this publication should not be construed as a promise or obligation to deliver specific outcomes.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

Contents

1. Executive Summary..... 5
Document Version History..... 6

2. Nutanix Platform Architecture..... 8

3. Nutanix Database Service..... 9
Nutanix Database Service Architecture..... 9

4. Nutanix Database Solution Usage Scenarios..... 13
Single-Instance Database..... 13
Clustered Database Instance..... 15
Maintaining Development and Test Databases..... 16

5. Database Infrastructure Design..... 18
Database Hardware..... 18
Nutanix Database Solution Cluster Configuration..... 19
Network Microsegmentation with Flow Network Security..... 22
Nutanix Database Solution Management Components..... 27

6. Nutanix Database Solution Monitoring..... 28
Monitoring Conceptual Design..... 28
Alerts and Event Monitoring..... 31
Nutanix Database Service Alert Management..... 32
Playbooks..... 32
Microsoft SQL Server Monitoring with Nutanix Cloud Manager Intelligent Operations..... 33
Database Monitoring Options..... 33
Monitoring Database VMs in Prism Central..... 36

7. Databases on Nutanix..... 38
Nutanix Database Service Initial Configuration..... 38
SQL Server Implementation Best Practices..... 39
Oracle Implementation Best Practices..... 41
PostgreSQL Implementation Best Practices..... 42

8. Software Patching with Nutanix Database Service..... 47
Patch Microsoft SQL Server Database Software..... 47
Patch Oracle Database Software..... 49
Patch PostgreSQL Database Software..... 51

9. Nutanix AHV High Availability..... 53
Nutanix Database Service Management High Availability..... 53
AHV High Availability Validation..... 53

10. Nutanix Database Service Time Machine Backup and Recovery..... 58
Microsoft SQL Server Backup and Restore Verification..... 58
Oracle Database Restore..... 60
PostgreSQL Backup and Restore Validation..... 61

11. Sample Bill of Materials..... 63

12. Database Test Plans..... 65
SQL Server Test Plans..... 65
Oracle Test Plans..... 72
PostgreSQL Test Plans..... 79

13. References..... 86

About Nutanix..... 87

List of Figures..... 88

1. Executive Summary

Enterprise database deployments aren't a one-size-fits-all proposition. Requirements range from many small database servers with mixed operating systems and database software vendors to large, mission-critical datastores and from web-scale environments where the redundancy is built into the software to environments where infrastructure provides availability and disaster recovery. This Nutanix Validated Design (NVD) offers components you can combine, including validation steps, to ensure that your deployment meets best practice standards and is ready to support your business.

Key benefits of deploying enterprise databases on Nutanix include the following:

- Simplified database management with Nutanix Database Service (NDB; formerly Era)
- Choice of hypervisor and hardware vendors with the latest Intel or AMD processors and latest storage technologies
- Enterprise-grade performance with software-defined architecture
- Reduced total cost of ownership compared to the public cloud
- Hybrid multicloud capabilities

This document covers use cases for deploying and managing databases on Nutanix Cloud Platform using NDB. NDB orchestrates and simplifies database deployments by incorporating database best practices so that you don't have to perform tasks manually at the infrastructure layer. Some of the NDB tasks related to infrastructure include compute creation, storage management, affinity rules, and storage mapping to database servers.

If you plan to deploy databases without NDB, see the best practice guide for your specific database engine:

- Oracle
- Microsoft SQL Server
- PostgreSQL
- MySQL

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2388

- MongoDB

Readers of this document should already be familiar with Nutanix AOS, the Nutanix Platform Architecture for Datacenters reference architecture, the Microsoft SQL Server Database Workloads on Nutanix reference architecture, and Nutanix best practices for databases.

This document describes the components, integration, and configuration for the deployment of NDB and covers the following topics:

- Design decisions for the deployment of NDB
- Validated solution design with NDB
- Sample bill of materials
- Test plan to validate your deployment

Document Version History

Version Number	Published	Notes
1.0	May 2022	Original publication.
1.1	June 2022	Updated the Hardware and NVD Test Cluster Details sections.
1.2	July 2022	Updated the Appendix section.
1.3	September 2022	Aligned with Hybrid Cloud: AOS 5.20 with AHV On-Premises Design.
2.0	November 2022	Added PostgreSQL content.
2.1	December 2022	Updated the Infrastructure Design and Performance Results sections.
2.2	June 2023	Updated the Executive Summary, Infrastructure Design, Nutanix Database Service, and Performance Results sections.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2389

Version Number	Published	Notes
3.0	October 2023	Updated for AOS 6.5.3 and NDB 2.5.2. Added the Network Microsegmentation and Monitoring sections. Removed the Performance Results, SQL Server HammerDB Script File, SQL Server Performance Measurement, and PostgreSQL HammerDB Script File sections.
3.1	November 2023	Updated the Application Connectivity Requirements and Patch PostgreSQL Database Software sections.
3.2	September 2024	Updated the Sample Bill of Materials section.
3.3	November 2024	Updated AOS release cycle descriptions.
3.4	March 2025	Added the NDB Alert Management section.
4.0	May 2025	Updated for AOS 6.10 and NDB 2.8.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2390

2. Nutanix Platform Architecture

The Nutanix hyperconverged solution combines storage, compute, networking, and virtualization into an industry-proven x86 platform for hosting database workloads.

For details on the Nutanix platform architecture, hyperconverged infrastructure, and software components, see the Hybrid Cloud: AOS 6.5 with AHV On-Premises Design and the Nutanix Platform Architecture for Datacenters.

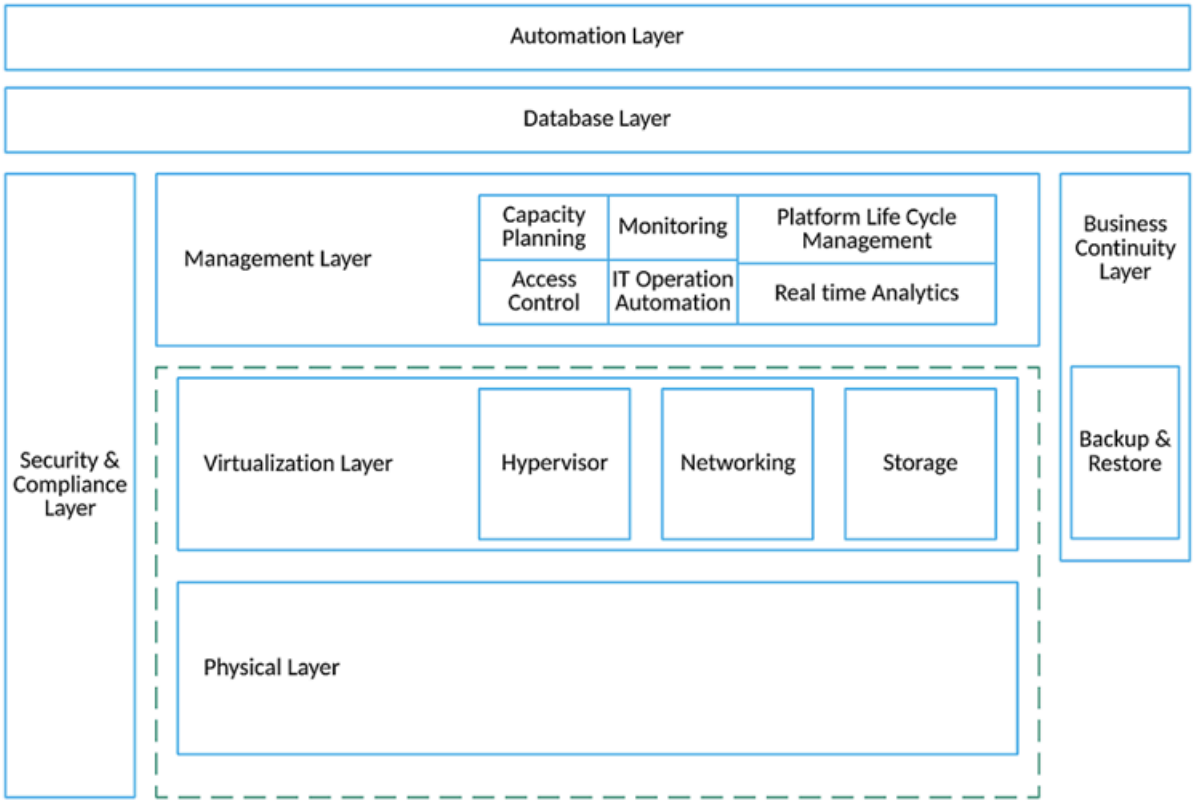


Figure 1: Nutanix Platform for Databases Architecture

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2391

3. Nutanix Database Service

Nutanix Database Service (NDB) is a software suite that automates and simplifies database administration, bringing simplicity and invisible operations to database provisioning and life-cycle management. With one-click database provisioning, copy data management (CDM), database protection, and patching, NDB enables database administrators to provision, clone, and refresh their databases to any point in time. NDB's API-first architecture can easily integrate with your preferred self-service tools, and every operation has a unique ID that's fully visible for auditing.

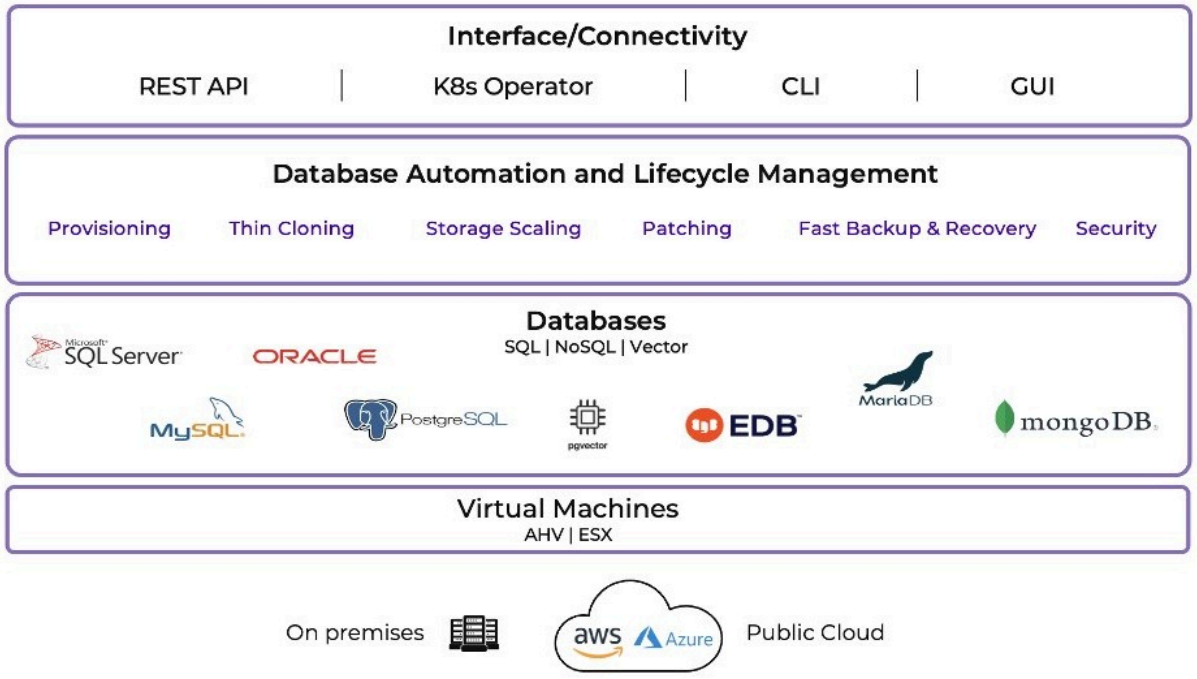


Figure 2: Nutanix Database Service Features

Nutanix Database Service Architecture

The NDB management plane operates on one or more VMs running in a Nutanix cluster with at least three Nutanix nodes (physical servers). The default NDB management plane deployment in a single Nutanix cluster consists of one VM running front-end

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2392

services (API, agent, web service) and the back-end service (database or repository). The following figure presents a logical implementation of the Nutanix database as a service (DBaaS) offering, including the NDB management VM, the logical components, databases, and one Nutanix cluster.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2393

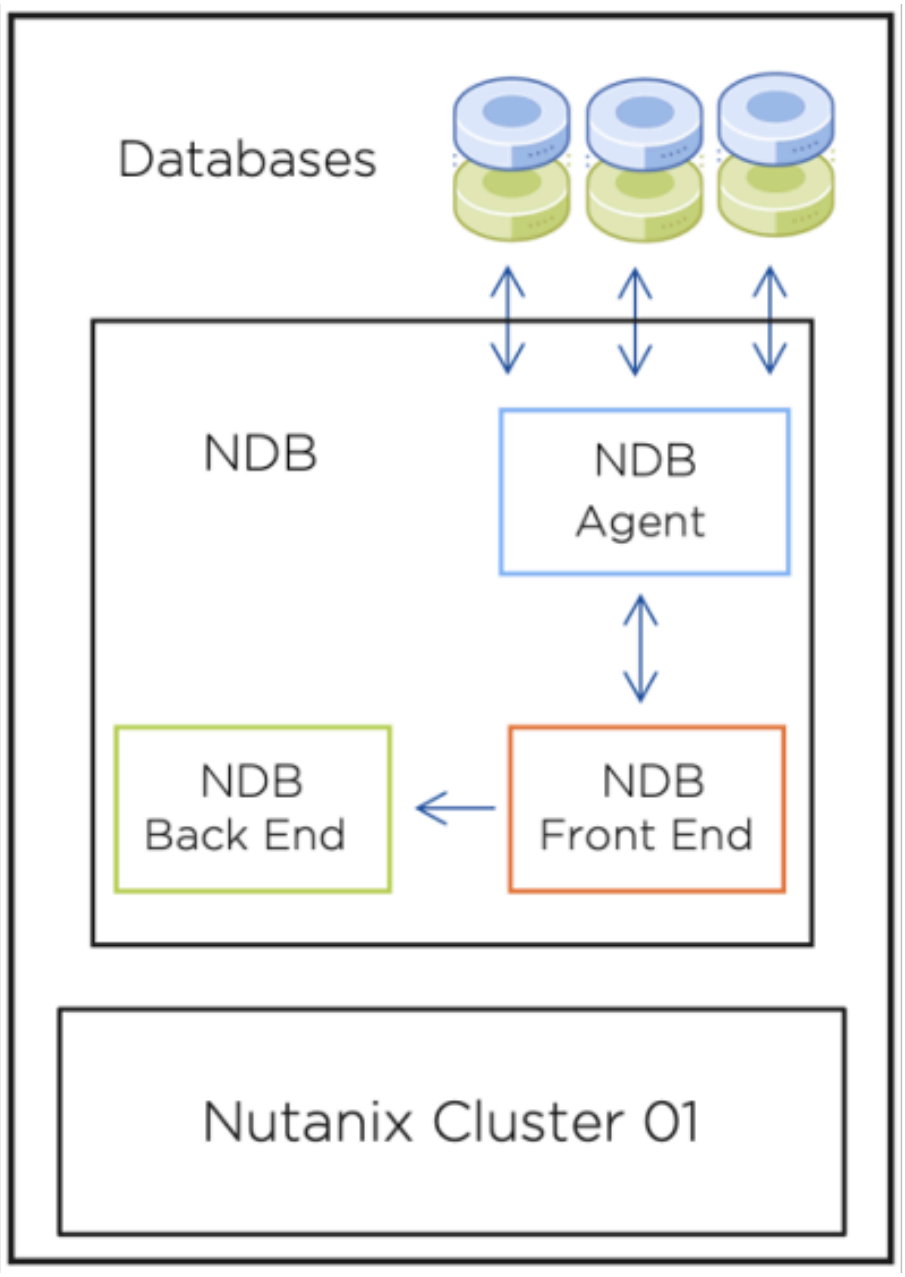


Figure 3: Nutanix Database Service Architecture

NDB is available as a VM shipped as a QCOW2 or OVA image preloaded with a web server, a Postgres repository to hold the database metadata, and the NDB agent.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2394

The NDB agent is deployed on the NDB server and on each of the database server VMs provisioned by NDB. It contains the tools required to perform each task (for example, snapshot, provision, and clone).

You can connect to NDB through the web interface, CLI, or REST APIs. NDB uses an API-first architecture.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2395

4. Nutanix Database Solution Usage Scenarios

With a high-level understanding of the Nutanix platform and Nutanix Database Service (NDB), you can plan database deployments on Nutanix. This section describes the deployment scenarios validated in this Nutanix Validated Design (NVD). The following scenarios are for Oracle, Microsoft SQL Server, and PostgreSQL databases:

- Single-instance database
- Clustered database (Oracle RAC, SQL Server Always On availability group, or PostgreSQL High Availability)
- Development and test database maintenance

Single-Instance Database

This single-instance workflow deploys one or more single-server database instances in a greenfield environment. The first step is creating a new database server VM template image and using that template image to provision a database server VM using NDB.

For the NVD testing, we provisioned a database server VM using NDB with a software profile generated from a newly created VM located in the Nutanix cluster. The validation includes Oracle, SQL Server, and PostgreSQL databases.

To use NDB to provision a single-server database instance, follow these steps:

1. Create a new database VM containing database software.

   The database type determines the software (Windows Server 2022 and SQL Server 2022, RHEL 8.10, Oracle Database 19c RU 24, Oracle Grid Infrastructure 19c RU 24, or PostgreSQL 16.6 with RHEL 8.10). NDB captures the OS disks and the disks with the database software from the source VM when creating the software profile. For more information, see Creating a Windows VM on AHV with Nutanix VirtIO and Creating a VM (AHV).

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2396

2. Install any other required software on the OS drive.
3. Run a check script before registering the database.

   A check script isn't required for SQL Server on Windows. For more information related to Oracle or PostgreSQL databases, see Database Server VM Registration Prerequisite Checks.
4. Register the newly created VM with NDB.

   For more information on database server VM registration, see Oracle Database Server VM Registration, SQL Server Database Server VM Registration, or PostgreSQL Database Server VM Registration.
5. Create a software profile from the newly registered VM.

   For more information on creating a software profile, see Nutanix documentation for Oracle, SQL Server, or PostgreSQL.
6. Create compute and network profiles to provision databases.

   For more information on creating a compute profile, see Nutanix documentation for Oracle, SQL Server, or PostgreSQL. For more information on creating a network profile, see Nutanix documentation for Oracle, SQL Server, or PostgreSQL.
7. Complete the appropriate parameter-definition step based on your database software:

   - Create a database parameter profile for Oracle.
   - Create a database parameter profile and Windows domain profile for SQL Server.
   - Create a database parameter profile for PostgreSQL.
8. Provision a database using the NDB profiles.

   For more information on provisioning a database, see Nutanix documentation for Oracle, SQL Server, or PostgreSQL databases.
9. Sign in to the new VM.
10. Verify that the VM was configured as expected.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2397

Clustered Database Instance

This clustered database workflow deploys clustered database instances in a greenfield environment. The first step is creating a new database server VM template image (containing clustered software components) and generating a clustered software profile from that template image. Using the clustered software profile, we provisioned a clustered database instance using NDB.

The validation includes Oracle, SQL Server, and PostgreSQL databases.

To use NDB to provision a clustered database instance, follow these steps:

1. Create a new database VM containing database software.

   The database type determines the software (Windows Server 2022 and SQL Server 2022; RHEL 8.10, Oracle Database 19c RU 24, Oracle Grid Infrastructure 19c RU 24, or PostgreSQL 16.6 with RHEL 8.10). Patroni high availability components are haproxy 1.5.18, patroni 3.0.2, and etcd 3.3.11. NDB captures the OS disks and disks that the database software is installed on from the source VM when creating the software profile. For more information, see AHV: Create Windows VM and AHV: Create VM (Linux).
2. Install any other required software on the OS drive.
3. Run a check script before registering the database.

   A check script isn't required for SQL Server on Windows. For more information on database server VM registration prerequisite checks, see Nutanix documentation for Oracle or PostgreSQL.
4. Register the newly created VM with NDB.

   For more information on database server VM registration, see Nutanix documentation for Oracle, SQL Server, or PostgreSQL.
5. Create a software profile from the newly registered VM.

   For more information on creating a software profile, see Nutanix documentation for Oracle, SQL Server, or PostgreSQL.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2398

6. Create compute and network profiles to provision the database.

   For more information on creating a compute profile, see Nutanix documentation for Oracle, SQL Server, or PostgreSQL.

   For more information on creating a network profile, see Nutanix documentation for Oracle RAC Database, Windows Clusters, or PostgreSQL HA Instance.
7. Complete the appropriate parameter-definition step based on your database software:
   - Create a database parameter profile for Oracle.
   - Create a database parameter profile and a Windows domain profile for SQL Server.
   - Create a database parameter profile for PostgreSQL.
8. Provision a database server VM using the NDB profiles.

   For more information on provisioning a database server VM using NDB profiles, see Nutanix documentation for Oracle RAC Database, SQL Server Availability Database, or PostgreSQL HA Instance.
9. Sign in to the new database VM.
10. Verify that the cluster and the database were configured as expected.

Maintaining Development and Test Databases

NDB simplifies the process of provisioning development and test databases by creating a production database that NDB registers and manages. The time machine associated with the production database has a service-level agreement (SLA) defined for backup frequency and retention. The snapshots created by the time machine maintain nonproduction copies from the production database for testing, development, and troubleshooting purposes, including automatically refreshing the copies at regular intervals.

To use NDB to provision a development and test database, follow these steps:

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2399

1. Register the production database VM with NDB.

   For more information on database server VM registration, see Nutanix documentation for Oracle, SQL Server, or PostgreSQL.
2. Create compute and network profiles to create nonproduction databases.

   For more information on creating a compute profile, see Nutanix documentation for Oracle, SQL Server, or PostgreSQL.

   For more information on creating a network profile, see Nutanix documentation for Oracle, SQL Server, or PostgreSQL.
3. Complete the appropriate step based on your database software:
   - Create a database parameter profile for Oracle.
   - Create a database parameter profile and a Windows domain profile for SQL Server.
   - Create a database parameter profile for PostgreSQL.
4. Validate the time machine for the production database.

   For more information, see Time Machine Behaviour and Functionality.
5. Create a clone from a source database and set a schedule for automatic refresh.

   For more information on creating single-node database clones, see Nutanix documentation for Oracle, SQL Server, or PostgreSQL.
6. Define a schedule to automatically or manually refresh the clones.

   For more information, see Refreshing Database Clones (Manual).
7. Sign in to the clone VM.
8. Connect to the clone database.
9. Verify the source data.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2400

5. Database Infrastructure Design

To begin the design process, collect your application requirements. Use your requirements to select hardware and apply best practices throughout your cluster. This section provides guidelines for selecting hardware and configuring clusterwide settings for a production database service. If you aren't deploying a mission-critical production application, you can change attributes like the CPU type, vCPU-to-CPU overcommit ratio, network configuration, and amount of free storage to meet your needs.

Database Hardware

Use the following guidelines when selecting hardware for production databases:

- Select a processor with a high clock speed and 12 or more cores per socket on dual-socket servers. Nutanix recommends selecting a CPU with a clock rate of at least 2.7 GHz.
- Use a balanced memory configuration. A balanced memory configuration delivers the highest bandwidth between the processor and memory and the best performance for CPU-intensive applications. The number of DIMMs required for balanced memory varies by model.
- Ensure that you have sufficient memory to allocate a minimum of 64 GB to the Nutanix Controller VM (CVM).
- Select a minimum of dual 25 GbE or faster network interface.
- Use all NVMe or a mix of NVMe and SSD storage.

For more information on OEM and third-party hardware vendors, see the Supported Hardware Platforms and Public Clouds page.

Storage Hardware

Use all NVMe or a mix of NVMe and SSD storage hardware for all databases on Nutanix. A mix of NVMe and SSD offers a high price-performance ratio, making it the best option for a variety of workloads.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2401

Don't use HDD storage for clusters running databases. You can use hybrid clusters with a mix of SSD and HDD storage for backup or archive targets to reduce costs.

CPU

For production database VMs, don't overcommit CPU. If your entire cluster isn't dedicated to production database VMs, you can use affinity rules to keep critical VMs isolated on nodes and increase vCPU overcommit on cluster nodes that run other services (like development, support, and backup database instances).

Nutanix isn't responsible for database license compliance. It's your responsibility to ensure compliance with database engine licensing requirements.

Memory

Configure your infrastructure with balanced memory and ensure sufficient memory for the CVM. A balanced memory configuration can greatly improve application performance because it uses all memory channels to transfer data between memory and CPU.

- In Intel G9 configurations, balanced memory means that you have 16 or 32 DIMMs populated in a two-socket server.
- The Nutanix CVM requires 64 GB of memory (32 GB more than the default) to support a high-performance database workload. Increasing CVM memory can improve random I/O performance by providing more space to cache metadata.

For more information, see the Nutanix Physical Memory Configuration tech note.

Network

Each node must have at least two 25 GbE or faster uplinks, and all nodes in a Nutanix cluster must be connected to the same pair of switches.

For more information, see AHV Networking Best Practices.

Nutanix Database Solution Cluster Configuration

Nutanix recommends deploying a cluster that can fully protect your data and maintain cluster high availability in the case of a node failure. Use an n + 1 configuration, where n is the number of nodes in the cluster. Nodes must have sufficient CPU, memory, and storage capacity to maintain redundancy when a node failure occurs.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2402

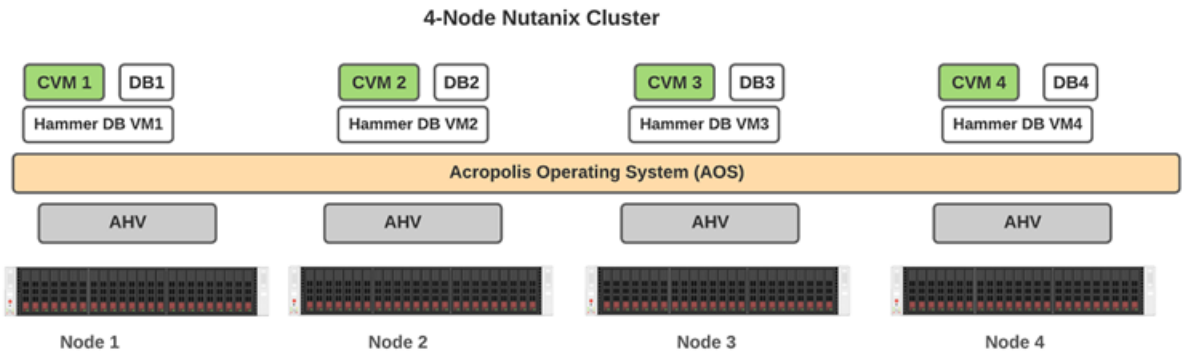


Figure 4: Sample Four-Node Cluster Hosting SQL Server Databases on Nutanix

For all database clusters, start with four nodes, the smallest possible n + 1 cluster. Ensure that you maintain n + 1 as you add nodes to the cluster. When you have at least four nodes, enable some additional configuration options. Enable high availability reservation using Prism to ensure that you have sufficient CPU and memory to fail all the VMs from any node over to other nodes in the event of a node failure.

To ensure that you have sufficient storage capacity, configure Prism so that it generates a warning when the cluster reaches the threshold for resilient capacity (the storage level at which you can still fully recover the data even if a failed node doesn't rejoin the cluster).

Table: Nutanix Validated Design Test Cluster Details

Item	Specification
Manufacturer	Nutanix
Model	NX-8170-G9
Nodes in the cluster	4
AOS version	6.10
AHV version	20230302.102001
CPU model	Intel Xeon Gold 6442Y @ 2.60 GHz
Base frequency	2.60 GHz
Maximum turbo frequency	4.00 GHz
CPUs per node	2
Threads per core	2

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2403

Item	Specification
Cores per socket	24
Sockets per node	2
NUMA node per CPU	2
Installed memory per node	1.48 TiB
NIC speed	100 Gbps
Storage	SSD-PCIe: 12 disks
CVM vCPU	16
CVM memory	64 GB

Storage Configuration

Place database data and logs in a storage container with compression enabled, zero delay, and no deduplication or erasure coding (default). Enabling inline compression saves space and can improve the performance of database workloads running on Nutanix. Don't use deduplication, which adds processing overhead and doesn't reduce space usage for databases. Erasure coding can save storage space, but it consumes significant CPU time to generate parity and checksums, so only use it for archives or other storage needs that don't require high performance.

When creating file systems that require high performance, spread each file system over multiple vDisks. Nutanix Database Service (NDB) automatically implements this best practice.

For a deep dive into Nutanix Data efficiency options, see the Data Efficiency document.

Network Configuration

In a cloud architecture, Ethernet handles client communication, transfers within databases, and storage traffic. High-performance networking is key to good database performance on Nutanix.

Networking best practices:

- Enable LACP in an active-active configuration.
- Check network configurations and related recommendations for each database software VM and type of deployment.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2404

- Create VLANs for use by NDB.

For more information on Nutanix networking best practices, see the following documents:

- Physical Networking Best Practices
- Nutanix AHV Networking Best Practices
- Nutanix Database Service Administration Guide

Network Details

This Nutanix Validated Design (NVD) configures the cluster network so that each port provides 100 Gbps. Nutanix recommends using redundant 25 Gbps (or faster) connections to ensure adequate bandwidth.

This NVD uses the standard 1,500-byte MTU, which delivers excellent performance and stability. For more information on networking in AHV, see Nutanix AHV Networking Best Practices.

We used the Spectrum_NDB_Managed VLAN (VLAN ID: 253) to manage Oracle, SQL Server, and PostgreSQL database VM host IP addresses with an NDB-managed IP address range.

Network Microsegmentation with Flow Network Security

Nutanix Flow Network Security enables VM- and application-based microsegmentation for traffic visibility and control. This NVD uses Flow Network Security to protect the database environment from network attacks, create strict traffic controls that segment the network, and gain visibility into application network behavior for all AHV hosts managed by a single Prism Central instance. Flow Network Security uses categories created in Prism Central and applies the security policies on the respective components.

This NVD covers the following use cases:

- Segment the network and enable application microsegmentation between standalone NDB instances and database server VMs.
- Segment internal networks based on database engine type, application type, or department.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2405

- Visualize and discover network traffic to NDB instances and traffic from NDB to the database server VMs.
- Categorize incoming connections to the database server VMs and configure a least-privilege inbound policy (no traffic allowed).
- Secure the connectivity ports between the NDB instances and the database server VMs.

We made the following Flow Network Security design decisions:

- Limit inbound and outbound security policies based on the requirements.
- Create unique AppType and DatabaseType categories for each application and database.
- Create address groups to define the corporate network for easy rule creation.
- Use port 22 (SSH).
- Use ports 2379 and 8679 (Patroni and etcd).

Application Connectivity Requirements

Define the database AppTypes and AppTiers. For example, set NDB as the AppType and define the AppTier as Web or Application when using NDB. When using PostgreSQL, set PostgreSQL as the AppType and define the AppTier as Database. Create the smallest number of application types and application tiers to uniquely identify and group your applications.

Create a category to organize the required database VMs based on database engine type (such as SQL Server, Oracle, PostgreSQL) and tier (like production, development, and QA). You can create categories at the source and destination entities.

For each application policy, determine whether the application's required inbound traffic comes from a VM in the Nutanix environment or from an external source. Then you must determine the required traffic between application tiers and decide whether to allow traffic within the same tier. Finally, you must decide whether to allow outbound traffic for the application.

Define the following database ports as services in Prism Central:

- The ports allowed between the NDB instance and the source

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2406

- The destination ports between NDB and the database VMs

For applications that require granular traffic control, create application tiers for different VMs. For example, NDB and Prism Element can be in different application tiers. Configure rules to allow traffic to and from individual application tiers.

For more information on ports and protocols between NDB and database VMs, see the Software Type: Ports and Protocols page and the NDB Network Requirements section of the Nutanix Database Service Administration Guide.

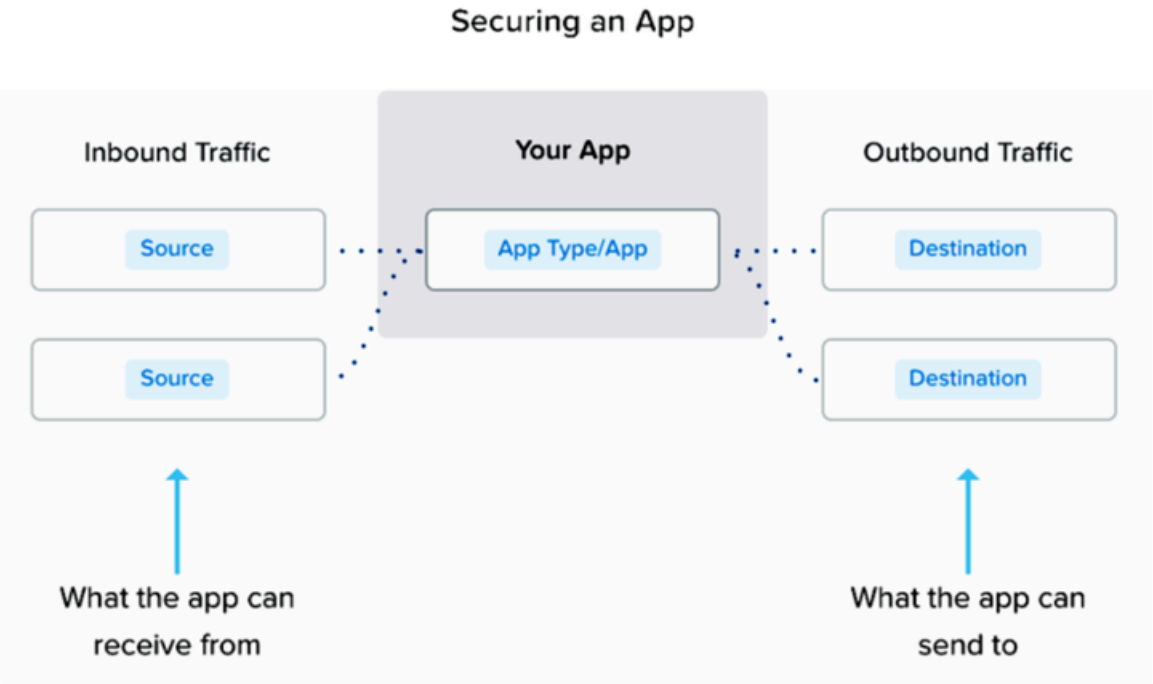


Figure 5: Securing an Application

The following tables provide example security policies between NDB and multiple types of database server VMs. Modify the name and specific addresses, categories, and ports based on the databases you protect.

Table: NDB and PostgreSQL Security Policy

Purpose	Source	Traffic	Destination	Port / Protocol
Allow corp clients to NDB	AddrCorpClient	Inbound	AppType: NDB; AppTier: Web	HTTPS 443

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2407

Purpose	Source	Traffic	Destination	Port / Protocol
Allow database VMs to NDB Server	AddrDatabasevms	Inbound	AppType: NDB; AppTier: Web	HTTPS 443
Allow NDB to database VMs	AppType: NDB; AppTier: Web	Outbound	AppType: PostgreSQL AppTier: DB	SSH 22; Patroni: 2379, 8679

Table: NDB and Oracle Security Policy

Purpose	Source	Traffic	Destination	Port / Protocol
Allow corp clients to NDB	AddrCorpClient	Inbound	AppType: NDB; AppTier: Web	HTTPS 443
Allow database VMs to NDB Server	AddrDatabasevms	Inbound	AppType: NDB; AppTier: Web	HTTPS 443
Allow NDB to database VMs	AppType: NDB; AppTier: Web	Outbound	AppType: OracleAppTier: DB	SSH 22

Table: NDB and SQL Server Security Policy

Purpose	Source	Traffic	Destination	Port / Protocol
Allow corp clients to NDB	AddrCorpClient	Inbound	AppType: NDB; AppTier: Web	HTTPS 443
Allow database VMs to NDB	AddrDatabasevms	Inbound	AppType: NDB; AppTier: Web	HTTPS 443
Allow NDB to database VMs	AppType: NDB; AppTier: Web	Outbound	AppType: SQL Server AppTier: DB	WINRM 5985

In this NVD, the management traffic and the database traffic are on the same VLAN. If your management and database traffic use separate VLANs, create different destination outbound rules.

This NVD represents address groups with the following addresses of corporate servers and clients to allow differentiated access from database server VMs. Replace these placeholders with addresses specific to your deployment.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2408

Table: Address Groups

Name	Addresses	Purpose
AddrCorpAll	10.0.0.0/8	Identify all corporate IP addresses.
AddrCorpClient	10.50.0.0/16	Identify all IP addresses that belong to corporate client devices.
AddrCorpServer	10.47.23.0/24	Identify all IP addresses that belong to corporate server devices.

The following figure presents a sample security policy configuration in Prism Central. It shows the traffic between the NDB instance and the database server VMs.

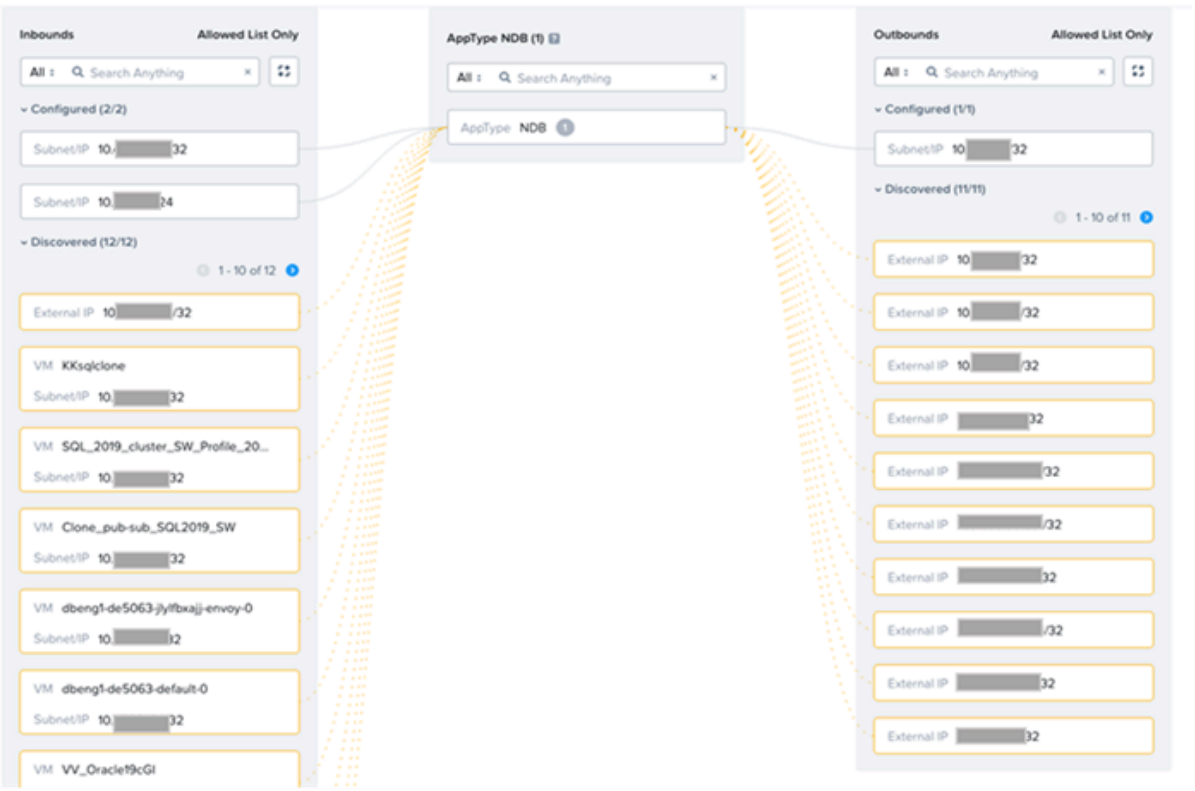


Figure 6: Prism Central Security Policy Example

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2409

Nutanix Database Solution Management Components

Management components such as Prism Central, Active Directory, DNS, and NTP must be highly available. Prism Central is responsible for VM management, replication, application orchestration, microsegmentation, and other monitoring and analytics functions. You can deploy Prism Central in either a single-VM or scale-out (three-VM) configuration.

For more information on VM resource assignment when deploying Prism Central, see the Hybrid Cloud: AOS 6.5 with AHV On-Premises Design.

For more information on installing Prism Central, see the Prism Central Deployment section of the Prism Central Infrastructure Guide.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2410

6. Nutanix Database Solution Monitoring

Monitoring in this Nutanix Validated Design (NVD) falls into two categories: event monitoring and performance monitoring. Each category addresses different needs and issues.

In a highly available environment, you must monitor events to maintain higher service levels. When faults occur, the system must raise alerts promptly so that administrators can remediate as soon as possible. This NVD configures the Nutanix platform's built-in capability to generate alerts in case of failure.

In addition to keeping the platform healthy, maintaining a healthy level of resource usage is also essential to the delivery of a high-performing environment. Performance monitoring continuously captures and stores metrics that are essential when you must troubleshoot application performance. A comprehensive monitoring approach tracks metrics related to the following areas:

- Applications and databases
- Operating system
- Hyperconverged platform
- Network environment
- Physical environment

By tracking a variety of metrics in these areas, the Nutanix platform can also provide capacity monitoring across the stack. Most enterprise environments inevitably grow, so you must understand resource utilization and the rate of expansion to anticipate changing capacity demands and avoid any business impact caused by a lack of resources.

Monitoring Conceptual Design

In this NVD, Prism Central performs most of the event monitoring. To cover situations where Prism Central might be unavailable, we configured each Nutanix cluster in this

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2411

NVD with SMTP-based email alerts. Each Nutanix cluster can send notifications to a different mailbox when Prism Central isn't available.

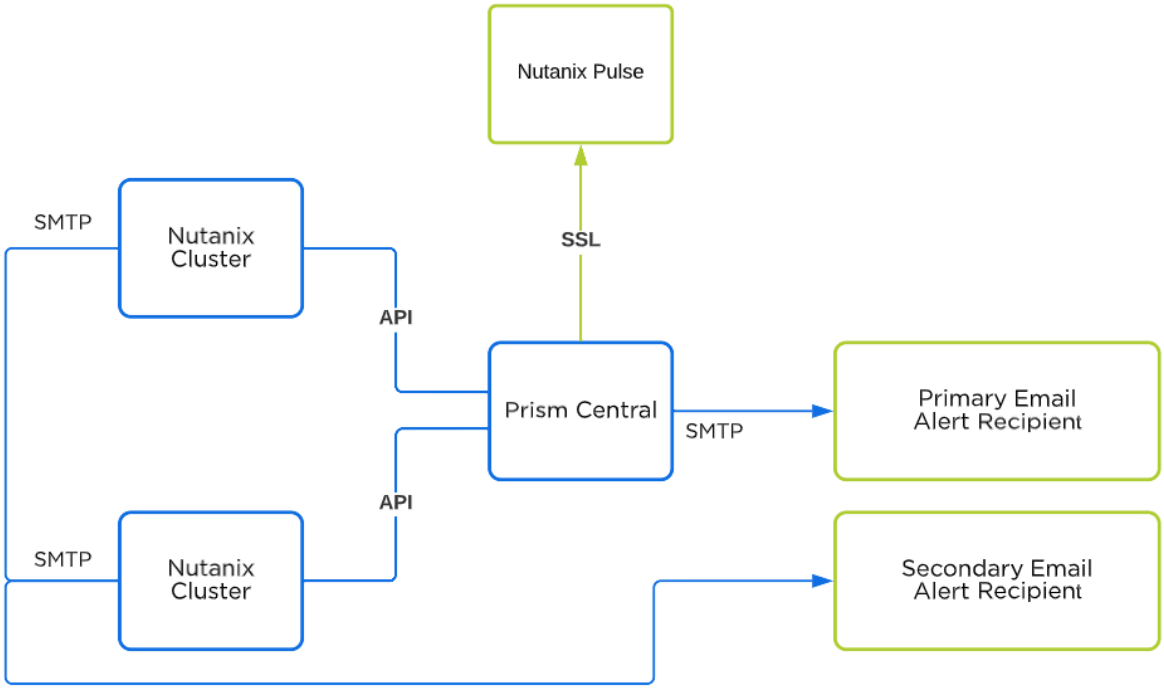


Figure 7: Hybrid Cloud On-Premises Monitoring Conceptual Design

Prism Central monitors and captures cluster performance in key areas such as CPU, memory, network, and storage utilization by default. When a Prism Central instance manages a cluster, Prism Central transmits all Nutanix Pulse data so it doesn't originate from individual clusters. When you enable Pulse, it detects known issues affecting cluster stability and automatically opens support cases.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2412

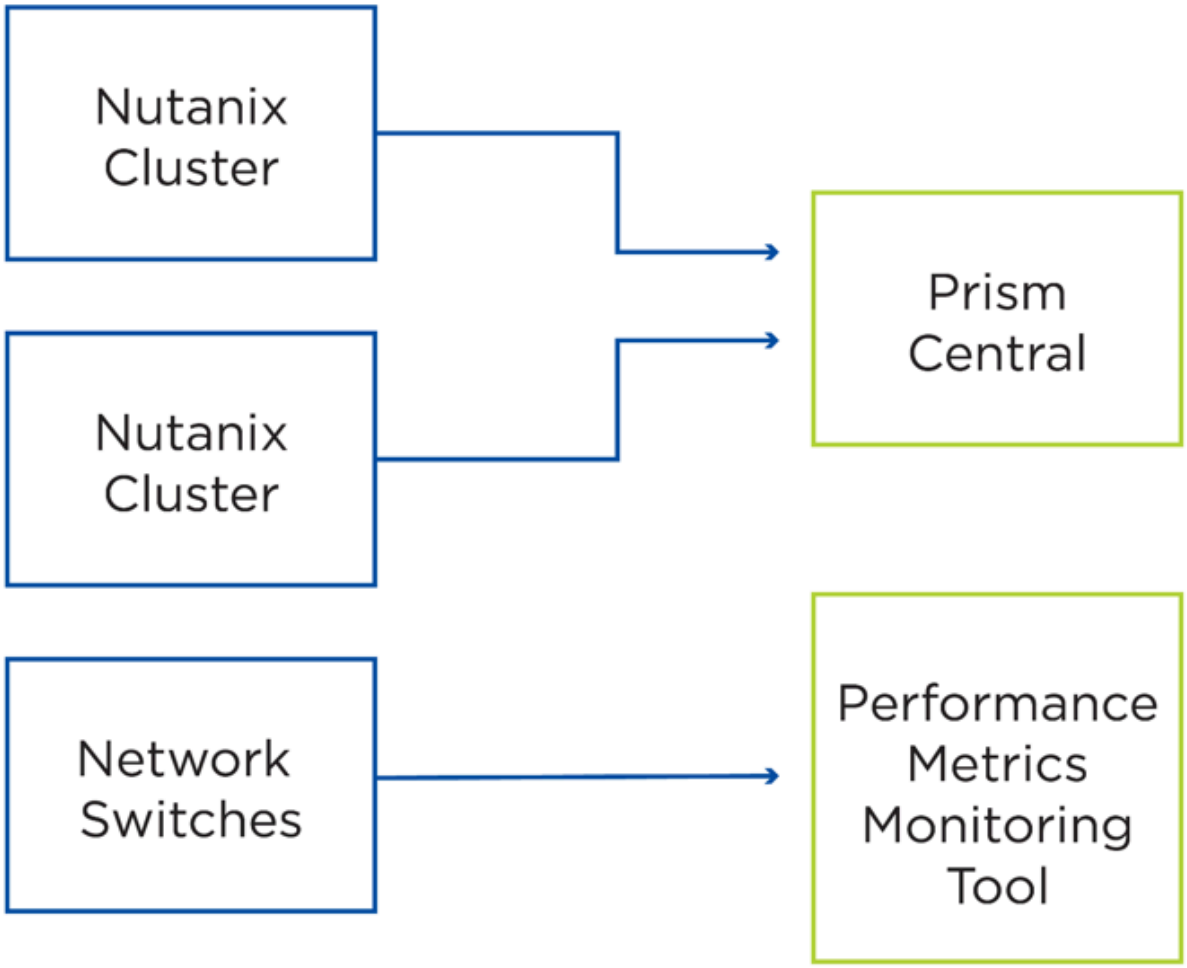


Figure 8: Hybrid Cloud Performance Metrics Systems

The network switches that connect the cluster also play an important role in cluster performance. A separate monitoring tool that's compatible with deployed switches can capture switch performance metrics. For example, an SNMP-based tool can regularly poll counters from the switches.

We made the following monitoring design decisions:

- Prism Central monitors Nutanix platform performance.
- A separate tool that performs SNMP polling to the switches monitors network switch performance.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2413

- On the database cluster with AOS 6.10.x, leave the Prism Element storage utilization warning threshold at 75 percent (the default value).
- For the Prism Element health check, leave the host CPU utilization warning threshold at 75 percent (the default value).
- SMTP alerting:
  - Use SMTP alerting; use an enterprise SMTP service as the primary SMTP gateway for Prism Element and Prism Central.
  - Configure the source email address to be `clustername@<yourdomain>.com` to uniquely identify the source of emails. For Prism Central, use the Prism Central host name in place of `clustername`.
  - Configure the Prism Central recipient email address to be `primaryalerts@<yourdomain>.com`.
  - Configure the Prism Element recipient email address to be `secondaryalerts@<yourdomain>.com`.
- Configure daily Nutanix Cluster Check reports to run at 6:00 AM local time and send them by email to the primary alerting mailbox.
- Configure Nutanix Pulse to send telemetry data to Nutanix.

Alerts and Event Monitoring

Prism Central provides a notification mechanism and allows you to configure and monitor database infrastructure alerts and events. You can also create custom, user-defined alerts and events based on your requirements.

- Create custom alert policies to monitor database infrastructure entities (such as VMs, hosts, and clusters).
- Group database VMs into categories to assign custom alert policies.
- Define a single alert policy for VMs, hosts, or clusters that share common criteria.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2414

- Monitor common metrics, including:
  - CPU usage
  - Memory usage
  - Controller average read and write I/O latency
  - Controller read and write IOPS

For a full list of metrics, see the Alert Metrics section of the Prism Central Alerts and Events Reference Guide.

For more information on Alert Policies, see the Alert Policies (Prism Central) section of the Prism Central Alerts and Events Reference Guide.

Nutanix Database Service Alert Management

NDB uses an alert management system to notify you if any operation fails. Each NDB operation, such as provisioning a database or creating a clone, is linked to an alert policy. If an operation fails and its associated policy is enabled, NDB generates an alert.

NDB supports both push and pull mechanisms for delivering alerts. For push notifications, alerts can be sent through SMTP. For pull-based access, you can retrieve alerts using NDB's REST API. NDB maintains its own alert management system and doesn't pass the alerts through Prism Element or Prism Central.

For more information on sending NDB alerts to an email recipient, see the Alert Notifications section of the NDB Administration Guide.

Playbooks

A playbook allows you to define a trigger for an action or a series of actions. A trigger can be an event that occurs in the system, such as an alert or a request. The resulting actions can be VM actions, communication actions, alerts, or reports. You can combine playbooks with alerts or events to perform corrective actions for database infrastructure.

You can create playbooks based on predefined alert triggers, or you can create a manual trigger. For more information, see Playbook Triggers.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2415

Microsoft SQL Server Monitoring with Nutanix Cloud Manager Intelligent Operations

Nutanix Cloud Manager Intelligent Operations provides application monitoring and deep insights into Microsoft SQL Server performance metrics. You can use it to discover, monitor, and collect SQL Server instance details with Nutanix and third-party data collectors.

For more information, see the Application Instance Details View (SQL Server) section of the Intelligent Operations Guide.

Database Monitoring Options

This NVD hasn't validated all of the tools described in this section. These tools are examples of common database monitoring options that you can choose from.

It's your responsibility to ensure compliance with database software licensing and the tools you use. Nutanix can't offer advice about whether a specific license or a specific number of licenses can guarantee that you can pass a database engine vendor licensing audit. Consult the database vendor for licensing guidelines.

Oracle Enterprise Manager

Oracle Enterprise Manager offers a centralized suite for monitoring, management, and integration tailored for Oracle databases. It provides visibility into database performance, facilitating advanced diagnostics. Oracle Enterprise Manager includes automatic tuning and diagnostic tools. You can extend the platform with various plugins for additional functionalities.

Choose Oracle Enterprise Manager if your organization predominantly uses Oracle databases and requires comprehensive native support, seamless integration, and a diverse array of database-specific features.

SolarWinds Database Performance Analyzer

SolarWinds Database Performance Analyzer (DPA) offers real-time monitoring and diagnostic capabilities customized for Oracle, Postgres, SQL Server, MariaDB, and MySQL databases. It specializes in SQL query analysis and provides tuning recommendations. DPA's interface offers customizable dashboards.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2416

Choose DPA if your organization needs a cross-platform monitoring tool that delivers real-time diagnostics and SQL query optimization.

Prometheus

Prometheus is an open-source monitoring solution designed for cloud-native environments. It offers extensive customization possibilities through a robust ecosystem of exporters and integrations. Prometheus supports autodiscovery and dynamic service monitoring.

Choose Prometheus if your organization operates in a cloud-native environment and needs a customized, scalable monitoring solution.

MongoDB Atlas Monitoring

MongoDB Atlas Monitoring is a fully managed, cloud-based solution that provides real-time monitoring capabilities for MongoDB clusters. Automated scaling and backup features are available. The tool integrates seamlessly with MongoDB Atlas database hosting.

Choose MongoDB Atlas Monitoring when using MongoDB Atlas as your database hosting platform.

Ops Manager

Ops Manager offers monitoring, backup, and automation features tailored for MongoDB. It provides both on-premises and cloud deployment options. Custom alerting and scaling policies are fully supported. Automation capabilities are available for backup and recovery tasks.

Choose Ops Manager when you need a monitoring and management tool (whether on-premises or cloud-based) that offers extensive customization options to meet specific requirements.

Percona Monitoring and Management

Percona Monitoring and Management (PMM) is an open-source monitoring and management solution. It provides real-time monitoring and in-depth query analytics for a variety of database engines like MongoDB, PostgreSQL, and MySQL. PMM supports custom alerting and query performance analysis. It's suitable for hybrid and on-premises deployments.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2417

Choose PMM if you prefer open-source solutions and require robust monitoring and query analysis for various database systems.

SQL Server Management Studio

Microsoft SQL Server Management Studio (SSMS) is a tool for managing and monitoring SQL Server instances. It offers a user interface for real-time monitoring, queries, and performance tuning. SMSS supports custom scripts and extensions for advanced management tasks.

Choose SSMS to manage and monitor individual SQL Server instances when additional costs are a concern.

SQL Diagnostic Manager for SQL Server

SQL Diagnostic Manager offers monitoring and alerting tailored for SQL Server environments. It provides real-time performance analysis and historical data tracking. You can customize alerting and reporting features in SQL Diagnostic Manager. It supports automation for routine maintenance tasks.

Choose SQL Diagnostic Manager if you need in-depth monitoring, advanced alerting, and automation for SQL Server environments.

pgAdmin

pgAdmin is an open-source solution that offers an interface for PostgreSQL database management and monitoring.

Choose pgAdmin if you need basic PostgreSQL monitoring and management capabilities for a small organization.

EnterpriseDB PostgreSQL Enterprise Manager

EnterpriseDB PostgreSQL Enterprise Manager (PEM) offers PostgreSQL monitoring, alerting, and performance tuning. It supports both open-source PostgreSQL and EnterpriseDB Postgres Advanced Server. You can use it for advanced query performance analysis and historical data tracking.

Choose EnterpriseDB PEM if you need advanced monitoring and performance tuning for both open-source and commercial PostgreSQL deployments.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2418

Monitoring Database VMs in Prism Central

The Analysis dashboard in Prism Central offers a wide range of monitoring options at many levels, from the entire cluster to individual virtual disks. It shows the historical development of a variety of metrics and can provide a quick overview of cluster performance.

You can access the Analysis dashboard from the Prism Central main dashboard by entering `Analysis` in the search bar. In older versions of Prism Central, you can access the Analysis dashboard from the Operations section of the main menu.

The following sections provide example procedures to demonstrate the database monitoring tools in Prism Central.

Monitoring Cluster Storage IOPS

To create a chart that tracks storage IOPS for one cluster, follow these steps:

1. Click **Add Chart**.
2. Select **Cluster** from the **Entity** dropdown.
3. Select a cluster from the cluster dropdown.
4. Enter **IOPS** in the **Metric** field.

   Entering a query in the **Metric** field filters the dropdown.
5. Select the following metrics for the chart:
   - Controller IOPS
   - Controller Read IOPS
   - Controller Write IOPS
6. Enter a name for the chart in the **Chart Name** field.
7. Click **Add**.

Monitoring Cluster CVM CPU Usage

To create a chart that tracks the CVM CPU usage for a cluster, follow these steps:

1. Click **Add Chart**.
2. Select **VM** from the **Entity** dropdown.
3. Choose the cluster CVMs to be monitored.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2419

4. Select **CPU Usage (%)** from the **Metric** dropdown.
5. Enter a name for the chart in the **Chart Name** field.
6. Click **Add**.

To monitor database VM CPU usage, follow the same steps but select database VMs instead of CVMs in the entity section.

Monitoring VM Storage Latency

To create a chart that tracks the storage latency for a database VM, follow these steps:

1. Click **Add Chart**.
2. Select **VM** from the **Entity** dropdown.
3. Select the database VM to be monitored.
4. Enter **Latency** in the **Metric** dropdown.
5. Select the following metrics:
   - Storage Controller Read Latency
   - Storage Controller Write Latency
6. Enter a name for the chart in the **Chart Name** field.
7. Click **Add**.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2420

7. Databases on Nutanix

To deploy databases on Nutanix, fulfill the infrastructure requirements and follow the best practices for optimal performance. Although this Nutanix Validated Design (NVD) covers database management using Nutanix Database Service (NDB), you can deploy databases manually without NDB and achieve the required goals.

Nutanix Database Service Initial Configuration

To configure and use NDB to manage databases, follow these steps:

1. Download NDB from the Nutanix Support portal.

   Note: This NVD uses NDB version 2.8. For more information on downloading NDB, see the NDB Downloads page (Nutanix credentials required).

2. Upload the image to the cluster using Prism Element.
3. Create an NDB VM.

   For more information, see Installing NDB on AHV.
4. Perform the initial NDB configuration.

   For more information, see NDB Initial Configuration.
5. Finish setting up NDB using the **Welcome to NDB** wizard.

   For more information, see Get Started with NDB.

NDB-Managed Networks in NDB

This NVD configures an NDB-managed IP address pool on each of the testing VLANs.

Each network (VLAN) can have static IP address management provided by NDB or DHCP provided by an external server.

NDB can use VLANs configured in AHV to provision database server VMs. NDB can manage a pool of IP addresses that are statically assigned to database VMs as they're provisioned. For single-node database server VMs, you can use an NDB-managed IP

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2421

address range or an external DHCP server. For clustered database provisioning, use NDB for IP address management.

NDB Networks

NDB uses network profiles to associate VLANs with database servers. This NVD validates the VLANs on the Nutanix cluster, adds those VLANs to NDB, and enables NDB IP address management. Use an NDB-managed network with an assigned static IP address range to provision SQL Server clustered databases and Oracle RAC databases. For more information, see NDB Network Management.

NDB Compute

This NVD broadly defines three VM sizes: small, medium, and large. These VM sizes are examples based on data from Nutanix Sizer, which uses VM requirements as input to generate an appropriate hardware configuration.

Table: Example VM Configurations for Database Validation

VM Size	vCPUs	Memory
Small	2	32
Medium	4	64
Large	8	128

These example VM sizes can meet some database requirements. For your environment, ensure that your VM size matches your application requirements before implementation.

SQL Server Implementation Best Practices

Set the SQL Server maximum memory setting to a value that leaves memory free for other processes running on the system. For examples and calculations for setting the SQL Server maximum memory parameter, see Microsoft SQL Server Design.

Keeping the SQL Server memory requirement within the vNUMA boundary can provide optimal performance. For large databases, you might need to make the SQL Server memory larger than the vNUMA boundary. For more information on vNUMA for SQL Server, see Microsoft SQL Server on Nutanix Best Practices.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2422

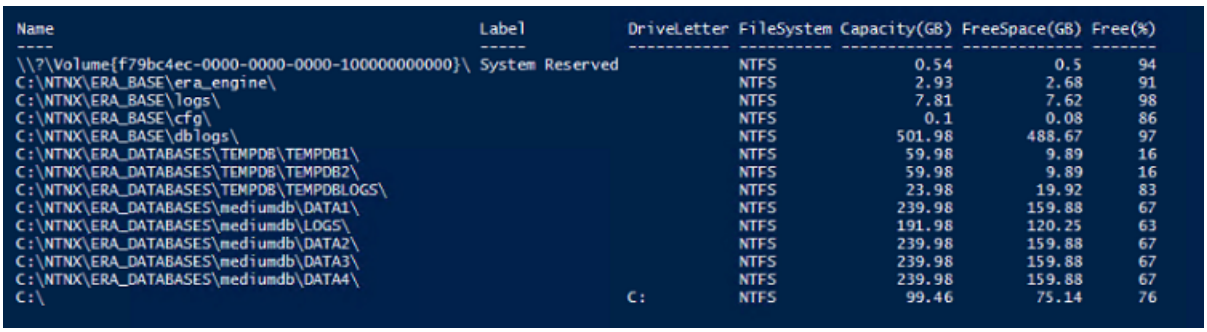
This NVD configures the SQL Server maximum memory settings using NDB SQL Server database instance profiles.

Table: Example SQL Server Database Instance Profiles

Size	Memory	Test Database Size	SQL Server Max Memory Setting
Small	32 GB	100 GB	27,148 MB
Medium	64 GB	300 GB	59,416 MB
Large	128 GB	500 GB	123,952 MB

SQL Server Storage Configuration

For databases smaller than 2 TB, NDB configures four data disks for each database and calculates the number of data files for each SQL Server database based on the number of vCPUs configured for the VM. NDB configures log files to be 20 percent of the database size and the initial tempdb size to be 10 percent of the database size by default.



Name	Label	DriveLetter	FileSystem	Capacity(GB)	FreeSpace(GB)	Free(%)
\\?\Volume{f79bc4ec-0000-0000-0000-100000000000}\	System Reserved		NTFS	0.54	0.5	94
C:\NTNX\ERA_BASE\era_engine\			NTFS	2.93	2.68	91
C:\NTNX\ERA_BASE\logs\			NTFS	7.81	7.62	98
C:\NTNX\ERA_BASE\cfg\			NTFS	0.1	0.08	86
C:\NTNX\ERA_BASE\dblogs\			NTFS	501.98	488.67	97
C:\NTNX\ERA_DATABASES\TEMPDB\TEMPDB1\			NTFS	59.98	9.89	16
C:\NTNX\ERA_DATABASES\TEMPDB\TEMPDB2\			NTFS	59.98	9.89	16
C:\NTNX\ERA_DATABASES\TEMPDB\TEMPDBLOGS\			NTFS	23.98	19.92	83
C:\NTNX\ERA_DATABASES\mediumdb\DATA1\			NTFS	239.98	159.88	67
C:\NTNX\ERA_DATABASES\mediumdb\LOGS\			NTFS	191.98	120.25	63
C:\NTNX\ERA_DATABASES\mediumdb\DATA2\			NTFS	239.98	159.88	67
C:\NTNX\ERA_DATABASES\mediumdb\DATA3\			NTFS	239.98	159.88	67
C:\NTNX\ERA_DATABASES\mediumdb\DATA4\			NTFS	239.98	159.88	67
C:\		C:	NTFS	99.46	75.14	76

Figure 9: SQL Server Database Example Disk File System

NDB creates the database disk drives and attaches them to the database server VM as mount points under the `C:\NTNX\ERA_DATABASES\` directory.

For SQL Server Always On cluster database servers, all the nodes contain a similar disk layout.

Nutanix best practices are a starting point for any SQL Server deployment. Analyze and calculate your storage requirements and adjust the storage environment, disk layout, number of data files, temp files, and log files accordingly. For more information on the

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2423

logical and physical disk designs for typical SQL Server environments, see Microsoft SQL Server on Nutanix Best Practices.

Oracle Implementation Best Practices

This NVD assigns 10 percent of system memory for the operating system and file cache. Of the remaining memory, 80 percent is assigned to the System Global Area (SGA) and 20 percent to the Program Global Area (PGA). This NVD configures temp tablespace, undo tablespace, and the processes parameter to accommodate these settings. Adapt these settings to fit your application requirements.

Oracle Storage Configuration

NDB spreads the DATA and RECO (redo and archive files) disk groups across multiple vDisks for optimal performance. NDB supports both Oracle Automatic Storage Management (ASM) and local file systems. It also supports ASMFD (if the operating system supports ASMFD), ASMLIB, and udev rules for ASM disk mappings.

When provisioning a database, NDB calculates the required number of vDisks for DATADG and RECODG disk groups based on the database size. This NVD configures all Oracle databases used for this validation to accommodate 2 TiB of data, which is considered a large database. The number of vDisks per disk group depends on the database size requested. For a 2 TiB database, NDB creates eight vDisks for DATADG (2,048 GB ÷ 8 = 256 GB per disk) and four vDisks for RECODG.

The storage configuration is independent of the vCPU and memory of the database VMs. Small, medium, or large database VMs in this NVD refer to the amount of vCPU and memory.

Table: Number of Disks Created by NDB Based on Database Size

Disk Groups	Small or Medium (< 2 TB)	Large (> 2 TB)
CRSDG	3 vDisks	3 vDisks
DATADG	4 vDisks	8 vDisks
RECODG	2 vDisks	4 vDisks

Note: The CRSDG disk group only exists for Oracle RAC databases.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2424

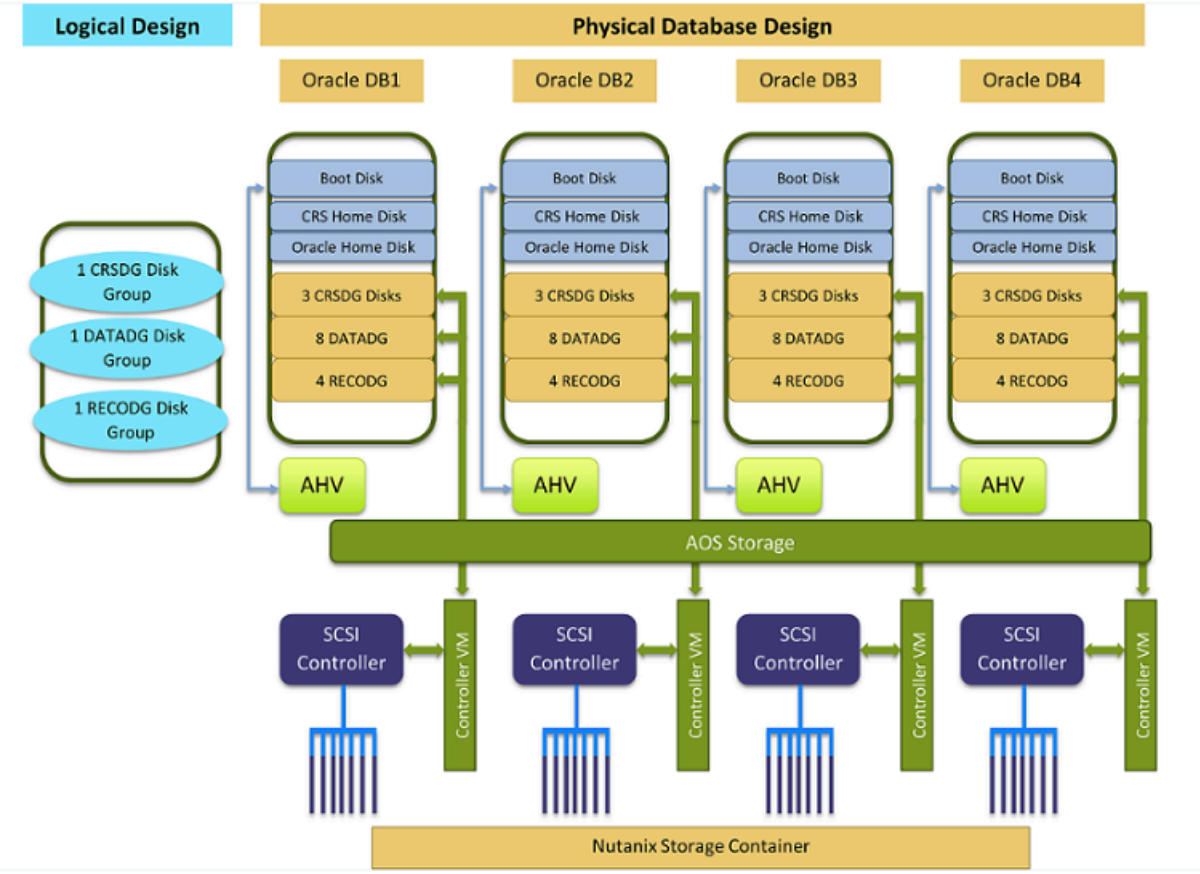


Figure 10: Logical and Physical Design for Oracle Database

Oracle Network Configuration

This NVD configures separate VLANs for the Oracle public network and Oracle private interconnect for cache fusion. After you configure the networks in NDB, NDB-managed networks assign the IP addresses for public, private, and virtual networks.

For more information, see AHV Networking Best Practices.

PostgreSQL Implementation Best Practices

We assigned 10 percent of system memory for the operating system and file cache, 25 percent for the `shared_buffers`, and 50 percent for the `effective_cache_size`. Adapt these settings to fit your application requirements.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2425

We used the following software versions in this NVD:

- PostgreSQL 16.6
- NDB 2.8

Prepare PostgreSQL Software Profile Version

You can create a software profile from a previously registered Postgres database server VM, or you can create a new database software VM that you register as a new software profile.

To create a new database server VM with NDB, follow these steps:

1. Use Prism to create a VM with a supported operating system.

   For more information on supported OS options, see the NDB release notes (Nutanix credentials required).
2. Install a supported version of PostgreSQL.

   You can install PostgreSQL binaries in any directory; specify the path to the binaries when you create the software profile. For more information on supported versions, see the latest NDB release notes.
3. Customize the VM as required.

   For more information, see PostgreSQL on Nutanix Best Practices.
4. Install any nondefault packages your environment uses.
5. Ensure that your VM meets NDB configuration requirements:
   a. Enable the `postgresql` user for `NOPASSWD sudo`.
   b. Configure software repositories for NDB OS updates.
   c. Add any scripts that must run before or after deployment for NDB configuration.

PostgreSQL Configuration

The following table captures the PostgreSQL configuration used in this NVD.

Table: Example PostgreSQL Database Instance Profiles

Size	Memory	Test Database Size	Shared Buffers	Effective Cache Size
Small	64 GB	100 GB	16 GB	32 GB

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2426

Size	Memory	Test Database Size	Shared Buffers	Effective Cache Size
Medium	128 GB	300 GB	32 GB	64 GB
Large	256 GB	500 GB	64 GB	128 GB

These example VM sizes can meet some database requirements. For your environment, ensure that your VM size matches your application requirements before implementation.

PostgreSQL Storage Configuration

This NVD uses the optimized storage configuration provided by NDB. NDB creates striped Linux logical volumes based on the database size specified during provisioning. The database software and logs are placed in the `data` directory, and the database tablespaces are placed in the `tsdata` directory.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2427

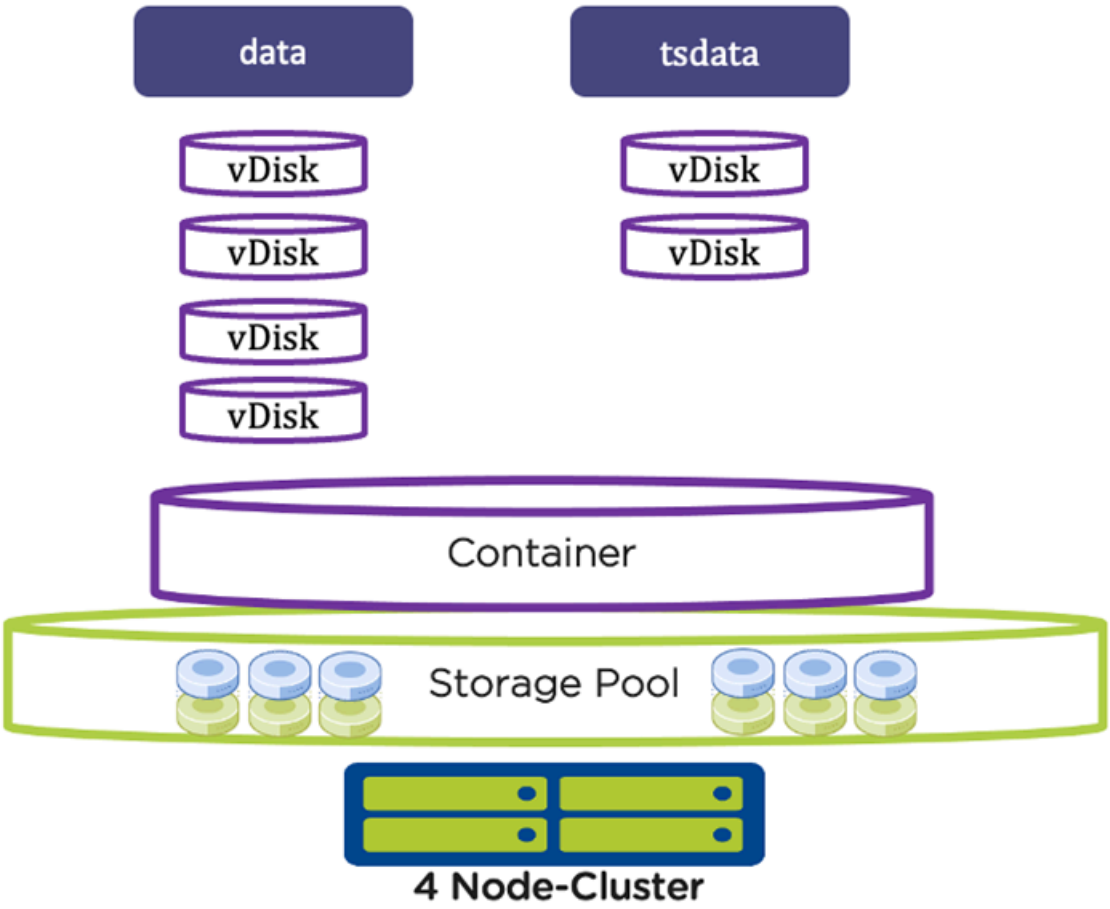


Figure 11: Storage Design for PostgreSQL Database

Example `data` and `tsdata` directories on an NDB PostgreSQL deployment include the following:

- `/pgsql/<Database Name>/data`: the PGDATA location
- `/pgsql/<Database Name>/tsdata`: the data tablespace location

Table: Number of Disks Created by NDB Based on Database Size

Disk Group	Small (<1 TB)	Medium (>1 TB)	Large (>2 TB)
data	2 vDisks	4 vDisks	4 vDisks
tsdata	2 vDisks	2 vDisks	4 vDisks

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2428

PostgreSQL Image Customization During Provisioning

You can use NDB pre and post commands to customize your database deployment. Pre and post commands run as the NDB drive owner, defined when you provision the database VM. This NVD has an NDB drive owner with the username **postgres** and uses a post command script to modify `pg_hba.conf` to configure the IP addresses that could access this PostgreSQL instance. The post command script `postgresql_post.bash` was included in the VM image used to create the software profile to ensure the script was available during deployment.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2429

8. Software Patching with Nutanix Database Service

Nutanix Database Service (NDB) automates the patching process for the OS and database software.

To patch the OS on Linux, NDB issues the update command for the package manager used. For example, if you use RHEL 7.x, NDB runs `yum`. If you use Centos 8.x, NDB runs `dnf`. For OS patching, the software profile must include the proper software repository configuration such that a `yum` update (in the case of Centos 7) performs the required actions.

Patch Microsoft SQL Server Database Software

NDB supports patching for Microsoft SQL Server database instances. Patching for SQL Server is validated on VMs provisioned by NDB (greenfield deployments).

Prepare SQL Server Software Profile Version

To patch SQL Server database server VMs, create a software profile version by uploading a SQL Server update executable in NDB. You can then use the SQL Server update to patch other database server VMs or provision a new database server VM with the updated software profile.

To create a software profile version, follow these steps:

1. In the dropdown list of the main menu, select **Profiles**.
2. Go to Software and open the software profile that you already created.

   For example, open the MSSQL_GoldVM software profile.
3. Click **Create**.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2430

4. In the Create Software Profile Version dialog, configure the following items:
   - **Name**: Enter a name for the software profile version.
   - **Description**: Enter a description for the software profile version.
   - **Patch File Location**:
     - › If your patch file is stored on the local computer, upload the patch file (.exe) from the local computer.
     - › If your patch file is stored in a file share, type the location of the file share that contains the patch file and provide the file share credentials in the **User Name** and **Password** fields.
   - **Patch Notes**: Enter a note to provide additional information about the patch file.
5. Click **Create**.

   Patch files are available for download from the Microsoft Download Center and the Microsoft Update Catalog site. You can provide any SQL Server service pack or cumulative update.
6. Monitor the progress of the operation.

NDB displays the software profile version that you added to the software profile in the list.

Patch a SQL Server Single-Instance Database

To apply updates from the available software profile versions to a provisioned, registered database server VM, follow these steps:

1. In the dropdown list of the main menu, select **Database Server VMs**.
2. Go to **List**.
3. Select the database server VM for the software profile version update.
4. In the Database Server VM Summary dialog, check the Software Profile Version widget.

   The Software Profile Version widget displays the current version, recommended version, and status of the software profile version.
5. Click **Update**.

Note: The Update option only appears when a new software profile version is available.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2431

6. In the Update Database Server VM dialog, configure the following items:
   - Update to Software Profile Version: Select the software profile version (for example, CU15) from the dropdown menu.
   - Start Update: Select **Now**.
   - Pre-Post Commands: Leave this field blank.
   - Provide the database server VM name.
7. Click **Update**.

   A dialog opens that indicates that the operation to update a database has started.
8. In the NDB Operations page, monitor the update progress.
9. Verify the upgrade by running the `select @@version` command again on the database server VM.
10. Ensure that the database hosted on the VM is healthy and active after the upgrade.

Note: The patching process for Microsoft SQL Server database server clusters using NDB is the same.

Patches are applied in a rolling upgrade. Rolling upgrade patching updates the secondary database replica first. After it patches the secondary replica, the rolling upgrade fails the availability group over to the (earlier) secondary replica. After it also patches the last (initial primary) node, the rolling upgrade fails the availability group over again to restore the availability group roles and configuration to its state before the update. This behavior is the default for database server cluster patching in NDB.

Patch Oracle Database Software

For Oracle database updates, NDB uses out-of-place patching. This method allows you to install updates on your template image or one database host, copy Oracle or GRID home, install the updates on one or more target servers, and start the services. Patching for Oracle databases is validated on VMs provisioned by NDB (greenfield deployments).

Prepare Oracle Software Profile Version

To patch an existing database with NDB, generate a new version of the software profile that you used to create the database:

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2432

1. Provision a database VM using an existing software profile version.

   We recommend this method over patching an existing source database or clone database because it minimizes the impact on these databases.

   Provision the database from an Oracle 19.23 RU software profile.
2. Manually patch the grid infrastructure and database software as described in the Oracle documentation accompanying the patch set.
3. In the software profile section of NDB, select the name of the software profile that you must create a new version for.
4. Click **Create**.
5. Enter a name for the new software profile version.
6. Select the VM that you just patched to 19.24.
7. (Optional) In the **Notes** section, enter additional information about the new software profile version.
8. Select the new version in the software profile's overview screen.
9. Click **Update**.
10. Set the status to **Published**.
11. Select the checkbox for the acknowledgment.
12. (Optional) Update the **Notes** section.

Patch an Oracle Single-Instance Database

After you publish the software profile version, the database VMs that can be patched with the new software profile version show an **Update Available** notification in the **Software Profile Version** widget.

To update an Oracle single-instance database VM, follow these steps:

1. In the **Software Profile Version** widget, click **Update**.
2. Choose the new software profile version from the dropdown list.
3. Select whether you want to patch the database VM now or later.

   NDB patches the Oracle software on the chosen database VM.

You can confirm that the patch was successful using NDB, opatch lsinventory, or the database dictionary.

The following output shows the single-instance database software version:

```
Before:
```

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2433

```
Patch description: "Database Release Update : 19.23.0.0.240416 (36233263)"
After:
Patch description: "Database Release Update : 19.24.0.0.240716 (36582781)"

You can get the oracle patch information from DBA_REGISTRY_SQLPATCH:

  PATCH_ID PATCH_TYPE ACTION STATUS  DESCRIPTION
           SOURCE_VERSION TARGET_VERSION
---------- ---------- ------ -------
 ---------------------------------------------------- --------------
 --------------
  36233263 RU      APPLY  SUCCESS Database Release Update : 19.23.0.0.240416
(36233263) 19.1.0.0.0  19.23.0.0.0
  36582781 RU      APPLY  SUCCESS Database Release Update : 19.24.0.0.240716
(36582781) 19.23.0.0.0 19.24.0.0.0
```

The patching process for Oracle Database server clusters using NDB is the same. You can perform the process in either a rolling or nonrolling fashion.

Patch PostgreSQL Database Software

NDB 2.8 supports automated minor version upgrades for PostgreSQL. This Nutanix Validated Design (NVD) tested the upgrade from PostgreSQL 16.6 to 16.8.

Prepare PostgreSQL Software Profile Version

Nutanix recommends using the source code or unzip method to install PostgreSQL, rather than using Linux package managers such as YUM or DNF. If you use a Linux software package manager to install the database engine, patching through NDB isn't supported, including both minor upgrades using a new software profile and patching from outside NDB.

To prepare a software profile to patch PostgreSQL, follow these steps:

1. Register a RHEL 8.10 VM with PostgreSQL version 16.6 installed:

   ```
   $ cat /etc/redhat-release
   Red Hat Enterprise Linux release 8.10 (Ootpa)
   ```

2. Set the VM name to **PostgreSQL16.6**.
3. Create a software profile using this VM.
4. Set the software profile name to **PostgreSQL16.6-SI**.
5. Sign in to the PostgreSQL16.6 VM.
6. Use the source code method to upgrade to PostgreSQL 16.8.
7. Create a software profile update version for the PostgreSQL16.8-SI profile using the PostgreSQL16.6 VM with the upgraded database software.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2434

Patch a PostgreSQL Single-Instance Database

To update a PostgreSQL single-instance database, follow these steps:

1. Click the database server VM, select the instance, and under Software Profile Version, click **Update**.
2. Sign in to the VM.
3. Verify that PostgreSQL 16.8 is running.

The patching process for PostgreSQL database server clusters using NDB is the same.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2435

9. Nutanix AHV High Availability

We performed two high availability validations to measure the effect on a running database workload:

- Unplanned outage: a hardware or software failure that results in the loss of a cluster node.
- Planned outage: the workload management process for a planned upgrade that requires you to restart a cluster node.

For more information on high-availability scenarios and database recoverability options, see the Availability and Resilience section in the documentation for your database:

- SQL Server
- Oracle
- PostgreSQL

Nutanix Database Service Management High Availability

You can configure the Nutanix Database Service (NDB) management plane for high availability. For more information, see NDB High Availability.

AHV High Availability Validation

In this section, we discuss the AHV high availability validation that we conducted on the test cluster to simulate SQL Server database migration. You can apply this process to any other database VMs.

Unplanned SQL Server VM Migration

When unplanned outages occur, AHV automatically restarts VMs affected by a failed node on a surviving node in the cluster. This test timed how long it took for a SQL Server database server VM with 6 vCPUs and 32 GB of memory to automatically resume on

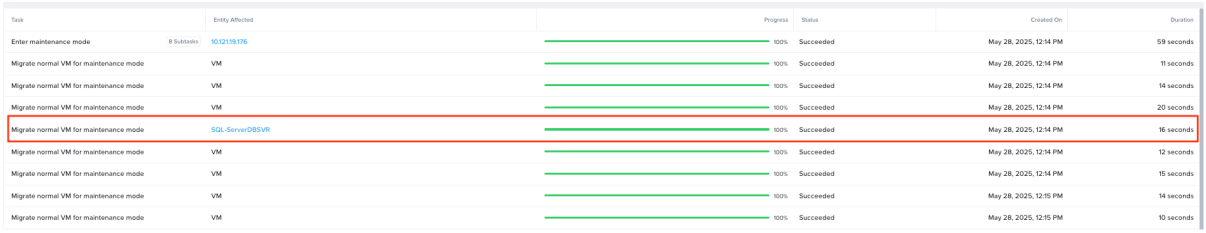
© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2436

another host by pinging from a different VM and running a benchmark task from a client VM that we monitored live. This NVD used the following test procedure:

1. Start with a database server VM running a benchmark workload.
2. Ensure that you enabled high availability for the cluster in Prism Element, then simulate an outage to one of the nodes by putting it in maintenance mode.

   Putting the node in maintenance mode migrates all the VMs to a different node.
3. Measure the time it takes for the migrated VM to respond to pings and the migrated database to accept connections.

The Prism Tasks page indicated that the migration finished in less than 16 seconds.



Task	Entity Affected	Progress	Status	Created On	Duration
Enter maintenance mode 8 Subtasks	10.12.19.176	100%	Succeeded	May 28, 2025, 12:14 PM	59 seconds
Migrate normal VM for maintenance mode	VM	100%	Succeeded	May 28, 2025, 12:14 PM	11 seconds
Migrate normal VM for maintenance mode	VM	100%	Succeeded	May 28, 2025, 12:14 PM	14 seconds
Migrate normal VM for maintenance mode	VM	100%	Succeeded	May 28, 2025, 12:14 PM	20 seconds
Migrate normal VM for maintenance mode	SQL-ServerDBSVR	100%	Succeeded	May 28, 2025, 12:14 PM	16 seconds
Migrate normal VM for maintenance mode	VM	100%	Succeeded	May 28, 2025, 12:14 PM	12 seconds
Migrate normal VM for maintenance mode	VM	100%	Succeeded	May 28, 2025, 12:14 PM	15 seconds
Migrate normal VM for maintenance mode	VM	100%	Succeeded	May 28, 2025, 12:15 PM	14 seconds
Migrate normal VM for maintenance mode	VM	100%	Succeeded	May 28, 2025, 12:15 PM	10 seconds

Figure 12: Unplanned Migration Task in Prism

The database server VM started accepting connections and we reached the VM after 16 seconds (it only missed one beat during the ping test).

During the migration process, the workload maintained full session continuity with no transaction failures observed. The workload with continuous insertion fluctuated during the migration but stabilized within a minute of the live migration finishing. Nutanix advises using high-speed networking infrastructure to ensure optimal performance—even for applications operating in a single VM.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2437

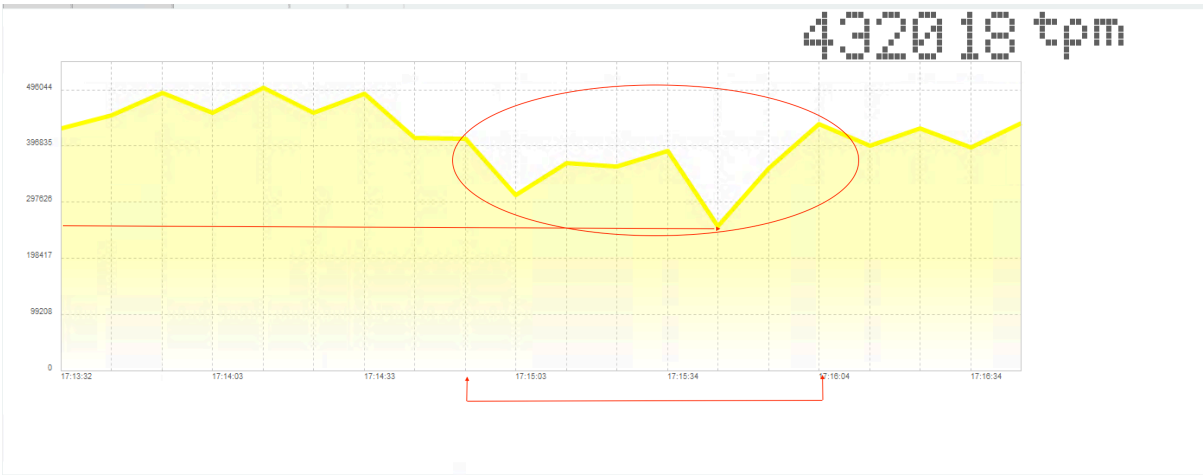


Figure 13: Monitor the Unplanned Migration Process

For more information, see KB-7949.

Planned SQL Server VM Migration

To maintain application availability during cluster maintenance, Nutanix performs rolling upgrades. Nutanix AHV supports hypervisor upgrades by live-migrating running VMs to another node in the cluster before upgrading a node. This NVD measured the effect of a live migration, simulating a rolling upgrade on a SQL Server database VM with 6 vCPUs and 32 GB of memory. We used the following procedure:

1. Start with a database server VM running a workload that continuously runs a benchmark.
2. Live-migrate the database server VM to another node:

```
acli> vm.migrate <vmname> host=<Destination Node IP Address>
```

3. Measure the effect on the benchmark workload during live migration.

The Prism Tasks page indicated that the live migration finished in less than 19 seconds.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2438

Figure 14: Unplanned Migration Task in Prism

The database server VM started accepting connections and we reached the VM after 19 seconds (it only missed one beat during the ping test).

During the migration process, the workload maintained full session continuity with no transaction failures observed. Although the transactions exhibited a small dip, performance stabilized a few seconds after the migration. Nutanix recommends using fast networks to ensure optimal performance, even when an application operates in a single VM.

Figure 15: Monitor the Planned Migration Process

© 2025 Nutanix, Inc. All rights reserved

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2439

For more information, see KB-7949.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2440

10. Nutanix Database Service Time Machine Backup and Recovery

Nutanix Database Service (NDB) uses a time machine to create backups in the form of application-consistent snapshots of a database and copies of database transaction logs. Service-level agreements (SLAs) define backup frequency and how long data is kept. For example, if you set Continuous Duration to 10 days, transaction logs are retained for 10 days from when the first daily snapshot is taken.

Snapshots are available locally in the cluster, so it only takes a few seconds to restore to the last snapshot. Based on the recovery point chosen, NDB restores the vDisks using the appropriate snapshot and applies the transaction logs to bring the database to a consistent state.

NDB time machine backups protect your data from application- and user-related errors, but they don't protect against disasters like a site failure. A comprehensive disaster recovery strategy should include a copy of the data stored in a separate location.

This validation includes database backup and recovery performed using the NDB time machine. To validate using time machine data for backup and recovery, follow these steps:

1. Create a database.
2. Populate the database.
3. Perform a time machine snapshot.
4. Delete a table.
5. Perform an in-place restore of the database using snapshots and logs.

Microsoft SQL Server Backup and Restore Verification

To validate the backup and recovery of a Microsoft SQL Server database using SQL Server Management Studio (SSMS), follow these steps:

1. In SSMS, create two tables.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2441

2. Insert data into the two tables.

   The following output shows the timestamps of when we created the tables and added the data.

   ```
   11:00 - Created two tables
   11:01 - insert primary data - 12000 rows have been inserted into the
    tblauthors table successfully
   11:02 - Inserted secondary data set - verified 20000 rows have been
    inserted to tblbooks
   ```

3. Verify that the time machine schedule creates a snapshot.

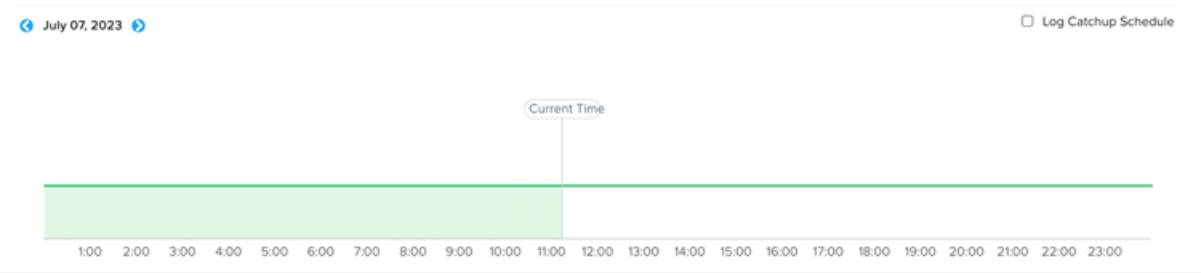


Figure 16: Snapshot Creation with Time Machine

4. Modify the database by inserting 2,000 additional rows into the `tblbooks` table:

   ```
   11:17 - insert 2000 records into the tblbooks table. The tblbooks table
    now contains a total of 22000 rows.
   ```

5. Restore the database to its previous state:

   a. Navigate to the time machine.
   b. Select the time machine you want to use for recovery.

      This Nutanix Validated Design (NVD) example uses the time machine NVD_backuptest2_TM.

6. Click **Actions**.
7. Select **Restore Source Database**.
8. In the Restore Source Database dialog, select **Point in Time** and select a time that is shortly before you modified the database.
9. Under **Restore Location**, select **Original Location**.
10. Click **Restore**.

    NDB uses the earlier snapshot and applies all the logs until right before the change to recover the database.

11. Connect to the VM.
12. Verify that the table has 20,000 rows.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2442

Oracle Database Restore

This validation provisions a new database using NDB a few days before attempting a restore. It applies a custom SLA, NVD_ORACLE_PROD, to back up the database and database transaction log files. The NVD_ORACLE_PROD SLA uses the following retention lengths:

- Continuous log retention: 30 days
- Daily snapshot retention: 7 days
- Weekly snapshot retention: 2 weeks
- Monthly snapshot retention: 2 months
- Quarterly snapshot retention: 1 quarter

For more information on configuring a time machine, see NDB Time Machine Management.

This test scenario used an Oracle single-instance database with a user schema that has a table with data to test the restore functionality by deleting the entire schema.

To find the database size, follow these steps:

1. Use a SQL select statement to query the DBA_SEGMENTS and DBA_TABLES metadata table to get the size of the table and number of rows in the table.

   In this example, we have a table with 617 records and 65,536 bytes:

```
SQL> select dt.OWNER, ds.SEGMENT_NAME, ds.TABLESPACE_NAME, ds.BYTES,
 dt.NUM_ROWS
from dba_tables dt, dba_segments ds
where dt.owner = ds.owner
and dt.table_name = ds.segment_name
and ds.segment_name = 'TIMER';

OWNER          SEGMENT_NAME   TABLESPACE_NAME           BYTES   NUM_ROWS
-------------------- -------------------- ------------------------------
 ---------- ----------
CASETESTER      TIMER       USERS                65536    617
```

2. Drop the user and all its objects:

```
SQL> drop user CASETESTER cascade;
```

3. Confirm that the schema is dropped.

To test how quickly NDB can restore the table, follow these steps:

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2443

1. Sign in to NDB.
2. From the main menu, click **Databases**.
3. Click **Sources**.
4. Select the source database.
5. From the Databases homepage, click **Restore**.
6. In the Restore Source Database dialog, select the **Point in Time** option and select the desired restore point.

   This test case uses a time before the CASETESTER schema was dropped from the database.

   Note: You can only run a point-in-time restore (PITR) if a snapshot and database transaction logs exist.
7. For Restore Location of Data Files, enter the original location of the data files.

   Note: NDB must have a backup of the log you select to facilitate a point-in-time restore operation. If the log is highlighted in yellow, the logs are available but not backed up.

   To manually trigger a log backup, select the **Archive/Online Redo Logs** checkbox and click **Run**.
8. Enter the name of the database.
9. Click **Restore**.

   The restore process begins and the source database becomes unavailable.
10. Monitor the status from the **Operations** tab.
11. Confirm that you restored the schema from DBA_SEGMENTS and DBA_TABLES:

```
select dt.OWNER, ds.SEGMENT_NAME, ds.TABLESPACE_NAME, ds.BYTES,
 dt.NUM_ROWS
from dba_tables dt, dba_segments ds
where dt.owner = ds.owner
and dt.table_name = ds.segment_name
and ds.segment_name = 'TIMER';

OWNER          SEGMENT_NAME   TABLESPACE_NAME           BYTES   NUM_ROWS
------------------- -------------------- ------------------------------
 ---------- ----------
CASETESTER      TIMER       USERS                65536    617
```

PostgreSQL Backup and Restore Validation

To validate the backup and restore process, follow these steps:

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2444

1. Validate the database size:

```
SELECT pg_size_pretty(pg_database_size('tpcc'));
pg_size_pretty
----------------
292 GB
```

2. After the NDB time machine automatically creates the restore point based on the schedule that you defined when you provisioned the VM, check the last recoverable time and the last snapshot.
3. Drop the database.
4. Restore the database to the restore time available in the time machine.
5. Verify that you restored the database:

```
SELECT pg_size_pretty(pg_database_size('tpcc'));
pg_size_pretty
---------------
292 GB
```

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2445

11. Sample Bill of Materials

This validation used the following software and hardware components:

- Nutanix Database Service (NDB) Platform Software License & Mission Critical Software Support Service for 1 CPU Core
- NX-8170-G9
- Nutanix software:
  - Foundation (hypervisor-agnostic installer)
  - Controller VM
  - Prism Management
  - Starter License Entitlement
- Intel Xeon Gold 6442Y @ 2.60 GHz
- 64 GB of memory, 4,800 MT/s DDR5 Synchronous Registered (Buffered)
- SSD-PCIe 3.36 TiB Samsung MZQL23T8HCLS-00A07
- Mellanox 100, 40, 25 GbE, 2-port NIC (Mellanox CX6)
- 24/7 Mission-Critical Level Hardware Support for Nutanix HCI appliance
- C13/C14, 15A, 4 ft power cord
- Services:
  - NDB Deployment and Database Migration - Starter Edition
  - NDB-Enabled Database Automation Pro Service

    Note: Small, medium, and large configurations can use this service.
  - Database Modernization, NDB Deployment

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2446

Note: Because available hardware, software, and services can change without notice, contact Nutanix Sales when ordering to ensure that you have the correct product codes.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2447

12. Database Test Plans

In the following sections, we provide the test plans for Microsoft SQL Server, Oracle, and PostgreSQL databases used in this Nutanix Validated Design (NVD).

SQL Server Test Plans

These test plans contain the validation tasks, expected results, and actual results of this NVD's single-instance SQL Server database tests.

SQL Server Test 1

Register the database server VM to NDB.

Validation tasks:

1. Prepare the VM (OS, SQL Server instance, custom changes, and desired tools; you don’t need the database).
2. Register the database server to NDB (continuous SLA with snapshot and log catchups).

Expected result: The database server registers to NDB without any errors.

Actual results: We registered the template VM (Microsoft SQL Server 2022 (RTM) - 16.0.1000.6 (X64) Enterprise Edition (64-bit)) without any errors.

SQL Server Test 2

Prepare software profile in NDB for provisioning.

Validation task: Create a software profile using the registered template database VM image.

Expected result: The software profile registers without any errors.

Actual result: We created the software profile from the template VM without any errors.

SQL Server Test 3

Add a medium VM compute profile for provisioning.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2448

Validation task: Create a medium compute profile in NDB.

Expected result: The compute profiles are created without any errors.

Actual result: We created medium compute profiles without any errors.

SQL Server Test 4

Add medium database instance parameter profiles in NDB for provisioning.

Validation task: Create a medium database instance parameter profile in NDB.

Expected result: The database instance parameter profiles are created without any errors.

Actual result: We created medium database instance parameter profiles without any errors.

SQL Server Test 5

Create network profiles for SQL Server deployments and select the option for database server VMs.

Validation tasks:

1. In NDB, navigate to Settings > Networks and under Administration, ensure that you added the VLANs.
2. Create a network profile for SQL Server single-instance deployments.
3. Select the database server VMs option.
4. Create a network profile for SQL Server Always On deployments.
5. Select the Windows clusters option.
6. Publish the network profiles.

Expected result: The network profiles are created without any errors.

Actual results:

- We created the validated VLANs in the Nutanix cluster and added them to the NVD networks.
- We created the SQLServer_NVD_MANAGED network profile for SQL Server single-instance provisioning.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2449

- We created the SQLServer_AG_NVD_MANAGED network profile for SQL Server Always On clusters.

SQL Server Test 6

Create snapshot SLAs for production and nonproduction environments based on RPO and RTO.

Validation task: Create an SLA with seven days of daily snapshots and seven days of continuous logs.

Expected result: The SLA is created without any errors.

Actual results: We created the NVD_SQLServer_NONPROD SLA with seven days of daily snapshots and seven days of continuous logs (nonproduction databases).

SQL Server Test 7

Provision a medium database on a VM using NDB. Configure with a continuous SLA with snapshot and log catchups.

Validation task: Provision a medium VM using the software profile (created using the template image) with medium compute, medium database instance parameters, and network and Windows domain profiles.

Expected results:

- All the provisioning operations complete without any errors.
- The SLA is applied to the database on NDB.
- The NDB time machine corresponding to the newly provisioned database performs the scheduled operations without any errors.

Actual results:

- We provisioned the medium database without any errors.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2450

- We verified that the database had the following configurations:
  - Suggested database instance parameter settings (SQL Server maximum memory, degree of parallelism, and so on)
  - Windows power policy set to High Performance
  - Custom OS settings (firewall and remote desktop) from the template VM applied to the new database servers

SQL Server Test 8

This test validates the backup and recovery process: Simulate data loss on the medium database and perform an in-place restore from NDB to recover the data.

Validation tasks:

1. Ensure that the NDB time machine for the test database runs smoothly.
2. Run the snapshots and log catchups to the nearest time.
3. Sign in to the test database (using SQL Server Management Studio) and record the database details (for example, file layout, database schema details, and table row counts).
4. After capturing essential database details, delete one of the tables.
5. Sign in to NDB and perform an in-place restore of the affected database.

Expected results:

- The in-place restore operation completes without any errors.
- Running the dbcc checkdb command on the restored database returns no errors.
- The database schema, layout, and row counts are as expected.

Actual results:

- We restored the medium database.
- After the dbcc checkdb ran, we verified the table row counts.

SQL Server Test 9

This test validates Nutanix zero-byte cloning: Create a point-in-time clone of a registered database on a new database server.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2451

Validation tasks:

1. Ensure that the database time machine runs without any issues.
2. Deploy a script to add a row (with a timestamp) to a test table in the test database every second.
3. Trigger a log catchup of the specific database and wait for it to complete.
4. Perform a point-in-time clone of the database to a new database server.

Expected results:

- The point-in-time clone operation finishes without any errors.
- The latest row of the timestamp table of the test database matches the point-in-time value selected during cloning.

Actual results:

- The point-in-time clone to a new database server finished without any errors.
- The point-in-time value we chose during the operation and the last logged data entry in the test database matched.

SQL Server Test 10

Use the snapshot to create a clone of a registered database on an existing database server.

Validation tasks:

1. Ensure that the database time machine runs without any issues.
2. Deploy a script to add a row (with a timestamp) to a test table in the test database every second.
3. Trigger a snapshot on the time machine and wait for it to finish.
4. Use the snapshot to clone the database to an existing database server.

Expected results:

- The clone operation finishes without any errors.
- The latest row of the timestamp table of the test database matches the snapshot time selected during cloning.

Actual results:

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2452

- We cloned the snapshot to an existing database server without any errors.
- The snapshot chosen during the operation matched the end time of the snapshot operation in NDB, and the last logged data entry in the test database matched the time of the Freeze Database and Perform Snapshot step in the NBD snapshot operation.

SQL Server Test 11

Simulate a data change on the cloned VM and perform a clone refresh from the source database time machine.

Validation tasks:

1. Create a clone of the test database (or reuse an existing clone).
2. Connect to the source database (using SQL Server Management Studio) and make a change (for example, add a new table).
3. Perform a snapshot or initiate a manual log catchup for NDB to capture the changes on the source database.
4. Sign in to NDB and perform a clone refresh of the associated clone.

Expected results:

- The clone refresh operation finishes without any errors.
- The clone database reflects the change performed on its source database.

Actual results:

- We refreshed the clone without any errors.
- We verified that the last logged data record entry on the cloned database (before refresh) and the data record entry after the refresh matched.

SQL Server Test 12

Apply a SQL Server update to the database server VM.

Validation tasks:

1. Sign in to NDB and provision a SQL Server database (with a database server) using the software profile (or reuse if a provisioned database is already using the software profile).
2. Upload a SQL Server patch file to the specific software profile.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2453

3. Upgrade the database server that you provisioned from the specific software profile.

Expected results:

- The upgrade of the database server finishes without any errors.
- The time machine associated with the upgraded database server continues to function normally as before the upgrade.
- Connect to the upgraded database server instance or database and confirm the upgrade by running `select @@version`.

Actual result: We updated the database server without any errors.

- SQL Server version before applying patch: Microsoft SQL Server 2022 (RTM) - 16.0.1000.6 (X64)
- SQL Server version after applying patch: Microsoft SQL Server 2022 (RTM-CU18) (KB5050771) - 16.0.4185.3 (X64)

SQL Server Test 13

Provision an Always On clustered database using NDB with a continuous SLA including snapshot and log catchups.

Validation task: Provision a database on a new two-node (synchronous commit with automatic failover) Always On cluster using the software profile (created using the database server VM image), compute, network, database instance parameter, and Windows domain profiles.

Expected results:

- The provisioning operation finishes without any errors.
- The SLA is applied to the database on NDB.
- The NDB time machine corresponding to the newly provisioned databases performs the scheduled operations without any errors.

Actual results:

- We provisioned the two-node Always On availability group (AG) cluster without any errors.
- We set up the two synchronous replicas with automatic failover enabled.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2454

- The health of the AG cluster was green.
- We verified that the database had the following configurations:
  - Suggested database instance parameter settings (for example, SQL Server maximum memory and degree of parallelism)
  - Windows power policy set to High Performance
  - Custom OS settings (firewall and remote desktop) from the template VM applied to the new database servers

---

Oracle Test Plans

The following test plans contain the validation tasks, expected results, and actual results of this NVD's Oracle database tests.

Oracle Test 1

Run the database server registration prerequisites script (Linux).

Validation tasks:

1. Download the script from NDB and copy it to the database server.
2. Run the registration prerequisites script.

   For more information, see Running the Prerequisites Script (Linux).

Expected result: Database server VM meets all the requirements for NDB registration.

Actual result: The machine satisfied the dependencies required by NDB and could be onboarded.

Oracle Test 2

Register a template image using NDB.

Validation tasks:

1. Prepare a template image VM by installing the Oracle Grid Infrastructure and Database software.
2. Register the database server and database in NDB (continuous SLA with snapshot and log catchups).

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2455

Expected results:

- The database and database server register in NDB without any errors.
- The time machine operations (snapshot, log catchup, and curations) progress without any errors.

Actual result: We registered the database server VM.

Oracle Test 3

Prepare a software profile in NDB for provisioning.

Validation tasks:

1. Create a software profile for Oracle deployments using the registered VM from Oracle Test 2.
2. Publish this software profile.

Expected result: Database software profile creation succeeds without error messages.

Actual result: We created and published a software profile.

Oracle Test 4

Add medium database compute profiles in NDB for provisioning.

Validation task: Create medium compute profiles in NDB.

Expected result: Compute profile creation succeeds without any errors.

Actual result: We created compute profiles for medium Oracle Single-Instance, High Availability (SIHA) and RAC databases.

Oracle Test 5

Add a medium database parameter profile in NDB for provisioning.

Validation task: Create medium database parameter profile in NDB.

Expected result: Database parameter profile creation succeeds without any errors.

Actual result: We created a database parameter profile based on a medium compute profile for Oracle SIHA and RAC databases.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2456

Oracle Test 6

Create network profiles for Oracle deployments.

Validation tasks:

1. In NDB, navigate to Settings > Networks and under Administration, ensure that you added the VLANs.
2. Create a network profile for Oracle SIHA deployments.
3. Create a network profile for Oracle RAC deployments.
4. Publish the network profiles.

Expected result: Network profile creation succeeds without any errors.

Actual results:

- We created the validated VLANs in the Nutanix cluster and added them to the NVD networks.
- We created the ORACLE_NVD_MANAGED network profile for Oracle SIHA provisioning.
- We created the ORACLE_RAC_NVD profile for Oracle RAC provisioning.

Oracle Test 7

Create SLAs for production and nonproduction environments based on RPO and RTO.

Validation tasks:

1. Create an SLA with 30 days of clearance.
2. Create an SLA with seven days of clearance.
3. Create an SLA with no clearance.

Expected result: The SLAs are created without any errors.

Actual results:

- We created the NVD_ORACLE_PROD SLA with 30 days of clearance for critical databases.
- We created the NVD_ORACLE_NONPROD SLA with seven days of clearance for nonproduction databases.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2457

- We created the NVD_ORACLE_NONE SLA with no clearance for noncritical databases that don’t require PITR operations.

Oracle Test 8

Provision medium database VMs using NDB.

Validation task: Provision a medium VM using the Oracle software profile (created using the template image), the medium compute profile, the network profile, and the medium database parameter profile. Create the software profile for this validation with udev rules.

Expected results:

- All the provisioning operations succeed without any errors.
- The SLAs apply to the databases on NDB.
- The NDB time machines that correspond to the newly provisioned databases perform the scheduled operations without any errors.

Actual result: We provisioned a medium SIHA database.

Oracle Test 9

Provision medium RAC database VMs using NDB.

Validation task: Provision a medium VM using the Oracle software profile (created using the template image), the medium compute profile, the RAC network profile, and the medium database parameter profile.

Expected results:

- All the provisioning operations finish without any errors.
- The SLAs apply to the databases on NDB.
- The NDB time machines corresponding to the newly provisioned databases perform the scheduled operations without any errors.

Actual result: We provisioned a medium RAC database.

Oracle Test 10

Simulate data loss on a database and restore in-place from NDB to recover the data.

Validation tasks:

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2458

1. Ensure that the NDB time machine for the test database runs smoothly and run the snapshots and log catchups to the nearest time.
2. Sign in to the test database and record the schema size and the number of records in the table:

```
SQL> create user CaseTester identified by cases default tablespace Users;

User created.

SQL> ALTER USER CaseTester QUOTA UNLIMITED ON users;

User altered.

SQL> GRANT CREATE SESSION TO CaseTester;

Grant succeeded.

SQL> GRANT CREATE TABLE, CREATE SEQUENCE, CREATE TRIGGER, CREATE VIEW,
 CREATE PROCEDURE,CREATE SYNONYM to CaseTester;

Grant succeeded.

SQL> GRANT EXECUTE ON DBMS_LOCK TO caseTester;

Grant succeeded.

SQL> connect caseTester

SQL> CREATE TABLE timer ( id NUMBER PRIMARY KEY, inserted_at TIMESTAMP
 DEFAULT SYSDATE ) TABLESPACE Users;

Table created.

SQL> CREATE SEQUENCE timer_seq START WITH 1 INCREMENT BY 1;

Sequence created.

SQL> CREATE OR REPLACE TRIGGER timer_trigger
BEFORE INSERT ON timer
FOR EACH ROW
BEGIN
  :NEW.id := timer_seq.NEXTVAL;
END;
/

Execute PL/SQL Anonymous block to insert rows with timestamp
 continuously :
```

3. Using an anonymous block, begin a simple loop inserting data into the TIMER table.
4. Commit every insert.
5. Use the DBMS_LOCKSLEEP(1) package from Oracle to sleep for 1 second then continue.

   The loop continues inserting data until you stop it with Ctrl + C.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2459

6. Interrupt and check the count:

```
SQL> select count(*) from timer;

  COUNT(*)
----------
  8

SQL> select * from timer where id = 8;

 ID    INSERTED_AT
---------- ---------------------------------------------
  8     08-MAY-25 07.57.42.000000 PM
```

7. Connect to the Oracle Database schema and run count(*) on a table that you intend to drop for the simulation:

```
SQL> select count(*) from timer;

  COUNT(*)
----------
  8

SQL> select * from timer where id = 8;

 ID    INSERTED_AT
---------- ------------------------------------------
  8     08-MAY-25 07.57.42.000000 PM
```

8. Record the essential details, then delete the table and capture the timestamp for PITR:

```
SQL> drop table timer;

Table dropped.
```

9. Verify that the table was dropped:

```
SQL> select * from timer;
select * from timer
         *
ERROR at line 1:
ORA-00942: table or view does not exist
```

10. Sign in to NDB and perform an in-place restoration of the affected database from the timestamp.
11. Verify that you restored the schema objects and table data:

```
SQL> select * from timer where id = 8;

 ID    INSERTED_AT
---------- ---------------------------------------------
  8     08-MAY-25 07.57.42.000000 PM
```

Expected results:

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2460

- The in-place restore operation finishes without any errors.
- The database schema, layout, and row counts are recorded before the simulated data loss and after the restore operation by NDB.

Actual result: We successfully restored user data using NDB's restore functionality.

Oracle Test 11

Create a point-in-time clone of the VM on a new database server.

Validation tasks:

1. Ensure that the database time machine runs without any issues.
2. Perform a point-in-time clone of the database to a new database VM.

Expected results:

- The point-in-time cloning process finishes without any errors.
- Querying the database matches the point-in-time value selected during cloning.

Actual result: The clone operation from the source database to a new database server VM using the time machine's point-in-time functionality succeeded.

Oracle Test 12

Use a snapshot to create a clone of a VM on an existing database server.

Validation tasks:

1. Ensure that the database time machine runs without any issues.
2. Deploy a script to add a row (with a timestamp) every second to a test table.

   For example, the table TIMER has a column called ID and another called VALUES (null).

   a. Using an anonymous block, begin a simple loop inserting data into the TIMER table.
   b. Commit every insert.
   c. Use the DBMS_LOCKSLEEP(1) package from Oracle to sleep for 1 second then continue.

      The loop continues inserting data until you stop it with Ctrl + C.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2461

3. Trigger a snapshot on the time machine and wait for it to finish.
4. Use the snapshot to clone the database to a database server.

Expected results:

- The snapshot operation finishes without any errors.
- The latest row of the timestamp table in the test database matches the snapshot time selected during cloning.

Oracle Test 13

Simulate data change on the cloned VM and perform a clone refresh from the source database time machine.

Validation tasks:

1. Create a clone of the test database (or reuse an existing clone).
2. Connect to the source database (using SQL*Plus) and make a change (for example, add a new table).
3. Sign in to NDB and refresh the associated clone.

Expected results:

- The clone refresh operation finishes without any errors.
- The clone database reflects the change made to its source database.

Actual results:

- For this test, we created a new table on the source database. NDB refreshed the clone databases (cloned from PROD). The clone database was validated and the new added table was available.
- We verified the new table, the number of rows in the table, and the size of the table on the cloned database.

PostgreSQL Test Plans

These test plans contain the validation tasks, expected results, and actual results of this NVD's PostgreSQL database tests.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2462

PostgreSQL Test 1

Run the database server registration prerequisite script (Linux).

Validation tasks:

1. Download the script from NDB and copy it to the database server.
2. Run the script (for detailed instructions, see Running the Prerequisites Script (Linux)).

Expected result: Database server VM meets all the requirements for NDB registration.

Actual result: This machine satisfied the dependencies required by NDB.

PostgreSQL Test 2

Register a template image using NDB.

Validation tasks:

1. Prepare a template image VM by installing the PostgreSQL Database software.
2. Register the database server and database in NDB (continuous SLA with snapshots and log catchups).

Expected results:

- Database and database server register in NDB without any errors.
- The time machine operations (snapshot, log catchup, curations) progress without any errors.

Actual result: We registered the database server VM.

PostgreSQL Test 3

Prepare a software profile in NDB for provisioning.

Validation tasks:

1. Create a software profile for PostgreSQL deployments using the registered VM from PostgreSQL Test 2.
2. Publish this software profile.

Expected result: Database software profile creation succeeds without any error messages.

Actual result: We created and published the software profile.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2463

PostgreSQL Test 4

Add a medium compute profile in NDB for provisioning.

Validation task: Create a medium compute profile in NDB.

Expected result: Compute profile creation succeeds without any errors.

Actual result: We created a medium compute profile for single-instance and high-availability PostgreSQL databases.

PostgreSQL Test 5

Add medium database parameter profiles in NDB for provisioning.

Validation task: Create medium database parameter profiles in NDB.

Expected result: Database parameter profile creation succeeds without any errors.

Actual result: We created medium database parameter profiles for single-instance and high-availability PostgreSQL databases.

PostgreSQL Test 6

Create network profiles for PostgreSQL deployments.

Validation tasks:

1. In NDB, navigate to Settings > Networks and under Administration, ensure that you added the VLANs.
2. Create a network profile for PostgreSQL deployments.
3. Create a network profile for PostgreSQL high availability deployments.
4. Publish the network profiles.

Expected result: Network profile creation succeeds without any errors.

Actual results:

- Validated VLANs are created in the Nutanix cluster and added to NVD Networks.
- Created the PostgreSQL_NVD_MANAGED network profile for PostgreSQL provisioning.
- Created the PostgreSQL_HA_NVD profile for PostgreSQL high availability provisioning.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2464

PostgreSQL Test 7

Create SLAs for production and nonproduction environments based on RPO and RTO.

Validation tasks:

1. Create an SLA with 30 days of clearance.
2. Create an SLA with 7 days of clearance.
3. Create an SLA with no clearance.

Expected result: The SLAs are created without any errors.

Actual results:

- We created the NVD_PostgreSQL_PROD SLA with 30 days of clearance for critical databases.
- We created the NVD_PostgreSQL_NONPROD SLA with 7 days of clearance for nonproduction databases.
- We created the NVD_PostgreSQL_NONE SLA with no clearance for noncritical databases that don’t require PITR.

PostgreSQL Test 8

Provision medium single-instance database VMs using NDB.

Validation task: Provision a medium VM using the PostgreSQL software profile (created using the template image), the medium compute profile, the network profile, and the medium database parameter profile.

Expected results:

- All the provisioning operations finish without any errors.
- The SLAs are applied to the databases on NDB.
- The NDB time machines corresponding to the newly provisioned databases perform the scheduled operations without any errors.

Actual result: We provisioned medium single-instance databases.

PostgreSQL Test 9

Provision medium high-availability database VMs using NDB.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2465

Validation task: Provision a medium VM using the PostgreSQL high availability software profile (created using the template image), the medium compute profile, the high availability network profile, and the medium database parameter profile.

Expected results:

- All the provisioning operations finish without any errors.
- The SLAs are applied to the databases on NDB.
- The NDB time machines corresponding to the newly provisioned databases perform the scheduled operations without any errors.

Actual result: We provisioned medium high-availability databases.

PostgreSQL Test 10

Simulate data loss on a database and restore in-place from NDB to recover the data.

Validation tasks:

1. Ensure that the NDB time machine for the test database runs smoothly and run the snapshots and log catchups to the nearest time.
2. Sign in to the test database and record the database size.
3. Drop the test database.
4. Run a select database size command on the dropped table.
5. Sign in to NDB and perform an in-place restoration of the affected database from the timestamp.
6. Validate the table and table data.

Expected results:

- The in-place restore operation finishes without any errors.
- The database is captured before the simulated data loss.

Actual result: We restored the database using NDB's restore functionality with PITR.

PostgreSQL Test 11

Create a point-in-time clone of a VM on a new database server.

Validation tasks:

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2466

1. Ensure that the database time machine is running without any issues.
2. Deploy a script to add a row (with a timestamp) to a test table in the test database every second.
3. Trigger a log catchup for the specific database and wait for it to finish.
4. Perform a point-in-time clone of the database to a new database VM.

Expected results:

- The point-in-time clone operation finishes without any errors.
- The latest row of the timestamp table in the test database matches the point-in-time value selected during cloning.

Actual result: The clone operation from the source database to a new database server VM using the time machine's point-in-time functionality succeeded.

PostgreSQL Test 12

Use a snapshot to create a clone of a VM on a database server.

Validation tasks:

1. Ensure that the database time machine is running without any issues.
2. Deploy a script to add a row (with a timestamp) to a test table called TIMER every second.

   For example, the table TIMER has a primary key called ID and TIMESTAMP as the default `insert now()` value.

   a. Run `$$` and begin a loop.
   b. Insert the default values into the TIMER table.
   c. Commit every insert.
   d. Use the pg_sleep(1) function from PostgreSQL to sleep for 1 second then continue.

   The loop continues inserting data until you stop it with Ctrl + C.
3. Trigger a snapshot on the time machine and wait for it to finish.
4. Use the snapshot to clone the database to a database server.

Expected results:

- The snapshot operation finishes without any errors.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2467

- The latest row of the timestamp table in the test database matches the snapshot time selected during cloning.

PostgreSQL Test 13

Simulate data change on a cloned VM and perform a clone refresh from the source database time machine.

Validation tasks:

1. Create a clone of the test database (or reuse an existing clone).
2. Connect to the source database (psql) and make a change (for example, add a new table).
3. Sign in to NDB and perform a clone refresh of the associated clone.

Expected results:

- The clone refresh operation finishes without any errors.
- The clone database reflects the change made to its source database.

Actual results:

- We created a table on the source database and NDB refreshed its clone databases.
- We validated the new table and size on the clones.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2468

13. References

1. Microsoft SQL Server Database Workloads on Nutanix
2. Microsoft SQL Server on Nutanix Best Practices
3. Oracle on Nutanix Best Practices
4. PostgreSQL on Nutanix Best Practices
5. Hybrid Cloud: AOS 6.5 with AHV On-Premises Design

© 2025 Nutanix, Inc. All rights reserved

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2469

About Nutanix

Nutanix offers a single platform to run all your apps and data across multiple clouds while simplifying operations and reducing complexity. Trusted by companies worldwide, Nutanix powers hybrid multicloud environments efficiently and cost effectively. This enables companies to focus on successful business outcomes and new innovations. Learn more at Nutanix.com.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2470

List of Figures

Figure 1: Nutanix Platform for Databases Architecture..... 8
Figure 2: Nutanix Database Service Features..... 9
Figure 3: Nutanix Database Service Architecture..... 11
Figure 4: Sample Four-Node Cluster Hosting SQL Server Databases on Nutanix..... 20
Figure 5: Securing an Application..... 24
Figure 6: Prism Central Security Policy Example..... 26
Figure 7: Hybrid Cloud On-Premises Monitoring Conceptual Design..... 29
Figure 8: Hybrid Cloud Performance Metrics Systems..... 30
Figure 9: SQL Server Database Example Disk File System..... 40
Figure 10: Logical and Physical Design for Oracle Database..... 42
Figure 11: Storage Design for PostgreSQL Database..... 45
Figure 12: Unplanned Migration Task in Prism..... 54
Figure 13: Monitor the Unplanned Migration Process..... 55
Figure 14: Unplanned Migration Task in Prism..... 56
Figure 15: Monitor the Planned Migration Process..... 56
Figure 16: Snapshot Creation with Time Machine..... 59

Prism Central Infrastructure Guide

Prism pc.2024.3

January 29, 2025

NUTANIX

Contents

About this Publication.....8

Prism Central Documentation Portfolio.....10

Related Documentation..... 11

Getting Started..... 12

Prism Central Deployment..... 12
- Requirements for Prism Central Deployment.....14
- Limitations of Prism Central Deployment.....15
- Deploy Multiple Prism Central Instances on a Prism Element Cluster..... 15
- Prism Central Installation..... 16
- Prism Central Upgrade.....27
- Service Manager for Installing Services and Applications..... 36

Prism Central Overview..... 38
- Logging Into Prism Central..... 39
- Prism Central Landing Page..... 41
- Application Switcher Function..... 45
- Prism Central Settings (Infrastructure).....49
- Understanding Displayed Statistics.....51
- Infrastructure Overview.....52
- Admin Center Overview..... 53
- Prism Central GUI Organization.....54

Prism Licensing..... 59

X-Small Prism Central.....60

Registering or Unregistering a Cluster with Prism Central..... 61
- Unregistering from Prism Central.....63

Application-specific Navigation Bar.....66

Searching for Information.....70

Main Dashboard - Infrastructure..... 80

Dashboard Management.....82
- Resetting Dashboard.....84
- Setting Data Density.....85
- Creating a New (Custom) Dashboard.....85
- Modifying a Dashboard..... 87
- Sharing a Dashboard..... 88
- Generating a Dashboard Summary Report..... 92

Widgets Management.....95
- Adding Dashboard Widgets.....98

Compute Entities.....103

VM Management..... 103
- VMs Summary View.....104

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2473

VM Details View....117
Creating a VM through Prism Central (AHV)....130
Managing a VM through Prism Central (AHV)....143
Adding Multiple vGPUs to the Same VM....156
VM Migration Specifications....157
Creating a VM through Prism Central (ESXi)....170
Managing a VM through Prism Central (ESXi)....172
Nutanix Guest Tools....173
Storage Quality of Service (QoS)....194
Memory Overcommit Management....196
Policies for VM Management....196
VM Template Management....196
VM Template Summary View....196
VM Template Details View....198
Limitations of VM Template Feature....201
Creating a VM Template....201
Deploying VM from a Template....204
Managing a VM Template....207
Kubernetes Clusters Management....210
Kubernetes Clusters Summary View....211
Kubernetes Cluster Details View....212
OVA Management....219
OVAs Summary View....220
Exporting a VM as an OVA....222
Uploading an OVA....223
Concatenating Upload using APIs....230
Deploying an OVA as VM....233
Downloading an OVA....240
Renaming an OVA....240
Deleting an OVA....241
Image Management....242
Images Summary View....243
Image Details View....246
Requirements....247
Limitations....247
Adding an Image....248
Image Upload Verification....263
Modifying an Image....264
Importing Images to Prism Central....265
Policies for Image Management....266
Catalog Management....266
Catalog Items Summary View....266
Adding a Catalog Item....268
Deleting a Catalog Item....270

Storage Entities....272
Storage Container Management....272
Storage Containers Summary View....273
Storage Container Details View....279
Storage Components....284
Storage Efficiency....286
Capacity Reservation Best Practices....293
Limitations for Storage Containers....294
Creating a Storage Container....294
Modifying a Storage Container....299

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2474

Deleting a Storage Container....301
Volume Group Management....301
Volume Groups Summary View....302
Volume Group Details View....307
Creating a Volume Group....315
Modifying a Volume Group....321
Configuring Mutual CHAP Authentication....324
Attaching Volume Groups to Guest VMs....325
Cluster RBAC for Volume Group....325
External vCenter Server Integration....326
External vCenter Datastores Summary View....327
External vCenter Datastore Details View....332
Registering External vCenter Server (Prism Central)....336
Unregistering a Cluster from the External vCenter Server (Prism Central)....339
Managing External vCenter Server Registration Changes (Prism Central)....340

Network and Security Entities....341
Subnets....341
Subnets Summary View....342
Subnet Details View....344
Network Configuration....346
Virtual Private Clouds....356
Virtual Private Clouds Summary View....357
Virtual Private Cloud Details View....358
Traffic Mirroring....363
Traffic Mirroring Summary View....364
Traffic Mirroring Details View....366
Creating a Traffic Mirroring Session....368
Disabling a Traffic Mirroring Session....373
Enabling a Traffic Mirroring Session....374
Updating a Traffic Mirroring Session....374
Deleting a Traffic Mirroring Session....375
Traffic Mirroring Session Alerts....375
Role-Based Access Control in Traffic Mirroring....375
Floating IPs....376
Floating IPs Summary View....376
Connectivity....378
Gateways Summary View....378
Gateway Details View....379
VPN Connections Summary View....381
VPN Connection Details View....383
Subnet Extensions Summary View....386
Subnet Extension Details View....387
BGP Sessions Summary View....390
BGP Session Details View....391
Security Policies....394
Security Dashboard....394

Data Protection and Recovery Entities....395
Protection Summary....395
Protection Policies....395
Recovery Plans....395
VM Recovery Points....395
VG Recovery Points....395

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2475

Consistency Groups..... 395

Hardware Entities..... 396
Cluster Management..... 396
Clusters Summary View..... 398
Cluster Details View..... 405
Creating a Cluster..... 409
Destroying a Cluster..... 411
Managing Cluster Fault Tolerance..... 412
Settings Profile for Clusters..... 413
Host Management..... 418
Hosts Summary View..... 419
Host Details View..... 423
Renaming an AHV Host..... 428
Expanding a Cluster through Prism Central..... 428
Removing a Node through Prism Central..... 435
Putting a Host into Maintenance Mode Using Prism Central..... 436
Exiting a Host from Maintenance Mode Using Prism Central..... 437
Disks Summary View..... 438
Disk Details View..... 442
GPUs Summary View..... 444
GPU Details View..... 445

Activity Entities – Alert and Event Monitoring..... 448

Activity Entities – Tasks and Audits..... 449
Audits Summary View..... 449
Audit Details View..... 451
Tasks View..... 452

Operations Entities..... 455

Administration Entities..... 456
Availability Zones..... 456
Category Management..... 456
Categories Summary View..... 457
Category Details View..... 458
Creating a Category..... 459
Modifying a Category..... 460
Assigning a Category..... 460

Policies in Infrastructure..... 463
VM Policy Management..... 463
VM-Host Affinity Policies Defined in Prism Central..... 463
VM-VM Anti-Affinity Policies Defined in Prism Central..... 474
NGT Policies..... 484
Image Policy Management..... 487
Image Placement Policies..... 488
Bandwidth Throttling Policies..... 496
Security Policy Management..... 501

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2476

Security Policies Summary View....501
Security Policy Details View....505
Storage Policy Management....506
Default Storage Policy....509
Storage Policies Summary View....511
Storage Policy Details View....514
Storage Policy Compliance....518
Storage Policy Based Replication Factor....519
Storage Policy Based Encryption....519
Creating a Storage Policy....520
Managing Storage Policies....525
Deleting a Storage Policy....527

Prism Self Service Administration....530
Prism Self Service Setup....530
Creating a VM (Self Service)....532
Creating a VM from Catalog Items (Self Service)....532
Managing a VM (Self Service)....539
Assigning a VM to a Project Member....539

Additional Operations....542
Managing Prism Central....542
Microservices Infrastructure....545
Prism Central Backup, Restore, and Migration....556
Intelligent Operations....566
Large Files Upload Using Objects Lite....567
Objects Lite Data Storage....567
Objects Lite Limitations....567
Objects Lite Access....567
High Availability in Prism Central....570
Finding the Prism Central Version....571
Finding the AHV Version on Prism Central....571
Finding the AOS Version Using Prism Central....572
Expanding (Scale Out) Prism Central....573
Shutting Down or Starting Up Prism Central VM....578
Shutting down or starting up all the PC VMs in a Prism Central Configuration....578
Shutting down or starting up a single PC VM in a scale-out PC configuration....579
Keyboard Shortcuts in Prism Central....579
IP Address Reconfiguration....580
Preparing to Reconfigure the IP Address and Gateway of PC VMs....580
Reconfiguring the IP Address and Gateway of Prism Central VMs....581
Logging Out of Prism Central....584

Customer Support Services....585
Configuring Remote Connection Using CLI....585
Creating a Support Case....586
Viewing Case Status....589
Accessing the Nutanix Support Portal (Prism Central)....590
Accessing the REST API Explorer....593

Help Resources....594
Accessing Online Help (Prism Central)....594

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2477

Accessing the Nutanix Next Community....595
Glossary....596

Copyright....597

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2478

ABOUT THIS PUBLICATION

This document provides the information about how to set up the site infrastructure using Prism Central.

- For information about all the documents applicable for Prism Central, see Prism Central Documentation Portfolio on page 10.
- For information about how to access this document using online help option, see Accessing Online Help (Prism Central) on page 594.
- To access other Nutanix documents, see Nutanix support portal.

Scope of the Document

The scope of this document is limited to describe the following infrastructure-specific attributes and operations that you can perform using Prism Central:

- Monitor and Analyze system performance using exhaustive Dashboard. For more information, see Main Dashboard - Infrastructure on page 80.
- Compute and Storage Settings. For more information, see Compute Entities on page 103.
- Network and Security Settings. For more information, see Network and Security Entities on page 341.
- Data Protection and Recovery Settings. For more information, see Data Protection and Recovery Entities on page 395.
- Checking the Hardware Entities and managing Hosts. For more information, see Hardware Entities on page 396.
- Checking Alerts and Events for fault management. For more information, see Activity Entities – Alert and Event Monitoring on page 448.
- Checking ongoing and completed tasks and performing system Audits. For more information, see Activity Entities – Tasks and Audits on page 449.
- Performance Monitoring, Application Discovery, and Reports Management. For details, see Operations Entities on page 455.
- Define policies for configuration ease. For more information, see Policies in Infrastructure on page 463.
- Additional operations that include how to find the Prism Central version, AHV version, AOS version, shutdown Prism Central, perform disaster recovery, reconfigure Prism Central IP address and gateway, pair Availability Zones (AZ), logout from Prism Central, and use keyboard shortcuts. For more information, see Additional Operations on page 542.
- Prism Central self service setup. For more information, see Prism Self Service Administration on page 530.
- Customer support services from Nutanix for Prism Central. For more information, see Customer Support Services on page 585.

For a quick overview about all the infrastructure-related operations that you can perform through Prism Central, see Infrastructure Overview on page 52.

The admin-related operations are covered in the *Prism Central Admin Center Guide*. For information about how the Prism Central documentation is organized, see Prism Central Documentation Portfolio on page 10.

For a quick overview about all the admin-related operations that you can perform through Prism Central, see Admin Center Overview on page 53.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2479

Intended Audience

The intended audience for this document are the site personnels, customer's operation teams and any tier or individual entity defined by the customer who is equipped to perform the site configurations and modifications. In addition to this, any individual with an intention to learn and develop understanding about Prism Central usage, can refer this document.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2480

PRISM CENTRAL DOCUMENTATION PORTFOLIO

The following table describes how Prism Central documentation portfolio is organized:

Table 1: Prism Central Documentation Portfolio

Deliverable Name	Description
Prism Central Admin Center Guide	This document describes all the administrative-level tasks that you can perform from Prism Central using **Admin Center** application. For more information about **Admin Center** application, see Admin Center Overview on page 53. For more information about how to access the **Admin Center** application in Prism Central, see Application Switcher Function on page 45.
Prism Central Alerts and Events Reference Guide	This document describes how to manage alerts and events management from Prism Central. The Alerts and Events generated in Prism Central enables you to perform the fault management related operations.
Prism Central Infrastructure Guide	This document describes all the field-specific settings required to host a cluster in Prism Central. It covers all the operations that you can perform from Prism Central using **Infrastructure** application. For more information about **Infrastructure** application, see Infrastructure Overview on page 52. For more information about how to access the **Infrastructure** application in Prism Central, see Application Switcher Function on page 45.
Intelligent Operations Guide	This document describes the Prism Central intelligent operations functionality, and how to enable, disable, and perform configurations related to Intelligent Operations part of Cloud Manager module.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2481

RELATED DOCUMENTATION

The Nutanix Support Portal provides software download pages, documentation, compatibility, and other information.

> **Note:** For information about the ports that are used by Prism Central, Microservices Infrastructure, and other Nutanix Software, see Ports and Protocols.
>
> On the Ports and Protocols page, select the appropriate software or application such as **Prism Central** or **Microservices Infrastructure** in the **Software Type** dropdown menu to view the ports and protocols used by that Nutanix software or application.

Documentation	Description
Release Notes | Flow Virtual Networking	Flow Virtual Networking Release Notes
Port And Protocols	Port Reference: See this page for details of ports that must be open in the firewalls to enable Flow Virtual Networking to function.
Nutanix Security Guide	Prism Element and Prism Central security, cluster hardening, and authentication.
Flow Network Security Next Gen	Flow Network Security Next-Gen is the next-generation Nutanix microsegmentation solution with an enhanced policy model, advance policy operation, and enterprise readiness features. FNG
AOS guides and release notes	Covers AOS Administration, Hyper-V Administration for Acropolis, Command Reference, Powershell Cmdlets Reference, AOS Family Release Notes, and AOS release-specific Release Notes
Life Cycle Manager Guide	How to upgrade firmware and software components.
AHV guides and release notes	Administration and release information about AHV.
Prism Central and Prism Element Web Console guides and release notes	Administration and release information about Prism Central and Prism Element. Select **Release** in the Release Version selector at the top of the page.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2482

GETTING STARTED

This section provides an overview of Prism Central that involves the following information:

- Prism Central landing page, Infrastructure dashboard and entities, statistics, application switcher, and Prism Central GUI Organization.
- Installation and upgrade specifics.
- Licensing information.
- Cluster registration and de-registration with Prism Central.
- Application-specific navigation bar and searchability attributes.
- Prism Central GUI access.

Prism Central Deployment

This section provides information about the Prism Central requirements, limitations, and how to install and upgrade Prism Central in Nutanix and non-Nutanix ESXi environment.

A Prism Central instance consists of either a single VM or as a three-VM scale-out architecture that functions as a multi-cluster monitoring and control interface. For information about the maximum tested and supported values for entities in Prism Central, see Nutanix Configuration Maximums.

You can install Prism Central in either a Nutanix or a non-Nutanix environment. The following table describes the supported methods for Prism Central installation and upgrade:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2483

Table 2: Prism Central Deployment - Supported Methods

Environment Type	Hypervisor	Prism Central Upgrade using Upgrade Prism Central option	Prism Central Install		
			1-Click Internet with Prism Element	1-Click No Internet with Prism Element	Manual installation using binaries
Nutanix (Nutanix AOS cluster)	AHV ESXi Hyper-V	Supported for all versions except Prism Central 2022.9	Supported for all versions except Prism Central 2022.9	Supported for all versions except Prism Central 2022.9	Not supported for Prism Central versions 2022.9, 2023.1.0.1, 2023.3, and 2023.4.
Non-Nutanix	ESXi Hyper-V		Not applicable	Not applicable	

Note: For information about installing or upgrading to Prism Central pc.2024.1 and later releases on a three-tier cluster, see Prism Central Installation in a Non-Nutanix ESXi Environment on page 21 and Prism Central Upgrade in Non-Nutanix ESXi Environment on page 32.

The following limitations apply when you install Prism Central in a non-Nutanix environment:

- 1-click method is not supported

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2484

- A single-VM instance is the only option (multi-VM instances are not supported)
- Hypervisor must be ESXi
- Some Prism Central features are not available such as Self-Service (formerly Calm) and Flow support.

  Additionally, the Prism Central VM supports certain software features and add-ons, such as Nutanix Kubernetes Environment (formerly Karbon), only in a Nutanix environment. For specific requirements, see the release notes and guides for your planned or installed software components.

  Note:

  - Nutanix does not support Prism Central and its managed clusters in NAT-deployed environments.
  - Do not add any additional vDisks or NICs to a Prism Central VM other than what is specified in the installation or upgrade instructions.

    For information about the dedicated Prism Central upgrade vdisk that the Prism Central upgrade process deploys and uses for upgrade operations, see Prism Central Upgrade vDisk on page 28.
  - For information on supported methods for Prism Central upgrade, see Prism Central Upgrade Methods on page 27.
  - To scale out an existing single VM Prism Central to multiple VMs, see Expanding (Scale Out) Prism Central on page 573.
  - To upgrade one or more managed clusters through Prism Central, see Prism Central-Managed Clusters Upgrade on page 30.
  - If you use a proxy server, see Prism Central Configuration When a Cluster Uses Proxy Servers information in *Prism Central Admin Center Guide*.

Requirements for Prism Central Deployment

Ensure that the following requirements are met when you deploy (install or upgrade) Prism Central deployment at your site:

- When using the 1-click method for installing Prism Central, you select from a set of preconfigured Prism Central VM sizes. The *Prism Central Scalability* section in the Prism Central Release Notes provides Prism Central VM resource and capacity specifications for the preconfigured sizes. In addition, certain optional features that you can enable such as application discovery and Self-Service (formerly Calm) require additional Prism Central VM resources (more memory and vCPUs). After installing Prism Central, you may need to increase the VM resources before enabling one or more of these optional features. The requirements for various feature combinations are listed in KB 8932.
- For Microservices Infrastructure deployment, ensure that all the requirements provided in Microservices Infrastructure Prerequisites and Considerations on page 545 are fulfilled.
- When upgrading Prism Central and AOS, upgrade Prism Central first, then upgrade AOS on the clusters managed by Prism Central. See Acropolis Upgrade Paths on the Nutanix Support portal to check the upgrade path from your current version to your target version for AOS and Prism Central.
- Nutanix does not support Prism Central and its managed clusters in NAT-deployed environments.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2485

- Do not use the AOS binary and metadata .json files to upgrade your existing Prism Central deployment.

  Prism Central requires the use of specific Prism Central binary and metadata .json for upgrades and deployments. Using AOS files to upgrade Prism Central from any version is not supported and can result in Prism Central unavailability.

  Do not use the Prism Central AHV / ESXi / Hyper-V components on the Nutanix support portal to upgrade an existing Prism Central instance.

- Prism Central and each managed cluster are taking advantage of NCC features, ensure that:

  - Each node in your cluster is running the same NCC version.
  - Prism Central and each cluster managed by Prism Central are all running the same NCC version.

Limitations of Prism Central Deployment

The following limitations apply when you deploy (install or upgrade) Prism Central at your site:

- Prism Central deployment is not supported on a mixed cluster consisting of different hypervisors.
- Number of clusters limit based on the Prism Central release. For more information, see Nutanix Configuration Maximums.
- If Prism Central is not registered with the AOS cluster hosting it, refer to KB-10596 for additional requirements before upgrading.
- Prism Central 2022.9 and later versions no longer support CLI-based PCDR. A pre-upgrade check blocks upgrade to Prism Central 2022.9 or later versions if a CLI-based PCDR setup is detected. Nutanix recommends removing the CLI-based PCDR configuration before upgrade and enabling Prism Central Backup and Restore (PCBR) post-upgrade. For more information, see Prism Central Backup, Restore, and Migration on page 556, KB-13875 and KB 9599.
- If a single-node Prism Central VM is upgraded to Prism Central 2022.9 or later versions, but the underlying Prism Element (PE) is not running AOS 6.6, a pre-check will prevent the scaling out of Prism Central VM from 1-node to 3-node Prism Central.
- Prism Central versions where one-click upgrade is not enabled must use the legacy one-click upgrade method available on Prism Element as the LCM bundle is not available on the portal for download. For more information, see Use Upgrade Software in the Prism Element Web Console (Legacy 1-Click Upgrade) in *Prism Element Web Console Guide*.

Deploy Multiple Prism Central Instances on a Prism Element Cluster

This section describes a use case where you need to deploy multiple Prism Central instances on a single Prism Element cluster.

You can deploy multiple Prism Central instances, single-VM or three-VM instances, on one Prism Element cluster

Note:

- Ensure that none of the Prism Central instances are registered to the Prism Element cluster until all the Prism Central instances are deployed. You can register only one Prism Central instance to the Prism Element cluster.
- If you are deploying multiple instances of Prism Central on the same Prism Element cluster, then ensure that you register the cluster to a Prism Central only after all the Prism Central instances are deployed.
- The Prism Central that is registered with the Prism Element cluster manages the Prism Element cluster.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2486

Where the Prism Element cluster is already registered to a Prism Central instance and you need to deploy more Prism Central instances on that Prism Element cluster, do the following:

1. Unregister the Prism Element cluster from the existing Prism Central instance.
2. Deploy all the Prism Central instances that you need.
3. Register the Prism Element cluster with the previously unregistered Prism Central instance.

> **Note:** When you unregister a Prism Element cluster from a Prism Central instance, the Prism Element cluster is blocked from being registered again to the same or another Prism Central instance. To unblock the Prism Element cluster, contact Nutanix Support.

Prism Central Installation

This section provides information about how to install Prism Central in a Nutanix and non-Nutanix environment.

Prism Central Installation in Nutanix Environment

This section provides information about how to install Prism Central in Nutanix environment.

You can Install a Prism Central VM using the 1-click method for both connected sites (with internet connectivity) and dark sites (without internet connectivity). For more information, see Installing Prism Central Using 1-Click Method on page 16. This method employs the Prism Element web console from a cluster of your choice and creates the Prism Central VM in that cluster.

For information on how to install Prism Central in the non-Nutanix ESXi environment, see Prism Central Installation in a Non-Nutanix ESXi Environment on page 21.

Installing Prism Central Using 1-Click Method

This section describes how to install Prism Central in Nutanix environment with a connected site (with internet connectivity) or dark site (without internet connectivity) setup.

Before you begin

Ensure that you meet the following prerequisites before you install Prism Central:

- Check the Requirements for Prism Central Deployment on page 14 and Limitations of Prism Central Deployment on page 15.
- Check the port requirements between Prism Central and Prism Element. For more information, see Ports and Protocols.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2487

- Check the following requirements for the connected site (with internet connectivity) and dark site (without internet connectivity) environment.

Table 3: Prism Central Installation Requirements - Connected Site and Dark Site

Connected site	Dark Site

• The specified gateway must be reachable.
• Ensure the port TCP port 2100 is open from the Prism Element cluster to the Prism Central VM IP address. For the complete list of required ports, see Ports and Protocols.
• Ensure network connectivity between the VM VLAN and portgroup of the Prism Element cluster Controller VM and the Prism Central VM VLAN and portgroup.
• No duplicate IP addresses are used.
• The storage container used for deployment is mounted on all hypervisor hosts.
• When installing on an ESXi cluster:
  • vCenter and the ESXi cluster must be configured properly. For more information, see vSphere Administration Guide for Acropolis.
  • vCenter must be registered in Prism.
  • DRS must be enabled in vCenter.
  • vCenter is up and reachable during the deployment.
	Download Prism Central binary .TAR and metadata .JSON files from the Nutanix Support portal from a connected machine.
	1. Log in to the Downloads page for Prism Central.
	2. Click **Download** and **Metadata** to save the **Prism Central 1-click deploy from Prism Element** binary .TAR and metadata .JSON files, respectively, to your local media.
	You can also copy these files to a USB stick, CD, or other media.
	Note: Do not use the Prism Central OVA, ZIP, AHV image, or AOS binary .TAR.GZ and upgrade metadata JSON files from the Nutanix support portal to create this new Prism Central instance. Use the .TAR format binary and metadata .JSON files.
	The Prism Central OVA is used only to install or upgrade Prism Central in non-Nutanix ESXi environment. For more information, see Prism Central Installation in a Non-Nutanix ESXi Environment on page 21 and Prism Central Upgrade in Non-Nutanix ESXi Environment on page 32.

About this task

Perform this procedure for both connected site (with internet connectivity) and dark site (without internet connectivity).

Procedure

1. Log in to the Prism Element web console as the user admin for your cluster.
2. Run NCC as described in Run NCC Checks .
3. Do one of the following:
   - » On the **Home** dashboard, click **Register or create new** from the **Prism Central** widget.
   - » Click the gear icon in the main menu and then select **Prism Central Registration** from the **Settings** menu.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2488

4. In the first screen of the **Prism Central** dialog box, click the **Deploy** button.

   This screen includes two options, **Deploy** and **Connect**. For information on how to connect to an existing Prism Central instance using **Connect** option, see Registering or Unregistering a Cluster with Prism Central.

   > **Note:** On an ESXi cluster, you must first register a vCenter Server before you deploy a new Prism Central instance.

5. *(Applicable for Dark site only)* In the **PC Version** step of **Prism Central Deployment** screen, click the **Upload Installation Binary** link, select the Prism Central Metadata File (.json) and Prism Central Installation Binary (.tar) files, and click **Upload**.

   If there is already an image uploaded, the system displays the available versions.

6. *(Applicable for Connected site only)* In the **PC version** step of **Prism Central Deployment** screen, select the required Prism Central version you intend to install.

   Select **Show compatible versions** checkbox to view the list of PC versions compatible with the AOS cluster.

   > **Note:** If the Prism Central version you want to install does not appear in the list, typically because the cluster does not have Internet access (such as at a dark site), you can click the **Upload Installation Binary** link to upload an image from your local media as described in Step 5 on page 18.

7. Click **Next**.
   The **Scale type** step appears.

8. In the **Scale type** step, do one of the following:

   » To deploy a 1-VM instance of Prism Central, select **Deploy Single-VM PC** .

   » To deploy a 3-VM instance of Prism Central, select **Deploy Scale-Out PC (on 3-VMs)**.

   A Prism Central instance can consist of either a single VM or a set of three VMs. A 3-VM instance increases both the capacity and resiliency of Prism Central at the cost of maintaining the additional VMs. For information on Prism Central scalability, see the *Prism Central Scalability* topic in the release notes Prism Central version to be installed.

9. Click **Next**.
   The **Configuration** step appears

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2489

10. In the **Configuration** step, do the following in the indicated fields:

    a. Select (click the radio button for) the Prism Central VM size based on the number of guest VMs it must manage across all the registered clusters:

       For Prism Central configuration limits, see KB-8932 and Nutanix Configuration Maximums.

    b. **Network**: Select an existing network for this Prism Central instance from the list.

       If the target network is not listed, click the **Create Network** link to create a new network. For more information, see Network Management.

    c. **Subnet Mask**: Enter the subnet mask value.

    d. **Gateway**: Enter the IP address of the gateway.

    e. **DNS Address(es)**: Enter the IP address for one or more DNS servers. Enter multiple addresses in a comma separated list.

    f. **NTP Address(es)**: Enter the IP address for one or more NTP servers. Enter multiple addresses in a comma separated list.

    g. **Select a Container**: Select a container for the Prism Central VM from the drop-down list.

    h. *(Applicable for Scale-Out PC (on 3-VMs) only)* **Virtual IP**: Enter a virtual IP address for the Prism Central instance

       > **Note:** A virtual IP can be used as a single point of access for Prism Central. When you enter virtual IP, the IP addresses for the three PC VMs are populated automatically. You can keep those addresses or change them as desired.

       > **Important:** The virtual IP and FQDN are mutually exclusive in Prism Central. However, while installing Prism Central, you can only configure the virtual IP. After installing Prism Central, you can use either FQDN or virtual IP. For more information, see Managing Prism Central.
       >
       > To configure FQDN, the administrator must configure the domain name in the DNS server to resolve to all the external IPs of the Prism Central VMs.

    i. **VM Name**: Enter a name for the Prism Central VM.

    j. **IP**: Enter a static IP address for the Prism Central VM.

11. Click **Next**.
    The **Microservices** step appears.

12. In the **Microservices** step, do the following in the indicated fields:

    a. **Prism Central Service Domain Name**: Enter a unique domain name for the Prism Central Microservices. For more information, see *Prism Central Service Domain Name restrictions* in Microservices Infrastructure Prerequisites and Considerations.

    b. **Internal Network**: Select the network to use for Prism Central micro services communication from the dropdown list.

       The default selection **Private Network [default]** is a pre-configured private VxLAN network. Instead, if you want microservices infrastructure to use a different network, you can select the network (managed or

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2490

unmanaged) from the drop-down list. If the network you want microservices infrastructure to use does not appear in the list, you must first configure it. For more information, see Network Configuration.

c. The **Use default settings (recommended)** checkbox is available only when you have retained the default selection (**Private Network [default]**) for **Internal Network** in the preceding step. This checkbox is selected by default. Do one of the following:

- Retain the check mark for the **Use default settings (recommended)** checkbox and click **Validate**. (Go to step 12.d on page 20.)

  Retaining the check mark for the **Use default settings (recommended)** checkbox allows Prism Central to use the **Private Network [default]** with the default values for **Subnet Mask**, **Gateway IP Address** and **IP Address Range**.

- Clear the **Use default settings (recommended)** checkbox, if you want Prism Central to use the **Private Network [default]** setting with specific (non-default or custom) values for **Subnet Mask**, **Gateway IP Address** and **IP Address Range**.

Configure the **Internal Network** for microservices infrastructure if you did one of the following:

- Selected a managed or unmanaged network other than **Private Network [default]** for **Internal Network**.

  If you selected a managed network, the values in the **Subnet Mask**, **Gateway IP Address** and **IP Address Range** fields are already configured. If you selected an unmanaged network, you must enter the necessary values in the respective fields.

- Cleared the **Use default settings (recommended)** checkbox with the **Private Network [default]** selection for **Internal Network**.

Enter the values for the following parameters to configure **Internal Network**:

Parameter	Description
Subnet Mask	Enter the subnet mask.
Gateway IP Address	Enter the IP address for the gateway.
IP Address Range	Enter a range of IP addresses that the network can use. Enter a range of at least 10 available (unreserved) addresses for a 3-VM (scale out) Prism Central instance or at least 5 addresses for a 1-VM Prism Central instance. The addresses must be consecutive or sequential. For a managed network, the range of addresses for microservices infrastructure must be outside the range of reserved IP addresses (for example, DHCP IP Pool) in the selected network.

d. After you check that the values entered for all the fields are correct, click **Next**.

13. Click **Next**.
The **Summary** step appears.

14. In the **Summary** step, check the details entered for Prism Central installation, and click **Deploy**.
This begins the deployment process. On the **Home** page, the Prism Central widget displays **Deploying** until the installation is completed, then it displays **OK**. Click **OK** to launch the Prism Central web console in your browser.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2491

15. Monitor the deployment progress (1-VM or 3-VM Prism Central instances) from the **Tasks** page and view information about the deployed VMs through the **VM** dashboard. For more information, see Tasks View.

What to do next

you can expand your cluster, remove nodes, and enable services such as Self-service, Flow Network Security, and Intelligent Operations without registering the hosting cluster with Prism Central.

Register this cluster with Prism Central, if you want to manage this cluster through Prism Central. For more information about how to connect to an existing Prism Central instance, see Registering or Unregistering a Cluster with Prism Central.

Prism Central Installation in a Non-Nutanix ESXi Environment

This section provides information about how to install Prism Central in non-Nutanix environment.

For information on how to install Prism Central in Nutanix environment, see Prism Central Installation in Nutanix Environment on page 16.

The procedures detailed in this section are intended for deploying Prism Central solely within an on-premises non-Nutanix environment.

Important:

- Ensure that you have appropriate ESXI credentials with **Administrator** privileges, to allow the CSI driver to perform the following VM updates and data store operations:
  - VM update operations.
  - Perform read and write operations on a data store.
  - Query storage policies

  For information on permissions, key roles and privileges for the vSphere User, see the *VMware vSphere Container Storage Plug-in* document in the VMware documentation.
- Nutanix Disaster Recovery is not supported for non-Nutanix ESXi Prism Central deployments.

Downloading Prism Central VM Installation Files (Manual Method)

This section describes how to download Prism Central VM installation files for manual installation (when the Prism Central 1-click deployment method is not available).

Procedure

1. Log on to the Nutanix Support portal and go to the Prism Central Downloads page.
   The page lists the latest available version. You can download previous release bits from the **Other Versions** tab.
2. Locate the **Prism Central Install on ESX (Version:** `pc version`) file, and click **Download** to get the Prism Central VM files, then save them to a folder, directory, or other location.
   The system downloads a `pc_version`.ova file, where `pc_version` is the Prism Central version.

   For example, the downloaded file for Prism Central pc.202x.x is named pc.202x.x.ova.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2492

Installing the Prism Central VM (ESXi)

About this task

A special VM runs Prism Central from which you can monitor and manage multiple clusters. You can install the Prism Central VM on an ESXi hypervisor.

Before you begin

- Nutanix does not support deploying a large Prism Central in a non-Nutanix environment. Increasing the size of a Prism Central in a non-Nutanix ESXi environment to large Prism Central is also not supported. Nutanix recommends that you consider deploying Prism Central on a Nutanix cluster if your environment requires a large Prism Central.
- Nutanix recommends a VM size of 6 vCPUs, 28 GB of memory, and 500 GiB of storage for a small Prism Central VM deployment.
- Ensure to enable memory hot-plug for ESXi. For 1-click deployment methods, memory hot-plus is automatically enabled.
- Ensure that you have disabled Intelligent Operations if the **Preupgrade Steps** fail due to a memory issue. For information on disabling Intelligent Operations, see Intelligent Operations Guide.

To install the Prism Central VM on an ESXi hypervisor, do the following:

Procedure

1. Download and extract the Prism Central files for ESXi as described in Downloading Prism Central VM Installation Files (Manual Method) on page 21.
2. Install the downloaded OVA file as follows:
   a. Connect to vCenter or an ESXi host using the vSphere client.
   b. Select the OVA file and deploy it.
      Select an OVA file called pc.2024.1.ova and deploy it from the download location on the workstation. In the OVA file name, the version 2024.1 indicates the Prism Central version. See the vSphere documentation for instructions on how to do deploy an OVA file.

      Note:

      - Nutanix recommends a VM size of 6 vCPUs, 28 GB of memory, and 500 GiB of storage for a small Prism Central VM deployment.

        Ensure that you have disabled AIOps if the **Preupgrade Steps** fail due to a memory issue. For information on disabling AIOps, see Intelligent Operations Guide.
      - In the OVA deployment wizard using vSphere web client, Nutanix recommends that you manually select **Thin Provision** as the virtual disk format while configuring the storage. Failing to manually select **Thin Provision** creates the default thick provisioned VMDK in vSAN.
3. Upgrade the Prism Central VM compatibility (VMX version).
   a. Right-click on the Prism Central VM, and navigate to **Compatibility** > **Upgrade VM Compatibility**.
   b. Set the **Compatible with** field to **ESXi 7.0 U2 and later**.
   c. Power on the Prism Central VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2493

4. Power on the Prism Central VM through the vSphere Client. Click **ACTIONS** > **Power** > **Power On** to start the VM.

   Wait for the Prism Central VM to reboot and complete the `nutanix-rc-local` service start.

   > **Caution:** Do not configure the next steps before the Prism Central VM boots up completely and the `nutanix-rc-local` service completes successfully. If you do and the Prism Central VM does not boot up, the Prism Central installation fails, and you cannot complete the installation.
   >
   > Run the following command to verify that the **Process** status of the `nutanix-rc-local` service as <PID> ExecStart=/etc/nutanix/rc.local (code=exited, status=0/SUCCESS).
   >
   > ```
   > nutanix@pcvm$ sudo systemctl status nutanix-rc-local.service
   > ```

5. Log into the Prism Central VM through the vSphere console (user name "nutanix").

6. Assign a static IP address to the Prism Central VM as follows:

   a. Open the ifcfg-eth0 file for editing.

      The following command opens the file using the vi editor:

      ```
      nutanix@pcvm$ sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0
      ```

   b. Add or update the `NETMASK`, `IPADDR`, `BOOTPROTO`, and `GATEWAY` entries as needed.

      > **Note:** Use the route -n command to retrieve the `NETMASK` and `GATEWAY` information. Ensure that the selected IP address is unreachable to the console IP address.

      ```
      NETMASK="xxx.xxx.xxx.xxx"
      IPADDR="xxx.xxx.xxx.xxx"
      BOOTPROTO="none"
      GATEWAY="xxx.xxx.xxx.xxx"
      ```

      - Enter the desired netmask value in the `NETMASK` field. (Replace *`xxx.xxx.xxx.xxx`* with the appropriate value.)
      - Enter the appropriate static IP address (usually assigned by your IT department) for the Prism Central VM in the `IPADDR` field.
      - Enter `none` as the value in the `BOOTPROTO` field. (You might need to change the value from `dhcp` to `none` if you employ DHCP. Only a static address is allowed; DHCP is not supported.)
      - Enter the IP address for your gateway in the `GATEWAY` field.

        > **Warning:** Carefully check the file to ensure there are no syntax errors, whitespace at the end of lines, or blank lines in the file.

   c. Save the changes.

   d. Remove any existing Nutanix Controller VM entries, that is ones which include "NTNX-*`<number>`*-CVM", from the /etc/hosts file. (Ensure that you do not remove any other entries from the file.)

      To edit the file using vi, enter

      ```
      nutanix@pcvm$ sudo vi /etc/hosts
      ```

      When the Prism Central VM starts the first time and DHCP is enabled in the network, an entry similar to the following is added to the /etc/hosts file. This entry (if present) needs to be removed from the /etc/hosts file before restarting the Prism Central VM in the next step, which generates a new entry if DHCP is enabled.

      ```
      127.0.0.1 NTNX-10-3-190-99-A-CVM
      ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2494

e. Restart the Prism Central VM.

```
nutanix@pcvm$ sudo reboot
```

> **Note:** The Prism Central VM is powered in approximately a minute.

7. Set up the installation environment.

   For more information, see Setting Up the Installation Environment on page 24.

After completing the steps in Setting Up the Installation Environment on page 24, continue to perform the following steps.

8. Log on to vCenter Server using an administrator account and do the following:

   a. Select the Prism Central VM.

   b. Right click **Edit Notes**.

   c. In the dialog box enter NutanixPrismCentral without any new line characters and then click **OK**.

   Creating a Prism Central instance through a 1-click method automatically enables certain best practice restrictions on who can manage a Prism Central VM. This step enables the same set of best practice restrictions for a manually installed Prism Central VM. (Non-administrators may not perform any operations while administrators may perform a limited set of permissions including launch console, power off or on, pause or resume, migrate, and configure VM host affinity.)

What to do next

This completes Prism Central installation. The next step is to register clusters with Prism Central. Port 9440 needs to be open in both directions between the Prism Central VM and any registered clusters. For more information on ports, see Ports and Protocols for Prism Central and Ports and Protocols for Microservices Infrastructure. For more information on how to connect to an existing Prism Central instance, see Registering or Unregistering a Cluster with Prism Central on page 61.

Setting Up the Installation Environment

This section describes setting up the environment for installing Prism Central pc.2024.1 or later releases.

Before you begin

Complete the initial steps prior to the set-up the environment step in Installing the Prism Central VM (ESXi) on page 22.

About this task

The installation environment setup involves the following phases:

- Installing the Prism Central pc.202x.x release using the OVA file. For more information, see Installing the Prism Central VM (ESXi) on page 22.
- Downloading the **vSphere CSI Bundle** from the Nutanix **Downloads** portal for Microservices Platform.
- Setting up the installation tool.
- Setting up target Prism Central cluster configuration.
- Setting up the site proxy environment and defining storage policies.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2495

Procedure

1. Log on to the Nutanix Support portal and browse to the Microservices Platform (MSP) page.
2. Download the CSI bundle and extract its contents into the /home/nutanix/data directory on the Prism Central VM.

   The **vSphere CSI Bundle** contains essential tools such as `setup_three_tier`.
3. Extract the vSphere CSI bundle tar.xz file by running the following command:

   ```
   nutanix@pcvm$ cd /home/nutanix/data
   nutanix@pcvm:/data$ tar -Jxvf vsphere_csi_bundle.tar.xz
   ```
4. SSH to the Prism Central VM as a `nutanix` user.
5. Run the `setup_three_tier` tool.

   The `setup_three_tier` tool creates the Prism Central environment configuration file.

   For example:

   ```
   nutanix@pcvm$ /home/nutanix/data/vsphere_csi_bundle/tools/setup_three_tier -e
   ```
6. Log on to the Prism Central VM again through the vSphere console and then run the command to create a cluster, specifying additional parameters such as DNS servers and NTP servers.

   ```
   nutanix@pcvm$ cluster --cluster_function_list "multicluster" -s
    static_ip_address --dns_servers "dns_server_Ip_1, dns_server_ip_2" --ntp_servers
    "0.centos.pool.ntp.org,1.centos.pool.ntp.org" create
   ```

   The *`static_ip_address`* is the Prism Central VM IP address.

   The *`dns_server_Ip_1`* and *`dns_server_ip_2`* are the IP addresses of the DNS server.

   When you enable Microservices Infrastructure, the services deployed on Microservices Infrastructure require dynamic storage allocation. To allocate the necessary storage when the services require it (on-demand storage), you must log on to the Prism Central VM through the vSphere console. The Microservices Infrastructure CSI driver for vSphere performs the following essential storage operations when you log on to the Prism Central VM through the vSphere console only:

   - Communicates with the vCenter to provision new storage
   - Performs VM update API calls to attach it to the Prism Central VM
   - Makes the attached storage available to services as persistent storage.
7. (Optional) Configure proxy settings.

   If a proxy setup is in place, ensure to configure Microservices Infrastructure (CMSP) URLs in the allowedlist in your proxy environment to allow access to docker images and other configuration files. Microservices Infrastructure requires access to the following URLs:

   - docker.io
   - production.cloudflare.docker.com
   - nutanix.github.io
   - us-west-2.amazonaws.com
   - quay.io

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2496

8. In the vSphere client, configure the vCenter settings:

   a. Create a tag and a category. Map the category to the tag.

   b. Assign the tag to the datastore hosting the Prism Central VM.

   c. Create a new VM storage policy and assign it to the newly created tag.
   For more information, see *vSphere Tags and Attributes* information in *VMWare vSphere documentation*.

> **Note:** Ensure that you select **Enable tag based placement rules** checkbox while defining the storage policy structure.

What to do next

Complete the steps after the set-up the environment step in Installing the Prism Central VM (ESXi) on page 22.

Configuring Prism Central VM in the Non-Nutanix ESXi Environment

This task describes how to configure Prism Central VM in the non-Nutanix environment running the ESXi hypervisor.

Before you begin

Ensure that you set up the install environment before you run the install tool (`setup_three_tier` tool). For more information, see Setting Up the Installation Environment on page 24.

Procedure

1. SSH to the Prism Central VM and run the `setup_three_tier` tool.
   The `setup_three_tier` tool accepts the user configuration and sets up the environment for PC and CMSP enablement.

   For example:

   ```
   nutanix@pcvm$ /home/nutanix/data/vsphere_csi_bundle/tools/setup_three_tier
   ```

   The system prompts you to enter the vCenter IP, vCenter port, user credentials, datacenter name, and storage policy name.

2. Enter the required details.
   The system verifies the entered data, and displays the result.

3. Check that the Prism Central ENV (pc_env_config.json) configuration file is created at /etc/nutanix.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2497

4. Run the `Enable Microservices Infrastructure` script.

   > **Note:** Before you run the `Enable Microservices Infrastructure` script, ensure that you have configured the DNS and NTP servers for the cluster before you enable Microservices Infrastructure.

   SSH to the Prism Central VM and run the script as follows:

   ```
   nutanix@pcvm$ python /home/nutanix/data/vsphere_csi_bundle/tools/
   enable_cmsp_3_tier.py
   ```

   All the files required for deploying and configuring the Prism Central VM are packaged in the Prism Central deployment package.

   Enabling Microservices Infrastructure could take up to 30 minutes for the supported single VM Prism Central deployment. To confirm if Microservices Infrastructure is enabled, run the `ecli task.list` command.

   Prism Central reports any failure of the enablement after about two hours and five minutes.

Prism Central Upgrade

This section provides information about how to upgrade Prism Central in a Nutanix and non-Nutanix environment.

Prism Central Upgrade in Nutanix Environment

This section provides information about how to upgrade Prism Central in Nutanix environment.

Prism Central Upgrade Methods

You can upgrade a Prism Central instance using the following methods:

- Upgrade directly from Prism Central web console.

  To upgrade directly from Prism Central, perform the following steps:

  1. Log in to Prism Central.
  2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Upgrade Prism Central** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
  3. Perform the steps as described in Upgrading Prism Central on page 28 section.

- Upgrade from Life Cycle Manager (LCM) tool.

  To upgrade Prism Central from LCM, perform the following steps:

  1. Log in to Prism Central.
  2. Select the **Admin Center** application from Application Switcher Function, and navigate to **LCM** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
  3. Choose either of the following upgrade methods based on the LCM connectivity status with the site:

     - *Upgrade Prism Central from LCM with Connected site* - Perform the actions as described in Performing Firmware and Software Updates in a Connected Site Setup section of *Life Cycle Manager Guide*.
     - *Upgrade Prism Central from LCM with Dark site using a web server* - Perform the actions as described in Performing Firmware and Software Updates in a Dark Site Setup section of *Life Cycle Manager Guide*.
     - *Upgrade Prism Central from LCM with Dark site using Direct Upload* - Starting with LCM 3.0, Prism Central also supports the **Direct Upload** functionality. A minimum supported version of pc.2024.1 is required to use the Direct Upload functionality on Prism Central. Perform the actions as described in Performing Firmware and Software Updates in a Dark Site Setup section of *Life Cycle Manager Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2498

For information on how to upgrade Prism Central in non-Nutanix ESXi environment, see Prism Central Upgrade in Non-Nutanix ESXi Environment on page 32

Prism Central Upgrade vDisk

Each Prism Central VM includes a `/home` disk partition that is used for storage during upgrade process. The Prism Central upgrade process can fail if the available disk space in this partition is near capacity.

For Nutanix clusters, the upgrade process uses a separate, dedicated vDisk of 30 GB capacity instead of the `/home` partition. Prism Central uses this dedicated vDisk to store the downloaded Prism Central software bundle, decompressing the bundle, and hosting the installer.

When you upgrade Prism Central version to the current version, the Prism Central upgrade process uses the vDisk image in the bundle to create the Prism Central upgrade vDisk. The upgrade process uses this vDisk for the upgrade operations that include any subsequent upgrade.

Requirements

- Ensure that the Prism Central instance is registered to a host in the cluster or microservices infrastructure is enabled on the Prism Central instance.
- Ensure that the Prism Element cluster hosting Prism Central is registered to this Prism Central instance.
- Ensure that the Prism Element cluster hosting Prism Central has sufficient disk resources to provide the 30 GB vDisk.

Running NCC (Prism Central)

About this task

Before doing any upgrade procedure, log on to the Prism Central VM and run the NCC checks from the ncc command line. You cannot run NCC from the Prism Central web console.

Procedure

1. Log in to the Prism Central VM through a secure shell session (SSH).
   - For single-VM deployments, use the Prism Central IP address.
   - For scale-out three-VM deployments, use the virtual IP address. If you did not configure a virtual IP address, use the Prism Central IP address of any of the Prism Central VMs.
   - If you do not know the PC VM IP address, contact your cluster administrator.
2. Run NCC.

   ```
   nutanix@pcvm$ ncc health_checks run_all
   ```

   If the check reports a status other than INFO or PASS, resolve the reported issues before proceeding. If you are unable to resolve the issues, contact Nutanix Support for assistance.

Upgrading Prism Central

About this task

This section describes how to upgrade Prism Central using the one-click **Upgrade Prism Central** method.

For information on how to upgrade Prism Central in non-Nutanix ESXi environment, see Prism Central Upgrade in Non-Nutanix ESXi Environment on page 32

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2499

Before you begin

Ensure that you meet the following prerequisites before you upgrade Prism Central:

- Check the Requirements for Prism Central Deployment on page 14 and Limitations of Prism Central Deployment on page 15.
- See the Prism Central Release Notes for resource requirements and capacity specifications for the Prism Central VM.
- If you have enabled Objects in the Prism Central managing the cluster, ensure that the Objects VMs are healthy and running when Prism Central upgrade process enables Microservices Infrastructure or you manually enable Microservices Infrastructure.

  > **Caution:** If the Objects VMs are not healthy and running, the task for enabling Microservices Infrastructure might fail. For information on how to start the Objects VMs, see Starting the Objects VMs in the *Objects User Guide*.

- Before performing any upgrade procedure, ensure that you are running the latest version of the Nutanix Cluster Check (NCC) health checks and upgrade NCC if necessary.

About this task

Perform this procedure to upgrade Prism Central in Nutanix environment.

Procedure

1. Run NCC as described in Running NCC (Prism Central) on page 28.
2. Log in to Prism Central through a web browser.
3. Select the **Infrastructure** application from Application Switcher Function, and click the Settings icon or navigate to **Prism Central Setting** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
   The system displays the **Settings** page.
4. Click **Upgrade Prism Central**, and perform the following steps to download and automatically install the Prism Central upgrade files.
   a. Do one of the following:
      - » If you previously selected **Enable Automatic Download** and the software has been downloaded, click **Upgrade**, then click **Yes** to confirm.
      - » If **Enable Automatic Download** is cleared, click **Download** to check if there is software available. When the download task is completed, click **Upgrade**, then click **Yes** to confirm.

   b. [Optional] To run the pre-upgrade installation checks only without upgrading, click **Upgrade** > **Pre-upgrade**. These checks also run as part of the upgrade procedure.
   The **Upgrade Software** dialog box shows the progress of your selection. When the upgrade process is complete, the Prism Central VM restarts. Wait a few minutes and log on again, as Prism Central might lose connectivity during the upgrade process.

   > **Note:** If you are upgrading an older version of a Prism Central "large" VM that contains just a single vDisk, the upgrade process might add three new vDisks. This allows Prism Central to shard Cassandra metadata to improve performance. While the listed disk capacity of a Prism Central VM includes all the vDisks, the additional vDisks do not impact overall capacity. During the upgrade you can monitor progress ("VM disk attach" tasks) from the Tasks dashboard.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2500

5. After the upgrade completes, run NCC as described in Running NCC (Prism Central) on page 28.
   The NCC health check pc_vm_resource_resize_check verifies that the configured amount of memory and vCPU on the Prism Central VM is adequate. If this check triggers a WARN alert, see the referenced Knowledge Base article to adjust Prism Central VM resources.

   After adjusting resources, run this check again to ensure a PASS status result: `nutanix@cvm$ ncc health_checks system_checks pc_vm_resource_resize_check`.

6. On the **LCM** page, click **Inventory** > **Perform Inventory** to enable LCM to check, update and display the inventory information.

   For more information, see Performing Inventory with the Life Cycle Manager section in *Life Cycle Manager Guide*.

Upgrading Prism Central by Uploading Binary and Metadata Files

About this task

- Do these steps to download Prism Central binary and metadata .JSON files from the Nutanix Support Portal, then upgrade through **Upgrade Software** in the Prism Central web console.
- Typically you would need to perform this procedure if your cluster is not directly connected to the Internet and you cannot download the binary and metadata .JSON files through the Prism Central web console.

Procedure

1. Log on to the Nutanix support portal and go to **Downloads** > **Prism Central**.
2. Click **Download** to save the **Prism Central Upgrade** binary and metadata .JSON files on your local media.
   You can also copy these files to a USB stick, CD, or other media.
3. Log on to the Prism Central web console.
4. Click the gear icon in the main menu and then select **Upgrade Prism Central** in the **Settings** menu.
5. Click the **upload the Prism Central binary** link.
6. Click **Choose File** for the binary and upgrade metadata (.JSON) files that you previously downloaded, browse to the file locations, and click **Upload Now**.
7. [Optional] When the file upload is completed, to run the pre-upgrade installation checks only without upgrading, click **Upgrade** > **Pre-upgrade**. These checks also run as part of the upgrade procedure.
8. When the file upload is completed, click **Upgrade** > **Upgrade Now**, then click **Yes** to confirm.
   The **Upgrade Software** dialog box shows the progress of your selection, including pre-installation and cluster health checks. After the upgrade process is completed on a Prism Central VM, the Prism Central VM restarts. This restart is not disruptive to node operations.
9. On the **LCM** page, click **Inventory** > **Perform Inventory** to enable LCM to check, update and display the inventory information.

   For more information, see Performing Inventory with the Life Cycle Manager section in *Life Cycle Manager Guide*.

Prism Central-Managed Clusters Upgrade

You can upgrade AOS on some or all of clusters registered to and managed by Prism Central through the Prism Central web console.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2501

You can upgrade AOS on some or all of clusters registered to and managed by Prism Central. The upgrade procedure, known as 1-click centralized upgrade, enables you to upgrade each managed cluster to a specific version compatible with Prism Central. Acropolis Upgrade Paths lets you check the upgrade path from your current version to your target version for AOS, Prism Central, and Nutanix Files.

Cluster Upgrade Requirements

- Upgrade clusters through the Prism Central web console.
- You can upgrade clusters if **Available Versions** is shown in the **Upgrade Software** dialog. It will display one or more AOS versions available to apply to clusters. If no versions are available (that is, none displayed), you might have to upgrade each cluster according to procedures described in this guide. Basically, if a version is available to Prism Central, it will be available to each cluster registered.
- Prism Central and each cluster (individually also known as Prism Element) must be connected to the Internet to access the Nutanix support portal.
- Prism Central and each cluster must be configured with a domain name server. For more information, see Configuring Name Servers (Prism Central) or Configuring Name Servers in the *Prism Element Web Console Guide*.
- Dark-site (internet-disconnected) upgrades cannot be performed using this feature. In this case, upgrade each cluster according to procedures described in this upgrade section.
- You cannot initiate an upgrade on a cluster that has an upgrade that is in process or is not completed.

Cluster Upgrade Features

- Sequential upgrade, in order, one cluster at a time. Select the order in which clusters are upgraded. Upgrade one cluster, then the next cluster is upgraded until all upgrades are complete. The clusters waiting be upgraded are placed in a Queued status. If one cluster fails to upgrade for some reason, the upgrade is cancelled for all remaining queued clusters.
- Parallel upgrade. Upgrade all clusters at the same time. If one cluster fails to upgrade for some reason, it does not affect the upgrade status of the other clusters. The upgrade status of each cluster is independent from every other cluster.
- Labeled clusters. You can apply a label to selected clusters and upgrade just the labeled clusters. The label also enables you to filter clusters by label.

Upgrading One or More Managed Clusters

Procedure

1. Log in to the Prism Central web console.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Hardware** > **Clusters** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
3. Click the **List** tab and do one of the following:
   - » Select one or more clusters from the list.
   - » Click **Filters** and select a cluster label if you have already created a label to group specific clusters.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2502

4. Click **Actions** > **Upgrade Software** to launch the **Upgrade Software** dialog box.

   a. **Available Versions** lists AOS versions available to apply to clusters

   b. **Upgrade Sequence** enables you to choose parallel upgrade (upgrade all selected clusters **At the same time**) or **One at a time (custom Order)** (upgrade one cluster at a time in order)

   c. List of clusters to select for upgrade order if you selected **Custom Order**

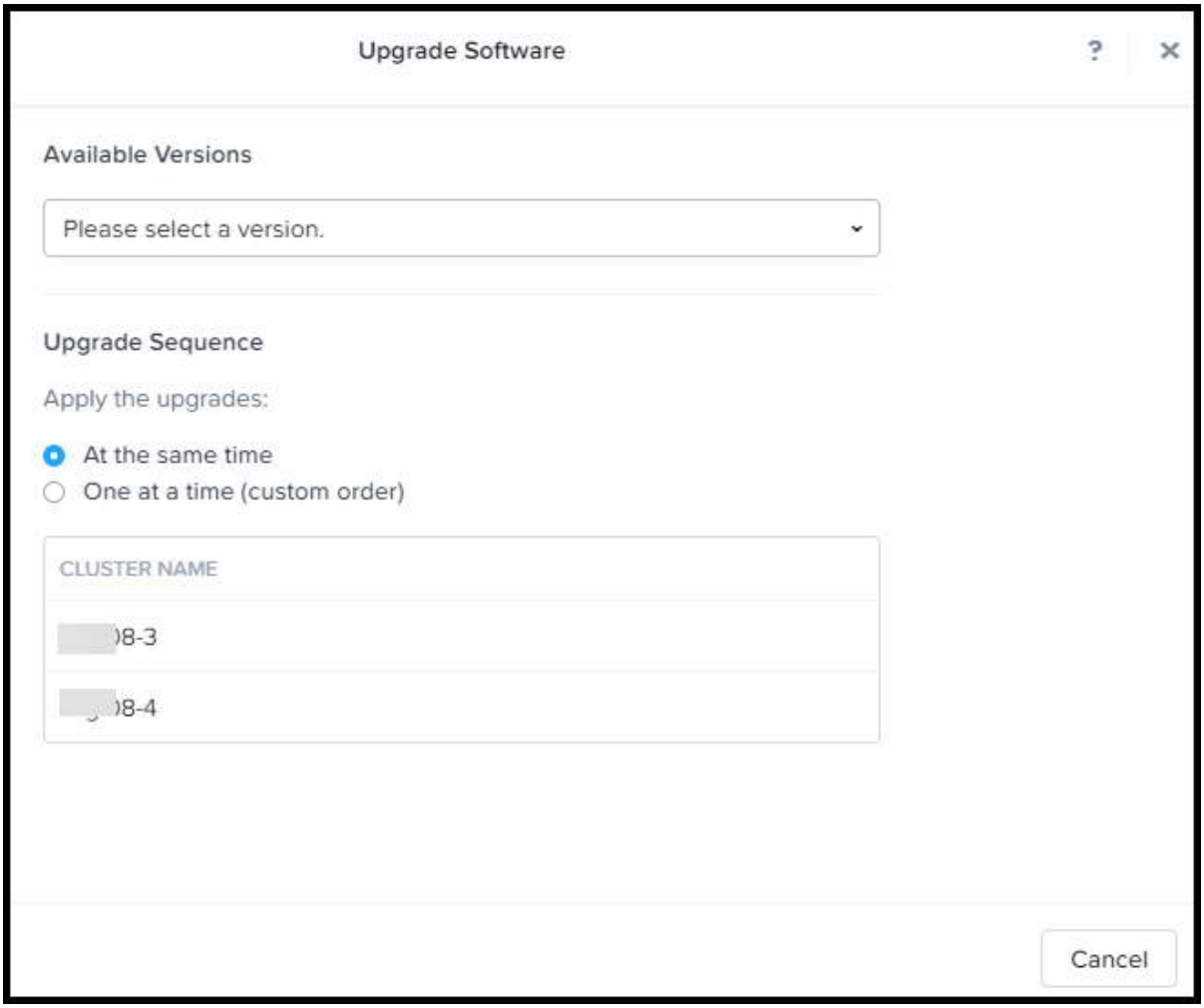


Figure 1: Upgrade Software

5. Select an AOS version and **Upgrade Sequence** choice, then click **Upgrade**.
   The upgrade begins. To view upgrade progress and status, click the blue task icon to open the **Tasks** page. The **Cluster** pane also displays **Upgrade Status**.

6. On the **LCM** page, click **Inventory** > **Perform Inventory** to enable LCM to check, update and display the inventory information.

   For more information, see Performing Inventory with the Life Cycle Manager section in

   Life Cycle Manager Guide.

Prism Central Upgrade in Non-Nutanix ESXi Environment

This section describes how to upgrade Prism Central virtual machine (VM) in a non-Nutanix environment with the ESXi hypervisor.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2503

Note:

- Use these procedures only when you install or upgrade the Prism Central VM to Prism Central pc.2024.1 or later versions. The Prism Central bundle downloads the necessary software that are required by Prism Central.
- Upgrading Prism Central to pc.2024.1 or later versions requires LCM 3.0 or later versions which is packaged with the Prism Central bundle. You need not upgrade LCM separately.
- The CSI bundle that you download while Setting Up the Upgrade Environment on page 33 supports ESXi 7.0.3 or later versions. Do not use the vSphere CSI Bundle to install the Prism Central VM and enable Microservices Infrastructure in Nutanix environments.
- For non-Nutanix deployments, the Prism Central upgrade vDisk is not supported during Prism Central deployment.

For information on how to upgrade Prism Central in Nutanix environment, see Prism Central Upgrade in Nutanix Environment on page 27.

ESXi Credentials

Ensure that you have the appropriate credentials with Administrator privileges, to allow the CSI driver to perform the following VM updates and data store operations.

- VM update operations.
- Perform read and write operations on a data store.
- Query storage policies

For information, see the *VMware vSphere Container Storage Plug-in* document in the VMware documentation.

Setting Up the Upgrade Environment

This section describes how to set up the non-Nutanix ESXi environment to upgrade to Prism Central 2024.1 or later release.

About this task

The upgrade environment setup involves the following phases:

- Configuring the Prism Central VM settings and upgrading compatibility
- Configuring the vCenter Settings
- Setting up the upgrade tool

Procedure

1. Access the hypervisor management interface such as the VMware vSphere client, and power off the Prism Central VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2504

2. Navigate to the **Prism Central VM Settings** page, and perform the following actions:

   a. In the **Virtual Hardware** tab, perform the following settings:

      Prism Central Pro and Ultimate licenses enable portfolio services. Running portfolio services requires increased vCPU and memory resources. Consider disabling the portfolio services to minimize the resource allocation to Prism Central.

      For Prism Central without portfolio services:

      - vCPU = 6
      - vRAM = 28 GB

        Check the Prism Central vRAM and upgrade it to 28 GB if necessary.

      For Prism Central with portfolio services:

      - vCPU = 10
      - vRAM = 30 GB

        Check the Prism Central vRAM and upgrade it to 30 GB if necessary.

      - Click **ADD NEW DEVICE** to add 3 new disks with sizes as 30 GB, 100 GB, and 270 GB, and allocate the disk space based on the activities planned such as Prism Central upgrade or CMSP configuration.

Figure 2: Virtual Hardware Settings - VSphere Client

   b. Enable Disk UUID support to access and modify the Prism Central VM configuration settings in IntelliJ.

      In the **VM Options** tab, navigate to **Advanced** > **Edit Configuration**, and set **disk.EnableUUID** to *TRUE*

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2505

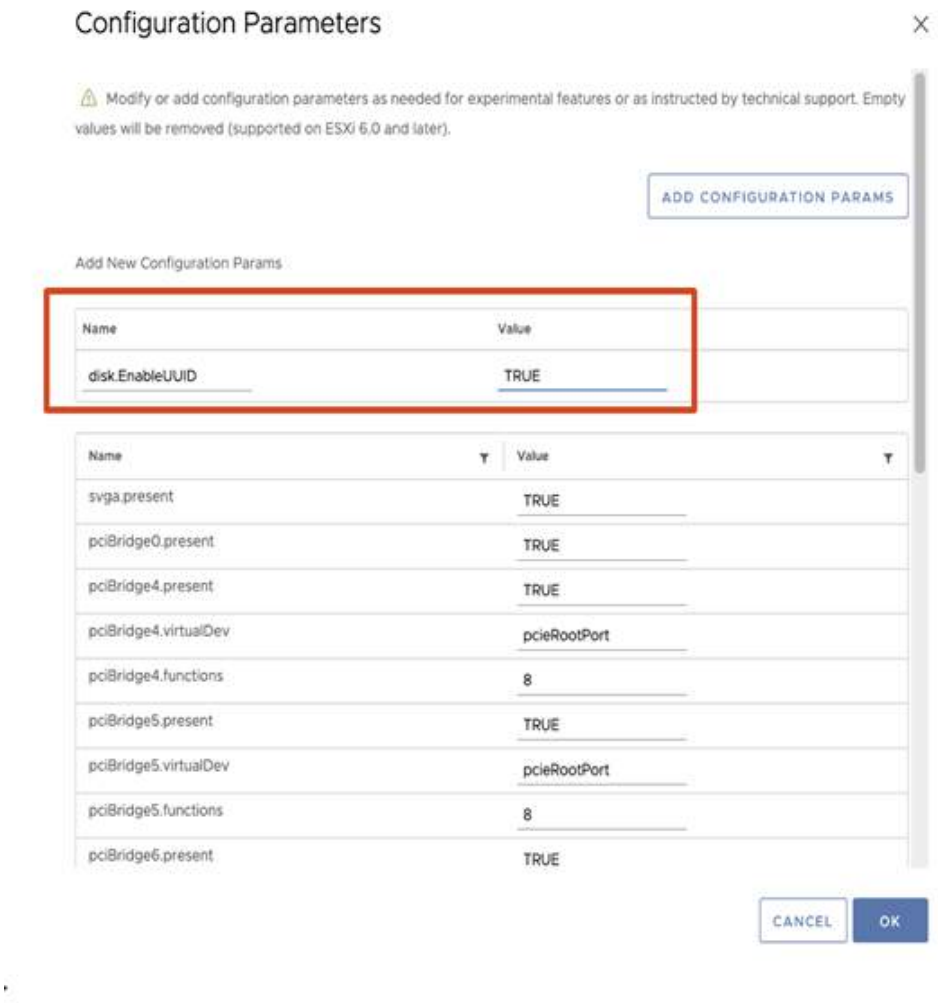


Figure 3: Enable UUID - Advanced Setting

3. Upgrade the Prism Central VM compatibility (VMX version).
   a. Right-click on the Prism Central VM, and navigate to **Compatibility** > **Upgrade VM Compatibility**.
   b. Set the **Compatible with** field to the **ESXi 7.0 U2 and later**.
   c. Power on the Prism Central VM.
4. Configure the vCenter settings.
   a. Create a tag and a category. Map the category to the tag
   b. Assign the tag to the datastore hosting the Prism Central VM
   c. Create a new VM storage policy and assign it to the newly created tag.
   For more information, see vSphere Tags and Attributes in *VMWare vSphere documentation*.

   Note: Ensure that you select **Enable tag based placement rules** checkbox while defining the storage policy structure.
5. Power on the Prism Central VM through the vSphere Client. Click **ACTIONS** > **Power** > **Power On** to start the VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2506

6. Set up the `setup_three_tier` tool.

   a. Log on to the Nutanix Support portal and browse to the Microservices Platform (MSP) page.

   b. Download the CSI bundle and extract its contents into the /home/nutanix/data directory on the Prism Central VM.

      The CSI bundle contains essential tools such as `CredHelper` and `setup_three_tier`.

      > **Note:** The CSI bundle supports ESXi version 7.0.3 or later.

      Extract the vSphere CSI bundle tar.xz file by running the following command.

      ```
      nutanix@pcvm$ cd /home/nutanix/data
      nutanix@pcvm:/data$ tar -Jxvf vsphere_csi_bundle.tar.xz
      ```

Upgrading Prism Central in Non-Nutanix Environment

This section describes how to upgrade Prism Central in the non-Nutanix environment (with ESXi hypervisors).

Before you begin

Ensure that you set up the upgrade environment before you run the upgrade tool (`setup_three_tier` tool). For more information, see Setting Up the Upgrade Environment on page 33.

About this task

> **Note:** Nutanix does not support deploying a large Prism Central in a non-Nutanix environment. Increasing the size of a Prism Central in a non-Nutanix ESXi environment to large Prism Central is also not supported. Nutanix recommends that you consider deploying Prism Central on a Nutanix cluster if your environment requires a large Prism Central.

Procedure

To upgrade Prism Central to pc.2024.1 and later versions, perform the following steps:

1. SSH to the Prism Central VM and run the `setup_three_tier` tool.

   ```
   nutanix@pcvm$ /home/nutanix/data/vsphere_csi_bundle/tools/setup_three_tier
   ```

   The system prompts you to enter the vCenter IP, vCenter port, user credentials, datacenter name, and storage policy name.

2. Enter the required details.
   The system verifies the entered data, and displays the validation results.

3. Upgrade Prism Central using the appropriate method.

   For more information, see the Upgrading Prism Central on page 28 topic.

Service Manager for Installing Services and Applications

The Service Manager feature is introduced to enable the installation of Prism Central services and application in a dark site. Service Manager enables the installation only when the Prism Central MSP Apps Bundle (`pc-app-onprem` bundle) packaged with the necessary charts and images is available in the LCM web server for the installation of the following services and applications:

- Security Dashboard
- Licensing application in Prism Central Admin Center

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2507

- Batch Service

> **Note:** Ensure that the LCM web server is reachable by all the Nutanix clusters in the dark site. For information on preparing the LCM web server, see the Life Cycle Manager Guide.

Service Manager downloads the necessary charts and images for the installation from the Prism Central MSP Apps Bundle that is placed in the LCM web server. The charts and images for the mentioned services are available in the LCM (Open Container Initiative-compliant) container registry, also called the LCM OCI registry.

Initiating Service Manager for a New Prism Central Installation

This section describes how to initiate Service Manager when you install Prism Central in a dark site for the first time.

Before you begin

Ensure that you have the following bundles in the dark site LCM web server.

- The Prism Central LCM Bundle
- The Prism Central MSP Apps Bundle that contains the necessary charts and images.

For information on preparing the LCM web server, see the Life Cycle Manager Guide.

About this task

Perform the following steps to install Prism Central with the Prism Central services and applications

Procedure

1. Install Prism Central in the dark site using the Prism Central LCM bundle.
2. Configure the LCM web server in the Prism Central Admin Center as the source for the installation bundles.

   On **Prism Central Admin Center** > **LCM** > **Settings**, select **Dark Site (Local Web Server)** in the **Source** field and provide the URL of the LCM web server in the **URL** field.
3. SSH to the Prism Central VM as a `nutanix` user, and run the following commands to restart the `pc_platform_bootstrap` service on the dark site cluster:

   ```
   nutanix@pcvm$ allssh genesis stop pc_platform_bootstrap
   ```

   This command stops the `pc_platform_bootstrap` service.

   ```
   nutanix@pcvm$ allssh cluster start
   ```

   This command restarts the `pc_platform_bootstrap` service on all the Prism Central VMs.

   Restarting the `pc_platform_bootstrap` starts the Service Manager which installs the services and applications.

Initiating Service Manager for a Prism Central Upgrade

This section describes how to initiate Service Manager when you upgrade existing Prism Central in a dark site.

Before you begin

- Ensure that you have the following bundles in the dark site LCM web server.
  - Prism Central LCM bundle
  - The Prism Central MSP Apps Bundle that contains the necessary charts and images.

  For information on preparing the LCM web server, see the Life Cycle Manager Guide.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2508

- Install Helm 3.0 for Service manager in the dark site.
- Ensure that you have configured the LCM web server in the Prism Central Admin Center as source for the upgrade bundles.

About this task

Perform the following step to install Prism Central with the Prism Central services and applications

Procedure

- Upgrade Prism Central in the dark site using the Prism Central LCM bundle.

  When you upgrade Prism Central to pc.2024.1 or later versions, Service Manager installs the services and applications using the Prism Central MSP Apps Bundle in the LCM web server.

Prism Central Overview

Prism Central provides a workspace to monitor and manage multiple clusters from a centralized environment. It runs as a separate instance that consists of either a single VM or as a three-VM scale-out architecture. For more information, see Expanding (Scale Out) Prism Central on page 573.

Prism Central provides the following functionalities:

- Platform-related functionalities that include:
  - Configuration and management of administrative activities such as Licensing, Life Cycle Manager (LCM), Identity and Access Management (IAM), Projects, Prism Central UI specific settings, and admin-specific settings, which are applicable across platforms and/or for various Nutanix Apps such as NCM Self-Service, Files, Move, Objects, Database Service, Foundation Central, or Kubernetes Management. IAM, LCM, or Projects are applicable for both Nutanix Apps and platforms.
  - Discover, deploy, and manage Nutanix Apps such as *NCM Self-Service*, *Files*, *Move*, *Objects*, *VolumesDatabase Service*, *Foundation Central*, or *Kubernetes Management* and other hybrid cloud applications (preferred partner apps) from Prism Central.
  - Facilitate consumption of pre-configured and custom apps (categorized as Other Apps) that are tailored for specific needs when Calm is deployed and licensed in the Prism Central instance.
  - Alerts and Notifications related configurations. For more information, see Configuring Alerts in Prism Central information in *Prism Central Admin Center Guide*.
  - Security-related configurations.

  For more information about all the admin-related activities that you can perform using Prism Central, see Admin Center Overview on page 53.
- Cloud Infrastructure-related functionalities that include:
  - Site-specific configurations and operations.
  - Fault and performance management operations. For more information, see Prism Central Alerts and Events Reference Guide.

  For more information, see Infrastructure Overview on page 52.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2509

- Cloud Manager-related functionalities that include accessing the Cost Governance (formerly called as Beam), NCM Self-Service and Security Central applications, and configuring Prism Intelligent Operations. For more information, see the following documentation:
  - Cost Governance
  - Self-Service
  - Security Central
  - Intelligent Operations

  Note:
  - Prism Central supports maximum 10 concurrent user sessions (UI or API or a combination of both).
  - From Prism Central version pc.2024.3 onwards, the registration dependency between Prism Central and the hosting cluster has been removed for Prism Central scaling-out, infrastructure operations, and service enablement. Now, you can deploy Prism Central on a hosting cluster and then expand your cluster, remove nodes, and enable services such as Self-service, Flow Network Security, and Intelligent Operations without registering the hosting cluster with Prism Central. A few services such as Move, Nutanix Database Service (NDB), and Nutanix Kubernetes Engine (NKE) still need the cluster to be registered with Prism Central. You need to register your cluster with Prism Central if you want to manage your cluster through Prism Central.

Logging Into Prism Central

About this task

This section describes how to log into Prism Central. The Knowledge Base article KB 1661 lists the default cluster credentials.

Procedure

To log in to Prism Central, perform the following steps:

1. Open a web browser, enter https://*prism_central_ip_addr*:9440 in the address field, and press **Enter**.
   Replace *prism_central_ip_addr* with the Prism Central VM IP address.

   Note: Prism Central supports the latest version, and the two preceding major versions of Firefox, Chrome, Safari, and Microsoft Edge browsers. The browsers must support TLS 1.2.

   The system redirects to the encrypted port (9440) and prompts you to accept the **Terms and Conditions**. The system might display an SSL certificate warning. Acknowledge the warning and proceed to the site. If user authentication is enabled and the browser does not have the correct certificate, a denied access message may appear. For the complete list of required ports, see Port Reference.

2. Click **Accept terms and conditions**. The system displays the login screen.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2510

3. Enter your Nutanix login credentials and press **Enter** or click **Log In**.

   The login credentials might vary based on the authentication mechanism configured to access Prism Central. For more information about supported authentication mechanisms for Prism Central, see Configuring Authentication information in *Security Guide*.

Figure 4: Login Screen

Note:

- If LDAP authentication is used, enter the user name in *username@domain* format; the *domain\username* format is not supported. The user principle name [UPN] attribute is used to find the user account in Active Directory, so your user name must be in that format.

  Note: If there is more than one LDAP/AD, the Prism Central login screen shows multiple boxes to select the configured domain names.

- The login page includes background animation that is enabled by default. You can modify it based on your requirement. For more information about how to configure Prism Central UI Settings, see *Prism Central Admin Center Guide*.
- If you are logging in as an administrator for the first time (user name admin and default password Nutanix/4u), the system prompts you to change the default password. Enter a new password in the **password** and **re-type password** fields and press **Enter**.

  Note: The system also prompts you to accept the license agreement if the EULA agreement is changed or you are logging in for the first time. In this case, enter appropriate information in the

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2511

Name, **Company**, and **Job Title** fields, and accept the terms and conditions for the license agreement.

The password must meet the following complexity requirements:

- At least 8 characters long
- At least 1 lowercase letter
- At least 1 uppercase letter
- At least 1 number
- At least 1 special character (allowed special characters are: "#$%&'()*+,-./:;<=>@[]^_`{|}~!)
- At least 4 characters different from the old password
- Should not be among the last 10 passwords

After you successfully change the password, the new password is synchronized across all Controller VMs and interfaces (Prism Element web console, nCLI, and SSH).

The default password expiration age for the `admin` user is 60 days. You can log in to PCVM with SSH and run the following commands to configure the minimum and maximum password expiration days based on your security requirement:

- `nutanix@pcvm$ sudo chage -M <MAX-DAYS> admin`
- `nutanix@pcvm$ sudo chage -m <MIN-DAYS> admin`
- After you upgrade from an AOS earlier version and then attempt to log in to Prism Central as the admin user, you are prompted to create a new admin user password.
- When you change the admin user password, ensure that you update any applications or scripts that uses the admin user credentials for authentication. Nutanix recommends that you create a service account with the admin role instead of using the admin user for authentication. For more information on authentication and roles, see Security Management Using Prism Central (PC) information in *Security Guide*.

Prism Central Landing Page

This section describes the functionalities available on the Prism Central landing page. The default application to be loaded in the Prism Central landing page is defined using the **Admin Center** application.

- For information about how to access the **Admin Center** application, see Application Switcher Function on page 45.
- For information about how to set the default landing page, see Prism Central Admin Center Guide.

Note: The **Main Dashboard** is the first page that appears after logging into Prism Central if the default landing page set is **Infrastructure**. For more information about **Main Dashboard**, see Main Dashboard - Infrastructure on page 80.

An example Prism Central landing page when **Infrastructure** is set as default landing page:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2512

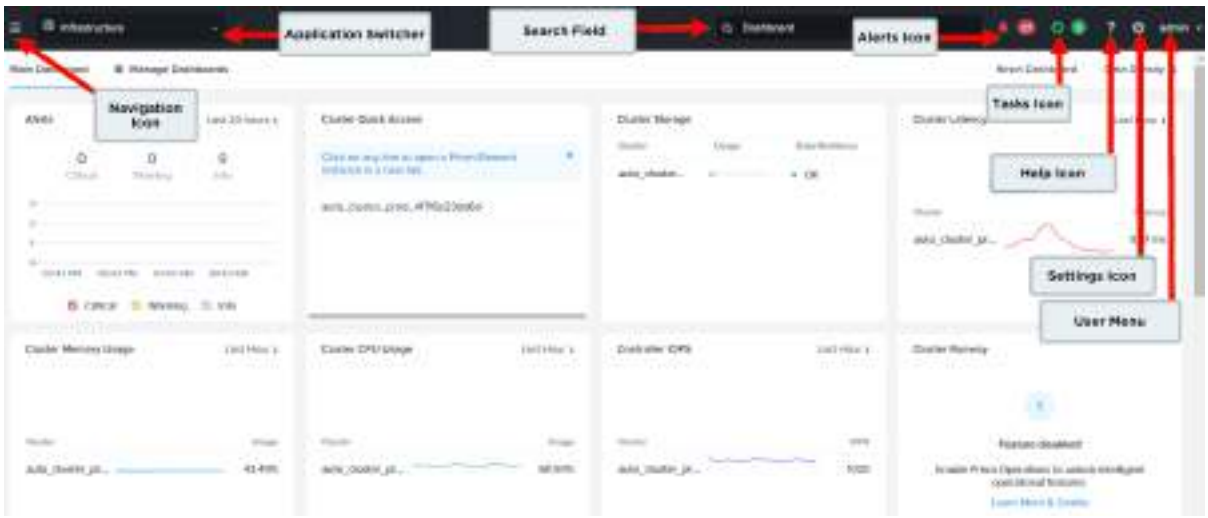


Figure 5: Prism Central Landing Page

Icons in Prism Central UI

The following table describes the list of icons used in Prism Central UI for accessibility, navigation, configuration, and observation purposes:

Table 4: Icons - Prism Central UI

Icon	Name	Description
	Alerts icon	The Alerts icon appears on the right of the Prism Central landing page. Select the Alerts icon to display the alert messages that are raised by the system. For more information about Alerts, see Prism Central Alerts and Events Reference Guide.
	Tasks icon	The Tasks icon appears next to the alerts icon on the Prism Central landing page. Select the tasks icon to view the running or completed tasks. The system displays the tasks data of the last 48 hours. You can also select **View All Tasks** at the bottom of the list to display all the tasks. For more information, see Tasks View on page 452. You can also navigate to **Activity** > **Tasks** from the **Navigation Bar** to view the **Tasks** page. **Note:** If one or more of those tasks do not complete successfully, the tasks icon turns yellow (warning) or red (failure). The tasks icon turns blue color when all the tasks are running properly or completed successfully. Select the Tasks icon to see a list of the current tasks.
	Help icon	The help icon appears on the right side of the Prism Central landing page. For more information about the help resources available in Prism Central, see Help Resources on page 44.
	Navigation icon	The navigation icon is used to access the **Navigation Bar** for the selected Prism Central application. For more information, see Navigation Bar on page 44.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2513

Icon	Name	Description
	Search icon	The Search icon appears on the right of the Prism Central landing page. Enter a string in this field to search for relevant content in Prism Central. For more information, see Searching for Information on page 70.
	Bookmark icon	The Bookmark icon is used for quicker access to a specific page or filtered entry. When you bookmark a page or a filtered entry, the system displays that page or filtered entry under **Bookmarks** in **Navigation Bar**.
	Settings icon	The Settings icon appears on the right side of the Prism Central landing page. Click the Settings icon to view the **Prism Central Settings** page for the **Infrastructure** application. For more information about list of settings available for the **Infrastructure** application, see Prism Central Settings (Infrastructure) on page 49. **Note:** The Settings icon also appears in some entities page such as **Alerts** page to enable alert emails and specify the email addresses to which alerts should be sent. For more information, see Prism Central Alerts and Events Reference Guide. You can also access the **Prism Central Settings** page from the **Navigation Bar**.
	Add icon	The Add icon is used to add an entry in a list of allowed entries.
	Remove icon	The Remove icon is used to remove an entry from the list of allowed entries.
	Label icon	The Label icon is used to create a label for the selected entity items.
	Edit icon	The Edit icon is used to modify an existing entry.
	Delete icon	The Delete icon is used to delete an existing entry.
	Share icon	The Share icon is used to share the information with any Prism Central user.
	Power icon	The Power icon is used to select the following VM power options in the VM console: • Power off • Power cycle • Reset • Guest shutdown • Guest reboot. For more information about the VM Power options, see Managing a VM through Prism Central (AHV) on page 143.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2514

Icon	Name	Description
	Launch icon	The Launch icon is used to launch the VM console.
	Reboot icon	The Reboot icon is used to send a **Control-Alt-Delete** command to the VM console.
	Screenshot-capture icon	The Screenshot-capture icon is used to take the screenshot of the VM console display.
	Back icon	The Back icon is used to return to the previous page.

Navigation Bar

The **Navigation Bar** enables you to view and select the required configuration options for the selected application.

For information about the **Navigation Bar** applicable for a specific Prism Central application, see Application-specific Navigation Bar on page 66.

For information about the applications available in Prism Central and how to access any application, see Application Switcher Function on page 45.

You can select **Lock Navigation Bar** to lock and **Unlock Navigation Bar** to unlock the **Navigation Bar**. It is a toggle. When the **Navigation Bar** is locked, it remains open all the time when you switch between multiple configurations on the Prism Central landing page.

Help Resources

The following table describes the help resources available when you select the help icon:

Table 5: Help Resources

Name	Description
Learn about search	Displays search guidelines. For more information, see Searching for Information on page 70.
Help with this page	Opens the online help that describes the current page. For more information, see Accessing Online Help (Prism Central) on page 594.
Online Documentation	Opens the online help at the introduction page. For more information, see Accessing Online Help (Prism Central) on page 594.
Support Portal	Opens a new browser tab (or window) at the Nutanix Support portal logon page. For more information, see Accessing the Nutanix Support Portal (Prism Central) on page 590.
Nutanix Next Community	Opens a new browser tab (or window) at the Nutanix Next Community entry page. For more information, see Accessing the Nutanix Next Community on page 595. The portal is an online community site for customers and partners to exchange ideas, tips, and information about Nutanix technologies and related data center topics.
Create Support Case	Opens the **Create a new support case** page to view or create support cases with Nutanix customer support. For more information, see Creating a Support Case on page 586.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2515

Application Switcher

The application switcher enables you to select the relevant application to perform any task or operation. For more information, see Application Switcher Function on page 45.

User Menu (<user_name>)

The <*user_name*> indicates the user identity such as admin, nutanix, or any configured user identity who is logged into the Prism Central. It appears on the far right side of the Prism Central landing page.

For information about how to define the Prism Central users, see Controlling User Access (RBAC) information in *Security Guide*. Select <*user_name*> to display a list of options to update your user account, log off from Prism Central, and other miscellaneous tasks.

The following table describes the options available in the <*user_name*> dropdown menu.

Table 6: User Menu Options

Name	Description
Change Password	Opens the **Change Password** window to update your password. For more information, see Updating My Account in *Security Guide*.
Update Profile	Opens the **Update Profile** window to update your user name and email address. For more information, see Updating My Account in *Security Guide*.
Download Cmdlets Installer	Downloads the PowerShell installer for the Nutanix cmdlets. For information about installing the cmdlets locally and for cmdlet descriptions, For more information, see Powershell Cmdlets Reference.
Download nCLI	Downloads the Nutanix command-line interface (nCLI) as a zip file to your local system. The download occurs immediately without additional prompts after you select this option. For more information about installing the nCLI locally and for nCLI command descriptions, see Command Reference.
REST API Explorer	Opens a new browser tab (or window) at the Nutanix REST API Explorer web page. For more information, see Accessing the REST API Explorer on page 593.
About Nutanix	Opens the **About Nutanix** window that displays Nutanix operating system (AOS) and other version information. For more information, see Finding the Prism Central Version on page 571.
Nothing To Do?	Opens a game that is strictly for entertainment. To quit the game, select "X" at the upper right of the screen.
Sign Out	Logs you out of Prism Central. For more information, see Logging Out of Prism Central on page 584.
Adjust Contrast (Chrome only)	Displays a contrast setting box at the bottom of the screen where you can set the Prism Central display to **Normal** (default) or **High** contrast. **Note:** This option is available only when you access Prism Central using the Chrome browser.

Application Switcher Function

The Application Switcher function facilitates you to seamlessly switch between following configuration module applications:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2516

- **Platform Services** module applications that include:
  - **Admin Center** - Select this to perform admin-related tasks, activities, and configurations. For information about the administrative tasks that you can perform using **Admin Center**, see Admin Center Overview on page 53.
  - **Apps and Marketplace** - Select this to directly access the application deployment and application management functionalities in Admin Center. For more information about the application types and deployment, see the Marketplace information in *Prism Central Admin Center Guide*. For more information about application management, see the My Apps information in *Prism Central Admin Center Guide*.

    Note: When you select **Apps and Marketplace** from the application switcher, the system redirects you to the **Admin Center** application with display of **Marketplace** menu.
- **Cloud Infrastructure** module applications that include:
  - **Infrastructure**. This document covers the complete information about **Infrastructure** application.
  - **Kubernetes Management** *(formerly called Karbon)*- Provides simplified provisioning and operations of Kubernetes clusters. Kubernetes is an open source container orchestration system for deploying and managing container-based applications. For more information, see Nutanix Kubernetes Engine documentation.
  - **Foundation Central** - Enables you to create clusters from factory-imaged nodes and re-image existing nodes that are already registered with Foundation Central, remotely from Prism Central. For more information, see Foundation Central Documentation.
- **Cloud Manager** module applications that include:
  - **Intelligent Operations** *(formerly called Prism Pro/Ultimate)*- Optimizes capacity, proactively detects performance anomalies, and automates operations tasks with ease and confidence. For more information, see Intelligent Operations Guide.
  - **NCM Self-Service** *(formerly called Calm)*- Allows you to seamlessly select, provision, and manage your business applications across your infrastructure for both the private and public clouds. Calm provides application automation, Life Cycle Management (LCM), monitoring, and remediation to manage the heterogeneous infrastructure, for example, VMs or bare-metal servers. For more information, see Self-Service documentation.
  - **Cost Governance** *(formerly called Beam)*- Allows you to cost govern your resources using our pre-built TCO model to govern the spending of business units or cost centers. For more information, see Cost Governance documentation.
  - **Security Central** *(formerly called Flow Security Central)*- A cloud based offering that provides complete visibility into the security posture and compliance of your multi-cloud environment (Nutanix, Azure and AWS). For more information, see Security Central documents.
- **Unified Storage** module applications that include:
  - **Files** - A software-defined, scale-out file storage solution that lets you share files in a centralized and protected location to eliminate the requirement of a third-party file server. For more information, see Files documentation.
  - **Objects** - A software-defined Object Store Service that is designed with an Amazon Web Services Simple Storage Service (AWS S3) compatible REST API interface capable of handling petabytes of unstructured and machine-generated data. Objects addresses storage-related use cases for backup, and long-term retention and data storage for your cloud-native applications by using standard S3 APIs. For more information, see Objects documentation.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2517

- **Database Services** module that includes:
  - **Move** - A cross-hypervisor mobility solution to move VMs with minimal downtime. For more information, see Move User Guide.
  - **Database Service** - The Nutanix Database Service (NDB) automates and simplifies database administration, bringing one-click simplicity and invisible operations to database provisioning and life-cycle management. It also enables you to perform operations such as database registration, provisioning, cloning, patching, and restore. It allows administrators to define provisioning standards with end-state driven functionality that includes network segmentation and high availability (HA) database deployments. For more information, see Nutanix Database Service User Guide.

Note:

- In a new deployment of Prism Central, the Application Switcher displays the **Admin Center**, **Infrastructure**, **Apps and Marketplace**, **Cost Governance**, and **Security Central** applications for users with the Nutanix admin role. You can view the Nutanix Apps in the Application Switcher after you enable them from the Marketplace.

  For information about how to deploy apps from Prism Central, see Nutanix Apps Deployment information in *Prism Central Admin Center Guide*.
- If you have upgraded to the current version of Prism Central, you can view all Nutanix Apps that you enabled in the previous version along with the **Admin Center**, **Infrastructure**, **Apps and Marketplace**, **Cost Governance**, and **Security Central** applications.
- For users with the non-admin role, the Application Switcher displays the applications based on the access policies. For example, a user with a system-defined consumer role can view only **Infrastructure**, **Apps and Marketplace**, and any other Nutanix Apps for which the access is provided to the user.
- You cannot add any custom applications to the Application Switcher.

Select the relevant application option to perform the configurations required at your site. The following is an example displaying the application options available through the Application Switcher function of Prism Central:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2518

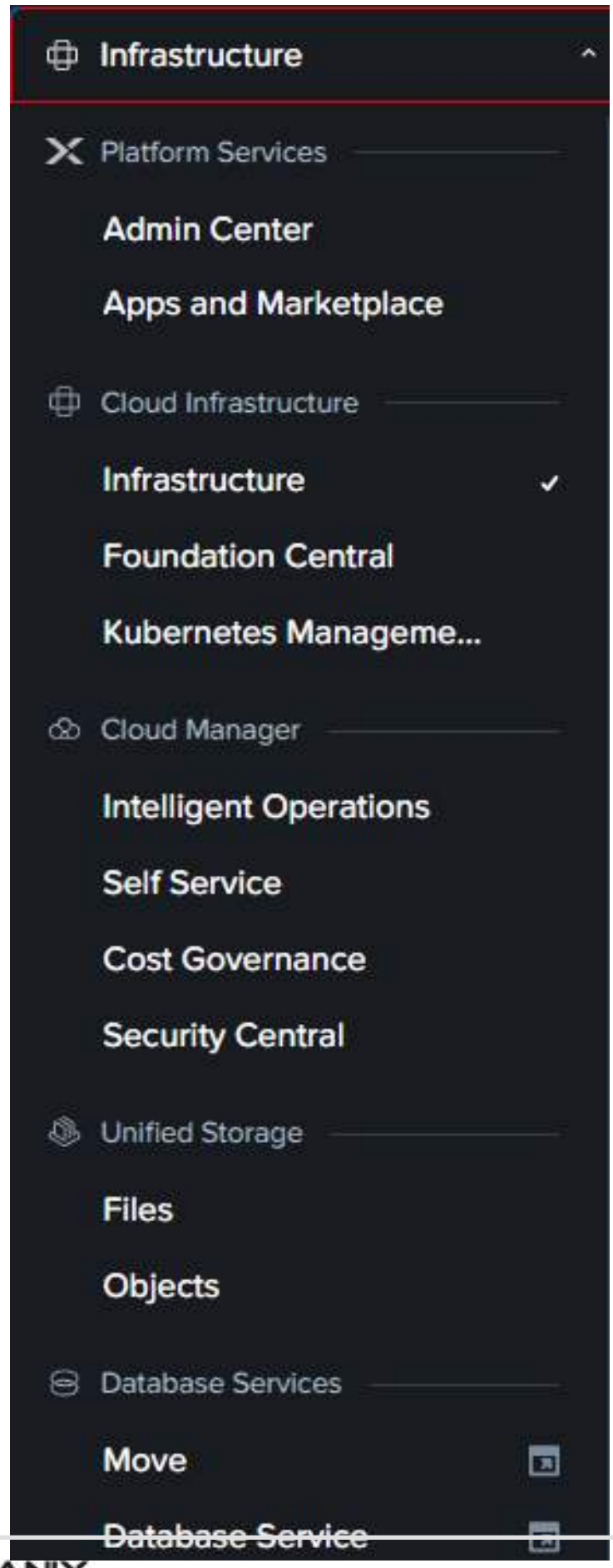


Figure 6: Application Switcher Options

Anexo Catalogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2519

Important:

The Domain Manager container serves the Prism Central UI and API calls for the new Prism Central experience and is a repository for all deployed applications such as application switcher, Admin Center, Marketplace, deployed apps, and other Prism Central services.

If the Domain Manager container is not accessible, the application switcher function becomes non-functional. However, you can use the fallback URLs to access the deployed apps, **Infrastructure** application, **Marketplace** application, and other Prism Central services. For more information, see KB-14217.

Prism Central Settings (Infrastructure)

The **Settings** page of the **Infrastructure** application enables you to configure the **Prism Central Settings** for infrastructure-specific services. You can access the **Settings** page using any of the following mechanisms:

- Click the Settings icon on the Prism Central Landing page. For information about Prism Central landing page, see Prism Central Landing Page on page 41.
- Navigate to **Prism Central Settings** from the **Navigation Bar** of **Infrastructure** application. For more information about the **Navigation Bar** of Prism Central applications, see Application-specific Navigation Bar on page 66).

The **Settings** page displays a list of tasks that you can perform for the **Infrastructure** application. Click the required task to open the window or page for that task.

The following is an example displaying the tasks available under **Settings** page:

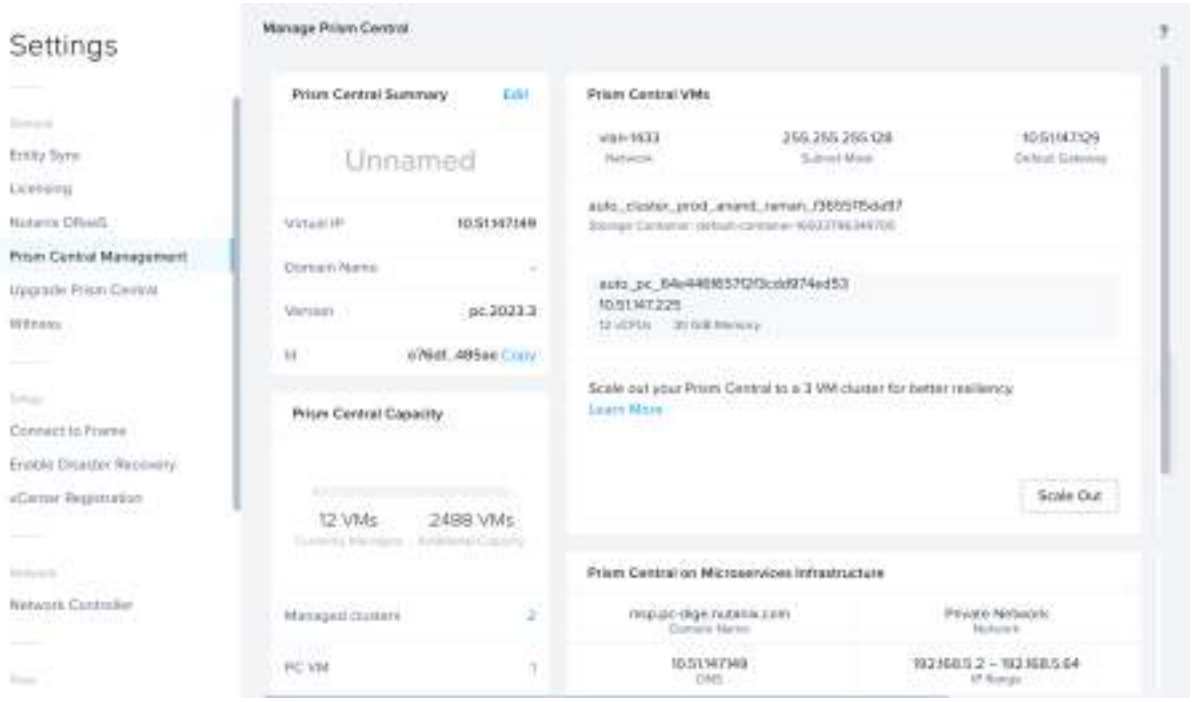


Figure 7: Settings Page - Infrastructure

The following table provides the information about all the tasks available on **Settings** page:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2520

Table 7: Settings Page Tasks - Infrastructure

Task Category	Task Name	Description
General	Entity Sync	Opens the **Force Entity Sync** page, which synchronizes entities with the specified availability zones. For more information, see Nutanix Disaster Recovery Guide.
	Licensing	Redirects to the **Licensing** page available under **Admin Center** application settings. For more information about how to access the Licensing page from Admin Center application, see Prism Central Admin Center Guide.
	Nutanix DRaaS	Opens the **Nutanix DRaaS** page to connect to DRaaS domain. For more information, see Nutanix Disaster Recovery Guide.
	Prism Central Management	Opens the **Manage Prism Central** page for viewing information about Prism Central and optionally expanding (scale out) Prism Central across multiple VMs. For more information, Managing Prism Central on page 542).
	Upgrade Prism Central	Opens the **Upgrade Prism Central** page to upgrade the Prism Central VM to a newer version. For more information, see Prism Central Deployment on page 12.
	Witness	Opens the **Witness** page. The witness service continuously monitors nodes and clusters to provide an automatic mechanism to handle any system failure. For more information about how to configure **Witness** service, see Configuring a Witness (Two-node Cluster) information in *Data Protection and Recovery with Prism Element* guide.
Setup	Enable Nutanix Disaster Recovery	Opens the **Enable Nutanix Disaster Recovery** page to enable the Disaster Recovery as a Service (DRaaS) capability. For more information, see Nutanix Disaster Recovery Guide.
	Self-Service Admin Management	Opens the **Self-Service Admin Management** page available under **Identity and Access Management** > **Settings** of **Admin Center** application. For information about how to access the **Admin Center** application in Prism Central, see Application Switcher Function on page 45. For information about the **Admin Center** application in Prism Central, see Admin Center Overview on page 53.
	vCenter Registration	Opens the **vCenter Registration** window to register (or unregister) clusters with vCenter. For more information, see External vCenter Server Integration on page 326.
Network	Advanced Networking	Opens the **Advanced Networking** page to enable the advanced networking for all On-Prem AHV Clusters in the Prism Central that runs AOS 6.1 or above acropolis version.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2521

Task Category	Task Name	Description
Flow	ID Based Security	Opens the **ID Based Security** page to add Active Directory domain services configurations and to import user groups for identity-based security policies. For more information, see Flow Microsegmentation Guide.
	Microsegmentation	Opens the **Microsegmentation** page to enable this feature, which is disabled by default. Before you can configure and use application security policies, isolation environment policies, and quarantine policies, you must enable the feature. For more information, see Flow Microsegmentation Guide.
User and Roles	Authentication	For information about User and Roles, see Security Guide.
	Local User Management	
	Role Mapping	
More Settings	For information about the settings available under **More Settings**, see Prism Central Admin Center Guide.	

Understanding Displayed Statistics

The Prism Element web console and Prism Central web console display various statistics that are derived from the following sources:

> **Note:** Most displayed statistics appear in 30 second intervals. The values in the tables represent the most recent data point within the last 30 seconds. Prism Central collects the statistical data from each registered cluster, so the process of collecting that data could result in a longer lag time for some statistics displayed in Prism Central.

1. *Hypervisor*: Hypervisor provides usage statistics only. The support to provide usage statistics is available only in ESXi, and not in Hyper-V and AHV hypervisors. If the cluster consists of Hyper-V or AHV hypervisor, the controller provides the usage statistics.

   > **Note:** Ensure that you consider the usage statistics reported from ESXi hypervisor in both Prism Central and Prism Element, only when it matches with the usage statistics in vCenter.

2. *Controller (Stargate)*: When hypervisor statistics are unavailable or inappropriate, the Controller VM (CVM) provides the statistics from Stargate. For more information about Stargate, see Nutanix Bible. The Controller-reported statistics might differ from those reported by the hypervisor for the following reasons:

   - An NFS client might break up large I/O requests into smaller I/O units before issuing them to the NFS server, thus increasing the number of operations reported by the controller.
   - The hypervisor might read I/O operations from the cache in the hypervisor which are not counted by the controller.

3. *Disk (Stargate)*: Stargate can provide statistics from both controller and disk perspective. The controller perspective includes reading both I/O operations from memory and disk I/O operations, but the disk perspective includes only disk I/O operations.

   > **Note:** The difference in statistics derived from the sources: Hypervisor, Controller, and Disk, only applies to storage-related statistics such as IOPS, latency, and bandwidth.

The following field naming conventions are used in Prism Central to identify the information source:

- A field name with **Controller** word indicates the statistic is derived from the controller (for example *Controller IOPS*).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2522

- A field name with **Disk** word indicates the statistic is derived from the disk (for example *Disk IOPS*).
- A field name without **Controller** or **Disk** word indicates the statistic is derived from the hypervisor. For example **IOPS**.

For VM statistics in a mixed ESXi/AHV cluster, the statistics source depends on the type of hypervisor that hosts the VM. If the Hypervisor is:

- ESXi - The hypervisor is the source for statistics.
- AHV - The controller is the source for statistics.

> **Note:**
>
> - The overview, VM, and storage statistics are derived from either the hypervisor or controller.
> - Hardware statistics are derived from disk.
> - Metrics in the analysis page are derived from any of the sources: hypervisor, controller, or disk, based on the type of metric.

The following table provides the information about the source for various statistics based on hypervisor type:

Table 8: Source for Displayed Statistics

Hypervisor Type	Statistics	Source	Analysis
ESXi	Overview, VM, and Storage	Both Hypervisor and controller	Metric dependent
		Controller for some storage statistics only	
	Hardware	Disk	
Hyper-V	Overview, VM, and Storage	Controller	
	Hardware	Disk	
AHV	Overview, VM, and Storage	Controller	
	Hardware	Disk	
Citrix Hypervisor	Overview, VM, and Storage	Controller	
	Hardware	Disk	
Mixed (ESXi + AHV)	Overview, VM, and Storage	Hypervisor	
	Hardware	Disk	

Infrastructure Overview

The **Infrastructure** application of Application Switcher Function on page 45 enables you to configure the field-specific settings required to host a cluster in Prism Central. It involves the following configurations:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2523

- Customizable main dashboard that displays summary information across the registered clusters (see Main Dashboard - Infrastructure on page 80).
- Dashboard and configuration options to manage VMs, VM templates, OVA, image placement, catalog items, storage, volume groups, Nutanix Guest Tools (NGT), and vCenter server across the registered clusters (Compute Entities on page 103).
- Dashboard and configuration options to manage subnets, network connections, Virtual Private Clouds (VPC), floating IPs, Virtual Private Network (VPN) connections, and security policies across the registered clusters (Network and Security Entities on page 341).
- Dashboard and configuration options to manage protection policies, recovery plans, VM recovery points, VG recovery points, and consistency groups (see Data Protection and Recovery Entities on page 395).
- Hardware component dashboards with drill-down options to view detailed information about individual clusters, hosts, disks, and GPUs across the registered clusters (see Hardware Entities on page 396).
- Activity monitors for alerts and events (see Activity Entities – Alert and Event Monitoring on page 448).
- Activity monitors for audits and tasks (see Activity Entities – Tasks and Audits on page 449).
- Dashboards to manage categories and availability zones (see Administration Entities on page 456).
- Settings menu from which you can configure Prism Central functions (see Prism Central Settings (Infrastructure) on page 49).

The **Infrastructure** application also provides the following additional functionalities for cluster and field-specific health checks:

- Fault Management based on Alerts and Events Customization. For more information on Alerts and Events, see Prism Central Alerts and Events Reference Guide.
- Detailed information about the cluster health.

> **Note:** The **Services** menu available in the earlier Prism Central versions is now retired. You can use the Application Switcher Function on page 45 to access Nutanix applications and services.

Admin Center Overview

The **Admin Center** application enables you to perform the following administrative-level tasks in Prism Central:

- Enable Marketplace in Prism Central. For more information, see Enabling Marketplace information in *Prism Central Admin Center Guide*.
- Enable Prism Intelligent Operations. For more information, *Enabling Prism Intelligent Operations* in Intelligent Operations Guide.
- Discover and deploy Nutanix apps such as NCM Self-Service (formerly known as Calm), *Files*, *Move*, *Objects*, *Database Service*, *Foundation Central*, and *Kubernetes Management*.
- Discover and deploy preferred partner apps from the Marketplace.
- Discover and deploy preconfigured and custom apps (Other Apps) when NCM Self-Service (formerly known as Calm) is deployed and licensed in the Prism Central instance.
- Manage all deployed apps from a common workspace.
- Define multiple projects as per the field requirements.
- Manage Nutanix applications License.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2524

- Define users, roles, and set up authentication mechanism for Identify and Access Management (IAM).

  Note: Prism Central provides the Self Service feature that allows you to create projects where the consumers of the IT infrastructure can provision and manage VMs in a self-service manner, without engagement of IT in day-to-day operations. The consumers of the IT infrastructure within an enterprise include individual users, development teams, test teams, and DevOps teams. Only a Prism Central administrator can create a self-service administrator role.

  For information about the roles and functions for Prism Central Self Service, see Prism Self Service Setup on page 530.

- Perform inventory and software updates as part of the Life Cycle Manager (LCM) functionality.
- Set welcome banner, language, default landing page, and other UI settings for Prism Central.
- Security management using Cluster Lockdown and SSL Certificate mechanisms.
- Define email aliases, SMTP server, and Syslog server to receive alerts and notification from Prism Central.
- Define network management guidelines for Prism Central using HTTP Proxy, Name server, NTP server, and SNMP settings.

For more information about **Admin Center**, see Prism Central Admin Center Guide.

Prism Central GUI Organization

This section provides the information about the GUI-related functionalities of Prism Central, how the Prism Central GUI is organized, and how to perform GUI-specific operations in Prism Central.

Entity Layout

In Prism Central GUI, you can access the entities from the **Navigation Bar** using the Navigation icon. For information about the **Navigation Bar**, see Prism Central Landing Page on page 41.

The entities are categorised into the following types:

- Compute Entities on page 103
- Network and Security Entities on page 341
- Data Protection and Recovery Entities on page 395
- Hardware Entities on page 396
- Activity Entities – Alert and Event Monitoring on page 448
- Activity Entities – Tasks and Audits on page 449
- Operations Entities on page 455
- Administration Entities on page 456

  Note: The **Services** menu available in the earlier Prism Central versions is now retired. You can use the Application Switcher Function on page 45 to access Nutanix applications and services.

When a list appears for the selected entity, the display may include:

- Entity tabs, **Actions** options (if any), **Group by** options, and **View by** options for the list, and a **Modify Filters** option on the far right. When you click **Modify Filters** option, the **Filters** pane appears.
- A query field that identifies the filters (if any) being applied to the list. This field displays all filter options that are currently in use. It also allows for basic filtering on the entity name.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2525

- A table (list) of entities. The table content is determined based on the **Group by**, **View by**, and **Modify Filters** options.

  > **Note:** By default, the system displays 20 rows of entity items per page. The system also provides you an option to configure the display with a different number of rows per page between 10 to 60. To specify a different number for rows per page, click *X* **Rows**, where x indicates the number such as 10, 20, 30, 40, 50, and 60.

- An export mechanism to download the table contents in CSV format with a maximum of 1000 rows. Click **Export** to download the table contents on your local machine.

Figure 8: Entity Layout (example)

Entity Tabs

Each entity provides relevant tabs such as **Summary, List, Policies, Alerts, Events, Audit, Metrics, Scenarios, Gateway, VPN connections, Subnet Extensions,** and **BGP Sessions**, to perform entity-related configurations and observe entity related-activities.

> **Note:** For some entities, no tab appears and the relevant content appears directly in the main page of the selected entity.

Sort Function

The sort function allows you to sort the entries in alphabetic or ascending-descending order. This function appears for the Tiles and Circles views only; ordering in the Grid (tabular) view is accomplished when you click a column header.

Filters Pane

Click **Modify Filters** option to display the **Filters** pane.

The **Filters** pane include a set of fields that vary according to the selected entity. When you type the desired field values in the **Filters** pane, an entry appears in the search field for each value you enter.

> **Note:**
>
> - You can bookmark (or save) a filter using the Bookmark icon in the search field. The selected filter is saved under **Bookmarks**. To remove the bookmarked filter, navigate to **Bookmarks** from the **Navigation Bar**, and click the Bookmark icon for the saved filter.
> - Numeric filters have **To/From** fields to specify a range. You can specify the numeric values along with units in these fields. For example, the filter adjusts the scale accordingly when you type in "10 K" or "100 M".

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2526

To apply a filter, enter a value or select the checkbox of the desired value (or multiple values) for the field you want to use as a filter . You can apply filters across multiple parameters. Some parameter filters require additional context such as a constraint string or a range.

The following is an example displaying the **Filters** pane:

Figure 9: Filters Pane

Group by

The **Group by** option enables you to organize the entity information based on attributes such as Cluster, Hypervisor, Power State, vCPU, Health, Type, Name, and so on. The **Group by** options vary based on the selected entity.

View by

The **View by** option enables you to specify the following view types for the displayed information:

- **General** - Displays a set of general information parameters.
- **Performance**- Displays a set of performance-specific parameters.
- **Anomalous Behavior** - Displays the Anomalous behavior. For example, Anomaly count of the VMs.
- **Efficiency** - Displays a set of efficiency-related parameters. **Efficiency** is determined through the VM behavioral learning engine. For more information, see Behavioral Learning Tools information in *Intelligent Operations Guide*.
- **GPU** - Displays a set of GPU-specific parameters.
- **Data Protection** - Displays a set of data protection-related parameters.
- **Storage Configuration** - Displays a set of storage configuration-related parameters.

> **Note:** The **General** view type is available for all entities, but the other options are available only if it is applicable for an entity.

In addition to the pre-defined view types, you can also create one or more custom view types.

To create a custom view type:

1. Click the **View by** option and select **+ Add custom**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2527

2. In the **<entity> Columns** window that is displayed, perform the following actions:
   1. Enter a name for the custom view type in the first (top) field.
   2. Click the Add icon in the left column for each entity property to be included in the custom view type. The selected entity property appears in the right column.

      Note:

      - By default, the **Name** column is already selected.
      - A maximum of 10 entity properties are allowed in a custom **View by** option including the **Name** column.
      - To arrange the order of the selected columns, hover on the column name and click the up or down arrow as appropriate.
      - To search and filter the required entity property from the list, enter the string in the Search field above the left column.
      - To remove an entity property from the custom **View by** option, click the Remove icon associated with the entity property.

   3. Click **Save** after the entity-property list in the right column is finalized.

   The following following is an example displaying the **VM Columns** window:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2528

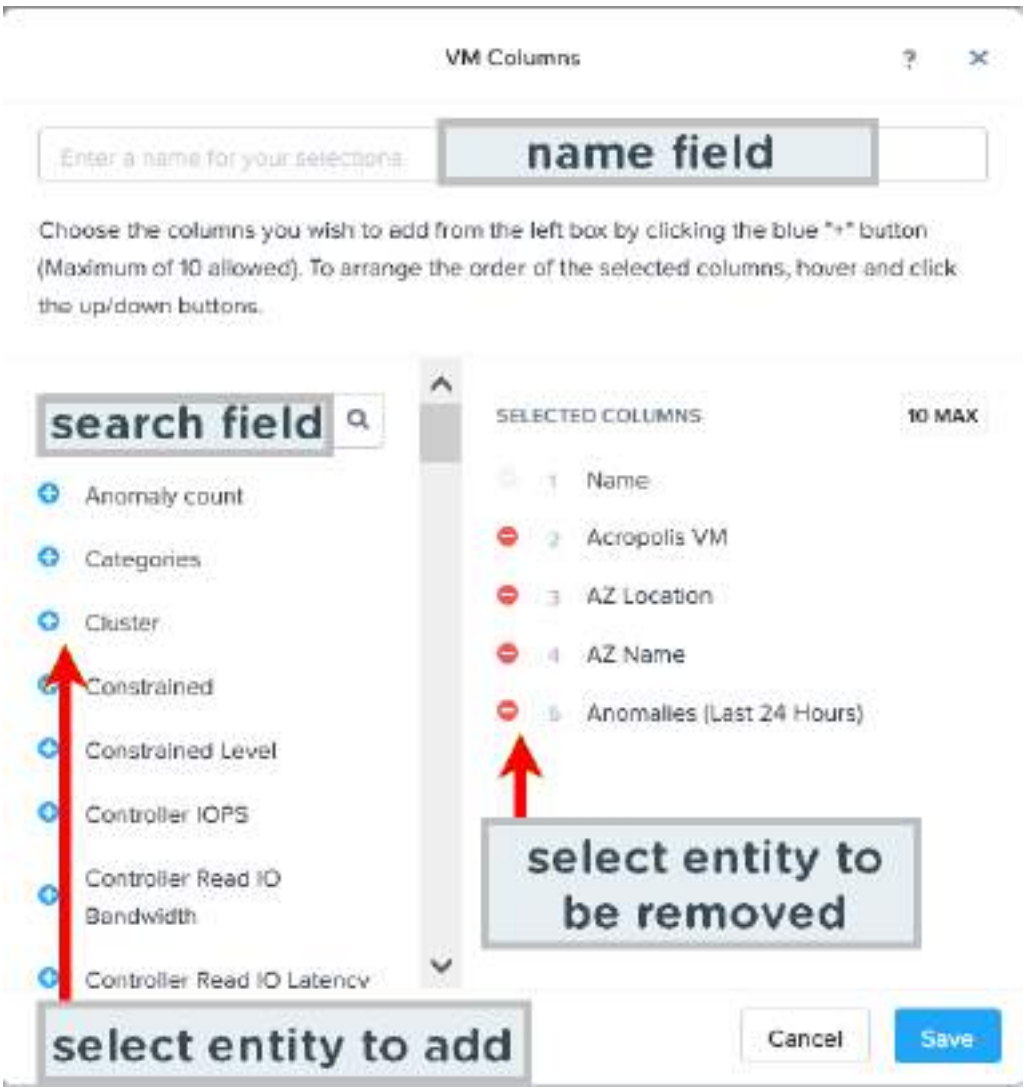


Figure 10: VM Column Window (example)

The custom view type appears (by name) in the available view types under **View By** option.

> **Note:** The custom view type appears only for the user who created it, and the administrative user and other users cannot view it.

Actions Dropdown Menu

The **Summary** page provides options to administer and categorize the entity items. The **Actions** dropdown menu is available for the selected entities in Prism Central. You can select an entity item, a set of entity items, or all entity items using the relevant checkbox available in the table list on **Summary** page. You can clear the relevant checkbox to clear a selected item from the table list.

You can also perform some administrative tasks for a cluster through Prism Element. For information about the tasks to be performed from Prism Element, see the Prism Element Web Console Guide.

> **Note:** The **Actions** dropdown list does not appear if there are no relevant actions available for the selected entity type.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2529

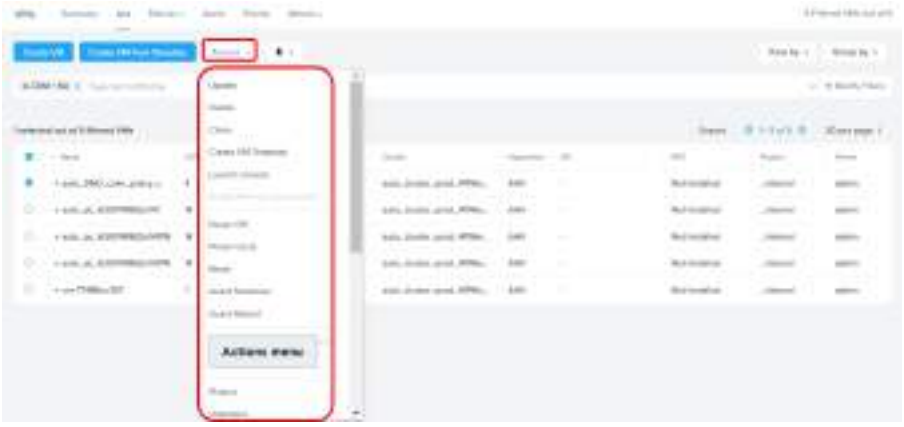


Figure 11: Action Dropdown Menu

Label

Labels enable you to create custom groupings for the entities. To add a label, click the Label icon, and enter the label name in the field. The label is applied to all the selected entity items in the table list.

> **Note:**
>
> - Only super admin and Prism admin roles have permissions to perform this operation.
> - Labels are available for VMs and clusters only.

Export

The **Export** option enables you to download the table, that contains the entity items list to a file. Click the **Export** option available on an entity item.

Entity-Related Observation Activities

The entity-related observation activities involve the following fault and performance related statistics:

- Alarms - For information on all the alarms generated in Prism Central, see Activity Entities – Alert and Event Monitoring on page 448.
- Events - For information on all the events generated in Prism Central, see Activity Entities – Alert and Event Monitoring on page 448.
- Tasks - For information on how to observe a task and its statistics in Prism Central, see Activity Entities – Tasks and Audits on page 449.
- Audits - For information on an audit activity in Prism Central, see Activity Entities – Tasks and Audits on page 449.

Prism Licensing

Nutanix provides licenses you can apply to enable a variety of features.

The Prism Central web console and Nutanix Support Portal provide the most current information on your licenses. For more information on licenses, see the License Manager Guide.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2530

X-Small Prism Central

X-Small Prism Central is a single-node Prism Central VM that is intended for small-scale deployments with limited workload.

> **Note:** You can deploy x-small Prism Central on clusters running AOS 6.8 or later versions only. X-Small Prism Central lets you manage clusters running AOS versions earlier than AOS 6.8.

For information on the type of Prism Central deployments, see the *Prism Central Scalability* topic in the release notes for the Prism Central version to be installed.

X-Small Prism Central is ideal for users who have five or fewer clusters on their site and use only the basic or essential capabilities of Prism Central. X-Small Prism Central provides the following capabilities:

- Multi-cluster management (up to 5 clusters)
- VM management
- Host management
- Infrastructure management, monitoring, and health
- Enterprise authentication and role-based access control (RBAC)
- REST APIs
- Comprehensive search
- Pulse Insights
- Life Cycle Manager (LCM)
- Prism Central backup and restore
- Categories
- Projects
- Microservices infrastructure
- Identity and access management (IAM)

Specifications

X-Small Prism Central has the following specifications:

Table 9: X-Small PC Specifications

Number of vCPU	4
Memory	18 GB
Total Storage Capacity	100 GiB

For information about the maximum tested and supported values for x-small Prism Central, see Nutanix Configuration Maximums.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2531

Limitations

- X-Small Prism Central does not support the scale-out Prism Central feature.

  For information on Prism Central scalability, see the *Prism Central Scalability* topic in the release notes for the Prism Central version to be installed.

- Adding entities to a x-small Prism Central deployment beyond the recommended number of VMs, clusters, or nodes results in an unsupported configuration. Nutanix recommends that you scale up to small, large, or x-large Prism Central deployment to increase its capacity. For more information, contact Nutanix Support.
- X-Small Prism Central does not allow you to enable the following features:

  - Flow Virtual Networking
  - Flow Network Security
  - Self-Service
  - Intelligent operations
  - Objects
  - Nutanix Kubernetes Engine
  - Nutanix Kubernetes Platform
  - Nutanix Data Services for Kubernetes (NDK)
  - Nutanix Enterprise AI
  - GPT-in-a-Box
  - Files
  - Foundation
  - Foundation Central
  - Quotas
  - Multi-site DR (available in PRO customers)
  - Marketplace
  - Reporting and Dashboards
  - Security Dashboard

  To enable these features, you must upgrade to a small, large or x-large Prism Central deployment. For more information, contact Nutanix Support.
- X-Small Prism Central does not support nearsync and synchronous replication.

Registering or Unregistering a Cluster with Prism Central

You need to register a cluster with Prism Central only if you want to manage the cluster through Prism Central.

Before you begin

- If you have never logged into Prism Central as the admin user, you must log in and change the password before you attempt to register a cluster with Prism Central. For more information, see Logging Into Prism Central on page 39.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2532

- Do not enable client authentication in combination with ECDSA certificates on a registered cluster since it causes interference when communicating with Prism Central.
- Ports 9440 and 80 need to be open in both directions between the Prism Central VM and all the Controller VMs (and the cluster virtual IP address if configured) in each registered cluster. For the complete list of required ports, see Ports and Protocols.
- If you have a proxy server configured and you want the cluster - Prism Central communication to go through the proxy, open the relevant ports on the proxy. If you do not want the communication to go through the proxy, add the Prism Central IP address to the proxy whitelist (allowlist) in the cluster settings. For more information about configuring proxy, see Configuring HTTP Proxy in *Prism Element Web Console Guide*. For the complete list of required ports, see Ports and Protocols.
- A cluster can register with just one Prism Central instance at a time. To register with a different Prism Central instance, first unregister the cluster.

About this task

To register a cluster with Prism Central, follow these steps:

> **Note:** To perform this task, ensure that you log in to the Prism Element web console as an admin user.

Procedure

1. Log in to the Prism Element web console on the target cluster.
2. To run Nutanix Cluster Checks, go to the **Health** dashboard, and from the **Actions** dropdown menu, click **Run Checks**.
3. Do either of the following:
   - » In the **Home** dashboard, click **Register or create new** from the **Prism Central** widget.
   - » Click the Settings icon, and navigate to **Setup** > **Prism Central Registration** in the **Settings** page.
4. In the **Prism Central Registration** window, click **Connect**.

   The **Prism Central Registration** window provides two options: **Deploy** and **Connect**. This procedure describes how to connect to an existing Prism Central instance. For instructions on how to deploy a new Prism Central instance, see Installing Prism Central.

   A window appears outlining what services are available through Prism Element and Prism Central.
5. Click **Next** after reviewing the message.
6. Enter the following information:
   a. **Prism Central IP**: Indicates the IP address of the Prism Central VM.
   b. **Port**: The default port number is 9440. This is an optional field. For the complete list of required ports, see Ports and Protocols.
   c. **Username**: Indicates the user name for Prism Central. You can enter admin as the Prism Central user name.
   d. **Password**: Indicates the password for the Prism Central user.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2533

7. Click **Connect** to save the values and close the window.
   The cluster is now registered with the specified Prism Central VM. After successful registration, the system allows passing information between the specified cluster and Prism Central.

   Note:

   - The user credentials provided when registering a cluster (Prism Element) with Prism Central are only used once. After registration, modifying the admin password would not impact any communication between Prism Central and the cluster.
   - On small, large, and x-large Prism Central deployments, when you register a new cluster to Prism Central, Prism Central synchronises the past 90 days of data (including multiple metrics) from the cluster. On x-small Prism Central deployments, Prism Central synchronises the past 2 hours of data (including multiple metrics) from the cluster. To view the list of metrics that are synced during registration, see the file */home/nutanix/config/arithmos/data_sender/arithmos_history.json* in the Controller VM. To view the list of metrics that are synced during a regular synchronisation between Prism Central and the cluster, see the file */home/nutanix/config/arithmos/data_sender/arithmos.json* in the Controller VM.

What to do next

Once your cluster is registered with Prism Central, you can configure various settings for network, security, and alerts. For more information, see Admin Center Settings Options.

Unregistering from Prism Central

Before you begin

Caution: Unregistering a cluster from Prism Central is not a supported workflow. The unregistered cluster might be disallowed for re-registration with a Prism Central instance.

You can use the destroy Cluster feature of Prism Central, which implicitly unregisters the cluster. For more information, see Destroying a Cluster on page 411.

If you still want to go ahead with unregistration of the cluster, consider the following points:

- Unregistering a cluster through the Prism Element web console is no longer available. This option is removed to reduce the risk of accidentally unregistering a cluster. Several features such as role-based access control, application management, micro-segmentation policies, and self-service capability require Prism Central to run your clusters. If a cluster is unregistered from Prism Central, it leads to features unavailability and configuration erasure. You can only use the following procedure from Controller VM (CVM) to unregister a cluster.
- Perform the entire registration process, followed by the cleanup process.
- Do not remove the IPs of the cluster and Prism Central from the whitelists on both sides until the unregistration process completes successfully.

If you have enabled additional applications or features in Prism Central, see the following table for recommendations before you unregister a cluster. For more information, see KB 4944.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2534

Table 10: Unregistering a cluster with additional applications enabled

Nutanix Disaster Recovery (Leap)	Before unregistering the cluster from Prism Central, you must remove any Nutanix Disaster Recovery (Leap) configuration involving virtual machines or volume groups for the cluster being unregistered. Otherwise you will not be able to manage the snapshot creation or replication policies configured on the cluster. For more information, see KB 12749. **Note:** Do not proceed with unregistration, if the stretch config (AHV Synchronous replication) is present.
Flow Networking	You must disable Flow Networking on the cluster before unregistering it from Prism Central, using the steps mentioned in Unregistering a PE from the PC in *Flow Virtual Networking Guide*. If Flow Networking is not disabled on the cluster prior to unregistering from Prism Central, attempts to enable Flow Networking in the same cluster does not work as expected. For more information, see KB 12449.
NuCalm/App Management	You must clean up Calm entities after unregistration. Contact Nutanix Support for assistance in cleaning up the CALM entities.
Prism Self Service configuration	Changes that have been made to the Prism Self Service configuration in Prism Central are lost after unregistration. Ensure that you follow the extra cleanup steps mentioned in KB 4944.
NKE Kubernetes	Do not unregister the cluster hosting an NKE Kubernetes cluster from Prism Central. Unregistration of cluster from Prism Central will prevent the management of the NKE clusters.

About this task

To unregister a cluster from an existing Prism Central instance, perform the following steps:

Procedure

1. Log in to any CVM of the registered cluster through an SSH session.
2. Run the cluster status command and verify that all services are in a healthy state.
3. Run the following command to unregister the cluster from Prism Central.

   ```
   nutanix@cvm$ ncli multicluster remove-from-multicluster external-ip-address-or-svm-ips=pc-name-or-ip username=pc-username password=pc-password
   ```

   Replace `pc-name-or-ip` with the Prism Central name or IP address and `pc-username` and `pc-password` with the login credentials for your Prism Central administrator account. If the password contains any special characters, ensure to enclose the password in single quotes. This step can take some time (though typically just a few seconds).

   If the unregistration process is successful at Prism Element cluster, you will see a task UUID in the command output. After you see the task UUID in the command output, wait for about 2 minutes to let the unregistration process complete at Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2535

4. Run the following command on Prism Element to verify if the cluster unregistration process is successful on Prism Element:

```
nutanix@cvm$ ncli multicluster get-cluster-state
```

The command output should list 0 as registered cluster count: Registered Cluster Count: 0

5. Run the following command on Prism Central to verify if the cluster unregistration process is successful on Prism Central:

```
nutanix@pcvm$ ncli multicluster get-cluster-state
```

If the command output does not include the name and UUID of the cluster you want to unregister, the unregistration process is successful. If the cluster information is still visible in the command output, refer to KB-4944 to troubleshoot the issue.

6. Run the following command to retrieve the UUID for the cluster:

```
nutanix@cvm$ ncli cluster info
```

The following output shows the **Cluster UUID** value in the cluster information output:

```
Cluster Id           : 586dd889-84dc-422f-b8e8-8ce3cd781dcf::4100682370753502671
    Cluster Uuid              : 586dd889-84dc-422f-b8e8-8ce3cd781dcf
    Cluster Name              : PC_10.51.147.185
    Cluster Version           : pc.2024.1
    Cluster Full Version      : el8.5-release-fraser-2024.1-stable-
ca1136cd25915d9b5635483235e1fd7af3ccddfb
    External IP address       : 10.51.147.185
    Is LTS                    : false
    External Data Services... :
    Support Verbosity Level   : BASIC_COREDUMP
    Lock Down Status          : Disabled
    Password Remote Login ... : Enabled
    Timezone                  : Atlantic/Reykjavik
    NCC Version               : ncc-5.0.0
    Degraded Node Monitoring  : Enabled
```

7. Log in to the Prism Central VM through an SSH session (as the *nutanix* user) and perform the following steps:

   a. Run the unregistration clean-up script.

   ```
   [pcvm]$ python /home/nutanix/bin/unregistration_cleanup.py uuid
   ```

   Replace *uuid* with the value you obtained in step 6 on page 65. This script removes all remaining registration information about that cluster and completes the unregistration process with the Prism Central VM.

   > **Note:** If you do not run the clean-up script, some artifacts continue to retain references to entities that are no longer managed by the cluster. Some artifacts that might have lost references due to the unregistration process might not be able to recover their references.

   b. Run the following command to retrieve the UUID for Prism Central:

   ```
   [pcvm]$ ncli cluster info
   ```

   Find the **Cluster UUID** value in the displayed information (see step 6 on page 65), which in this case is the UUID for Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2536

8. Go back to the CVM, and run the unregistration_cleanup.py script to complete the unregistration process on the cluster.

   ```
   nutanix@cvm$ python /home/nutanix/bin/unregistration_cleanup.py uuid
   ```

   In this case the *uuid* is the Prism Central UUID obtained in substep 7.b on page 65.

   If you do not encounter any error after running the cleanup script, you can consider that the cleanup is successful.

What to do next

Once the unregistration process is complete, you are not allowed to re-register the cluster with a new or re-created Prism Central instance. If you need to register the cluster again, see KB-15679 or contact Nutanix Support.

If the clean up process is not completed successfully, perform the following actions:

- Check the logs to indicate if there are any input errors when calling the script. The logs for the unregistration cleanup script are available under ~/data/logs/unregistration_cleanup.log.
- If any error occurred during script processing, run the cluster status command and check that the cluster services are up and running. Re-run the script and check if the script processes successfully.

> **Note:** If Prism Self Service is enabled and the unregistered cluster is set as the default cluster, you must update the default project to select a new (registered) cluster. For information about how to modify a project, see Modifying a Project information in *Prism Central Admin Center Guide*.

Application-specific Navigation Bar

Infrastructure

Select the **Infrastructure** application from the Application Switcher Function on page 45, and click Navigation icon to display the **Navigation Bar** on the left side.

The following is an example showing the **Navigation Bar** for the **Infrastructure** application:

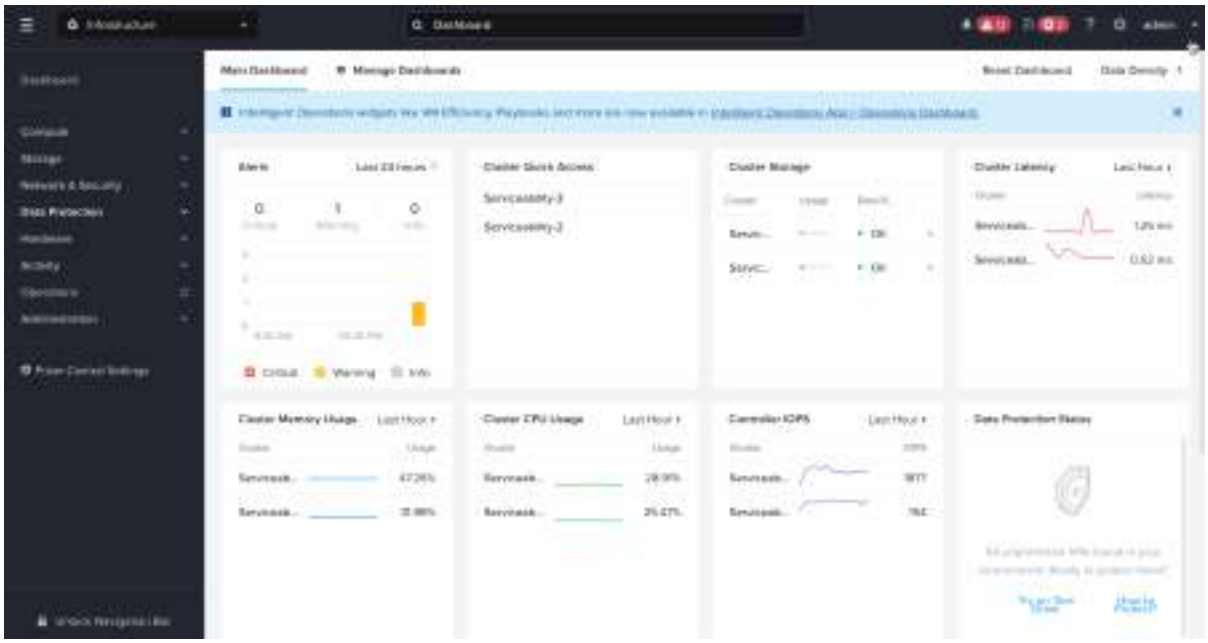


Figure 12: Navigation Bar - Infrastructure

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2537

Note:

- The **Navigation Bar** consists of **Dashboard**, **Bookmarks**, entity lists (**Compute**,**Storage**, **Network & Security**, **Data ProtectionHardware**, **Activity**, **Operations**, **Administration**, and **Prism Central Settings**.
- Click an entity list (for example, **Compute**) to display the entity items available in it.
- Click the entity item (for example **VMs**) to display the **Lists** page or the main page for that entity item.
- For quicker access to one or more entities in the entity list, you can bookmark the required entity to promote to the primary view of the **Navigation Bar** . Click the Bookmark icon displayed at the right of the entity name to bookmark the entity. The **Bookmarks** category appears below the **Dashboard**.

  Note: To remove a bookmarked entry, navigate to **Bookmarks**, and click the bookmark icon displayed at the right of the selected bookmarked item name.

The following table describes the entity list available in the **Navigation Bar** of the **Infrastructure** application:

Table 11: Entities - Infrastructure

Entities	Entity Items	Description
Dashboard		Displays the **Main Dashboard** (see Main Dashboard - Infrastructure on page 80).
Compute & Storage	VMs	Displays the VMs configuration page (see VM Management on page 103).
	Templates	Displays the Templates configuration page (see VM Template Management on page 196).
	OVAs	Displays the OVAs configuration page (see OVA Management on page 219).
	Images	Displays the Images configuration page (see Image Management on page 242).
	Catalog Items	Displays the Catalog configuration page (see Catalog Management on page 266).
	Storage Containers	Displays the Storage Containers configuration page (see Limitations for Storage Containers on page 294).
	Volume Groups	Displays the Volume Groups configuration page (see Volume Group Management on page 301).
	Storage Policies	Displays the Storage Policies configuration page (see Storage Policy Management on page 506).
	vCenter Datastores	Displays the vCenter Datastores configuration page (see External vCenter Server Integration on page 326).
Network & Security	Subnets	Displays the subnets configuration page (see Subnets Summary View on page 342).
	Virtual Private Clouds	Displays the virtual private clouds configuration page (see Virtual Private Clouds Summary View on page 357).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2538

Entities	Entity Items	Description
	Floating IPs	Displays the floating IPs configuration page (see Network and Security Entities on page 341).
	Connectivity	Displays the Connectivity configuration page (see Connectivity on page 378).
	Security Policies	Displays the Security Policies configuration page (see Security Policies Summary View on page 501).
	Security Dashboard	Displays the Security Dashboard (see Security Dashboard on page 394).
Data Protection	Protection Summary	Displays the Protection Summary dashboard for disaster recovery. (See Protection Summary on page 395).
	Protection Policies	Displays the Protection Policies configuration page (see Protection Policies on page 395).
	Recovery Plans	Displays the Recovery Plans configuration page (see Recovery Plans on page 395).
	VM Recovery Points	Displays the VM Recovery Points configuration page (see VM Recovery Points on page 395).
	VG Recovery Points	Displays the VG Recovery Points configuration page (see VG Recovery Points on page 395).
	Consistency Groups	Displays the Consistency Groups configuration page (see Consistency Groups on page 395).
Hardware	Clusters	Displays the Clusters management page (see Clusters Summary View on page 398).
	Hosts	Displays the Hosts management page (see Host Management on page 418).
	Disks	Displays the Disks management page (see Disks Summary View on page 438).
	GPUs	Displays the GPUs management page (see GPUs Summary View on page 444).
Activity	Alerts	Displays the Alerts dashboard (see Prism Central Alerts and Events Reference Guide).
	Events	Displays the Events dashboard (see Prism Central Alerts and Events Reference Guide).
	Audits	Displays the Audits dashboard (see Audits Summary View on page 449).
	Tasks	Displays the Tasks dashboard (see Tasks View on page 452).
Operations	Analysis	Displays the Analysis management page (see Analysis Dashboard in *Intelligent Operation Guide*).
	Discovery	Displays the App Discovery dashboard or the enable wizard if application discovery is not enabled (see Application Discovery in *Intelligent Operation Guide*).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2539

Entities	Entity Items	Description
	Monitoring Configurations	Displays the Monitoring Integrations dashboard or the enable wizard if monitoring integrations is not enabled (see Application Monitoring in *Intelligent Operation Guide*).
	Operations Policies	Displays the Operations Policies dashboard (see Operations Policy Management in *Intelligent Operation Guide*).
	Planning	Displays the capacity Planning dashboard (see Resource Planning in *Intelligent Operation Guide*).
	Playbooks	Displays the list of playbooks (see Task Automation-Playbooks in *Intelligent Operation Guide*).
	Reports	Displays the Reports dashboard (see Reports Management in *Intelligent Operation Guide*).
	Settings & Configurations	Displays the Settings and Configurations dashboard (see Settings & Configurations in *Intelligent Operation Guide*).
Administration	Categories	Displays the Categories dashboard (see Category Management on page 456).
	LCM	Displays the Life Cycle Manager (LCM) dashboard (see Life Cycle Manager Guide).
	Projects	Displays the Projects dashboard (see Project Overview information in *Prism Central Admin Center Guide*).
	Roles	Displays the Roles dashboard (see Security Guide).
	Users	Displays the Users dashboard (see Security Guide).
	Availability Zones	Displays the Availability Zones dashboard (see Availability Zones on page 456).
Prism Central Settings		Displays the **Settings** menu for the **Infrastructure** application (see Prism Central Settings (Infrastructure) on page 49).

Admin Center

For information about the navigation bar of **Admin Center** application, see Prism Central Admin Center Guide.

Nutanix_Apps and Other_apps

For more information about all the navigation bar of Nutanix_Apps and Other_apps that you can discover, deploy, and manage from Prism Central, refer to the application-specific documentation as described in Application Switcher Function on page 45.

Apps and Marketplace

No specific navigation bar is available for **Apps and Marketplace** option that appears in the Application Switcher. When you select **Apps and Marketplace** from the Application Switcher, the system redirects you to the **Admin Center** application with display of **Marketplace**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2540

Searching for Information

The **Infrastructure** application page includes a search field on the right (see Prism Central Landing Page on page 41) that allows you to find information about selected entities in various ways.

If you need help at any time to navigate Prism Central or apply a search filter, click the Help icon in the **Infrastructure** application page, and select **Learn about search**. This displays the **Search Guidelines** page that explains the search rules and options.

Search Basics

An *entity* is an object type such as a VM, cluster, node, security policy, project, report, event, alert, or audit. The search field is context-sensitive, which means it is populated automatically based on where you are in Prism Central. The first screen after logging on is the main dashboard, so *Dashboard* appears in the search field initially.

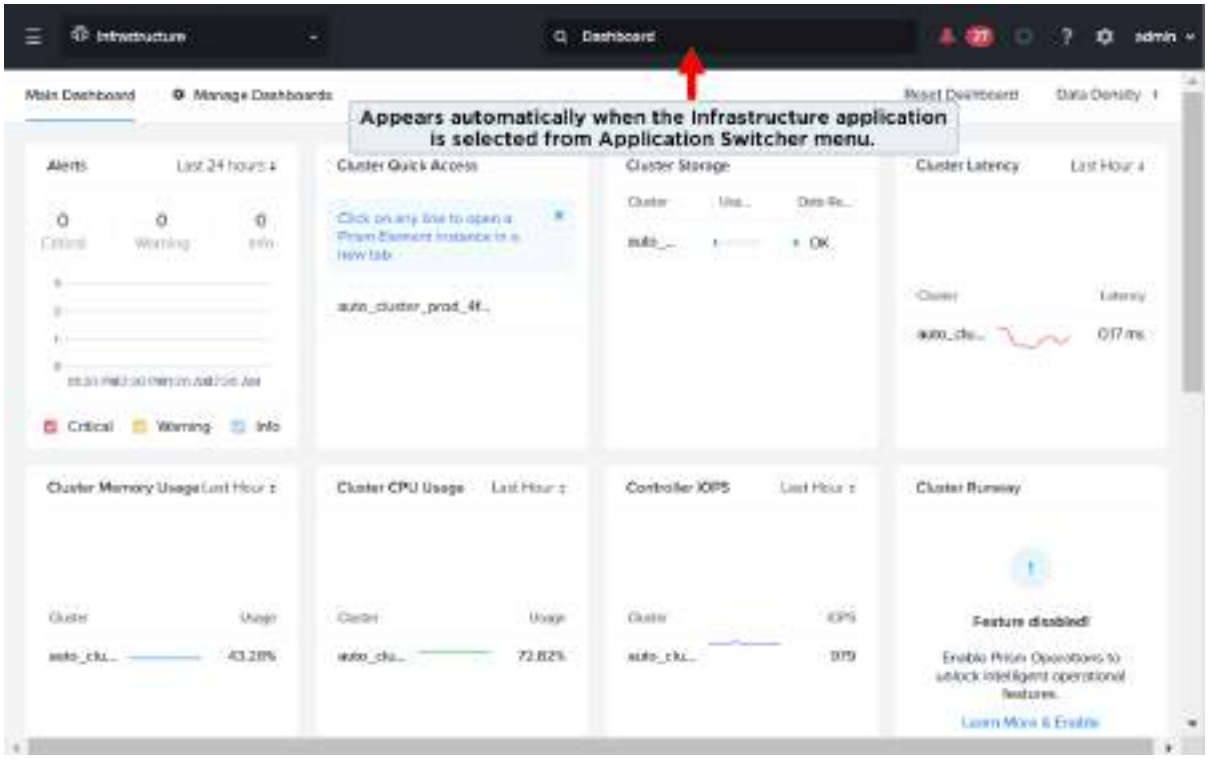


Figure 13: Search Field (Prism Central Landing page - Infrastructure)

When you navigate to different Prism Central entity pages, the search string changes automatically to match the current entity.

The following is an example showing the example of search string that appears on the VMs page:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2541

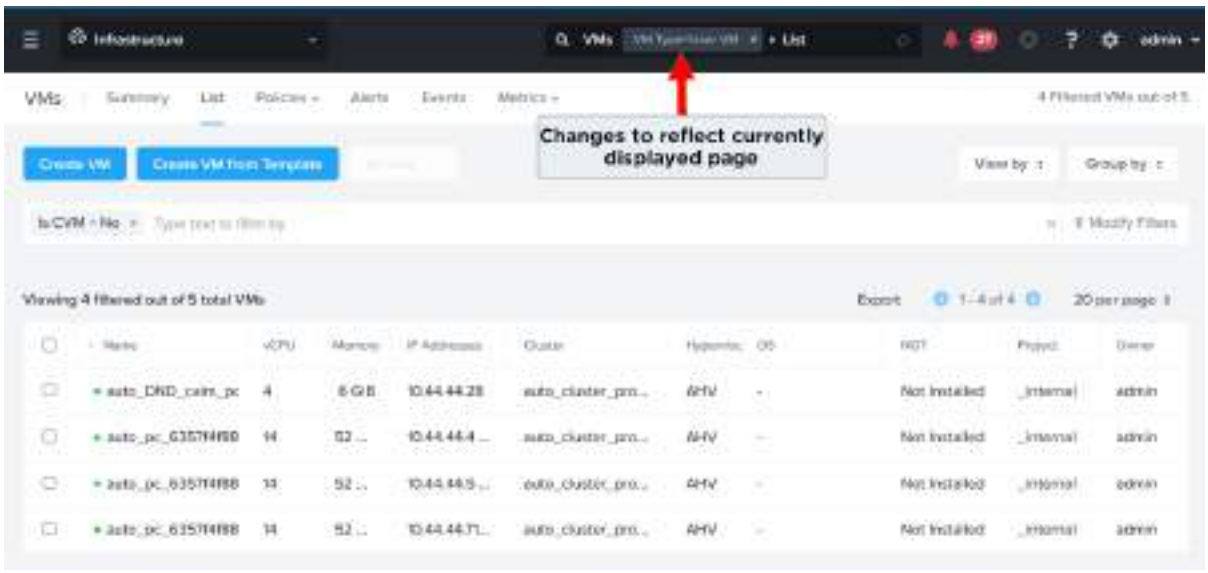


Figure 14: Search Field (Entity page)

When you enter a string in the search field, a dropdown menu appears with relevant matches across Prism Central.

> **Note:** The search strings are case insensitive.

The following is an example showing the sample dropdown menu that appears when you enter the string *VM*:

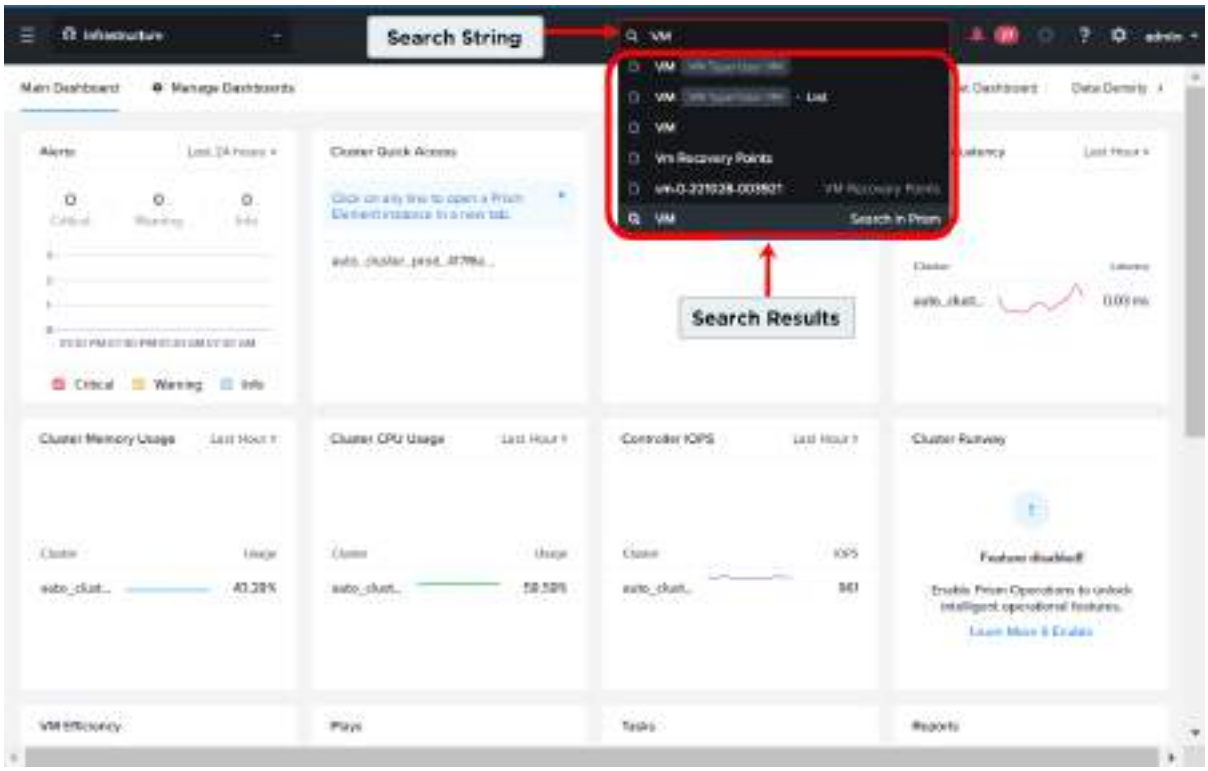


Figure 15: Search Results (for an entity type)

- *Category Value*: Select this option to display the **Category** page with any VM-related entries.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2542

- *VM Type=User VM*: Select this option to display the filtered **Summary** page for user VMs.
- *[blank]*: Select this option to display the unfiltered **Summary** page for any user VM.
- *VM Type=User VM > List*: Select this option to display the **List** page of the user VMs.
- *VM Type=User VM > Alerts*: Select this option to display the **Alerts** page of the user VMs .
- *Search in Prism*: Select this option to search across Prism Central for any information about the target entity.

  In the following example, two tables appear in the results, a list of the top VMs and a list of the top VM-related alerts. The top VMs list includes a link to the full list of VMs, and the top alerts list includes a link to the full list of alerts (which in this case is the same). When you click the VM or alert name, the system redirects you to the details page for that VM or alert.

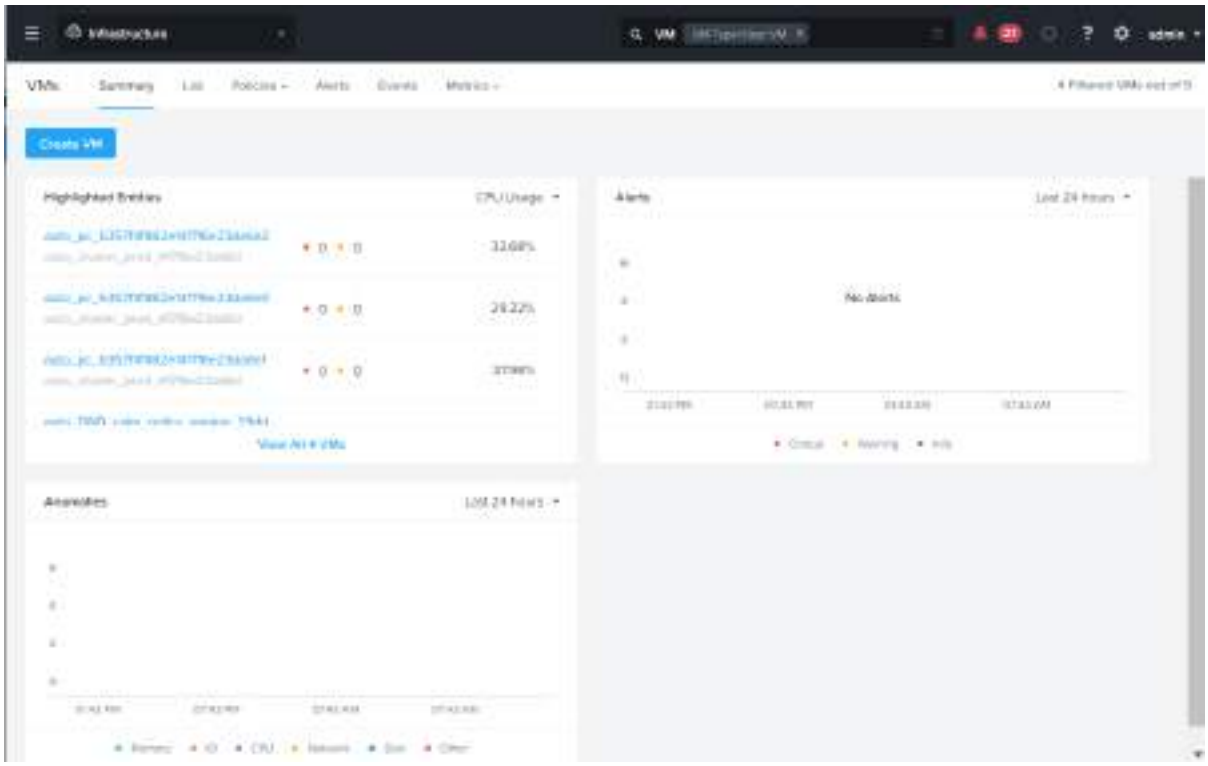


Figure 16: "Search in Prism" Results

The search is context-sensitive. You can do a quick search from your current location without entering an explicit string. For example, if you are on the user VMs summary page, clicking in the search field (or clicking the forward slash [/] character) displays the search results for user VMs. In the following example, clicking the List, Alerts, or Events entry is the same as clicking those tabs on the page. Clicking *Memory Swap* displays the Memory Swap metrics page, and *Search in Prism* displays a results page for user VMs.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2543

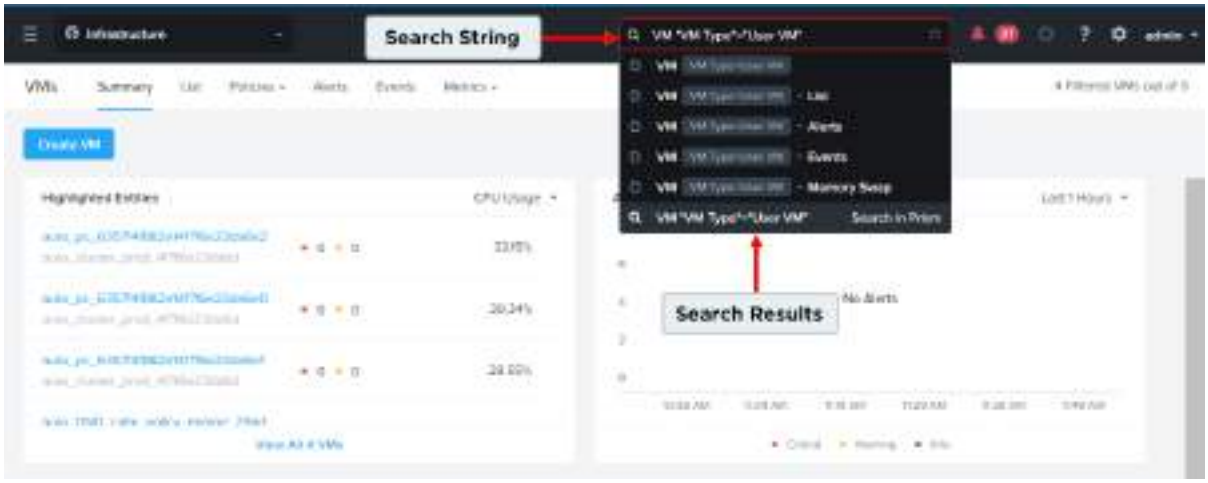


Figure 17: Search Results (for the current location)

Search provides intelligent responses based on whatever you enter in the field. For example, entering *scale out* returns a link to the Manage Prism Central page from which you can scale out Prism Central. If you enter a more generic string such as *version*, the search engine returns results with links to pages across entities with version information.

Figure 18: Search Results (for generic string)

Click the Star icon in the search field to bookmark a filtered page. This adds a bookmark for that page in the **Navigation Bar**. For more information about **Navigation Bar**, see Application-specific Navigation Bar on page 66).

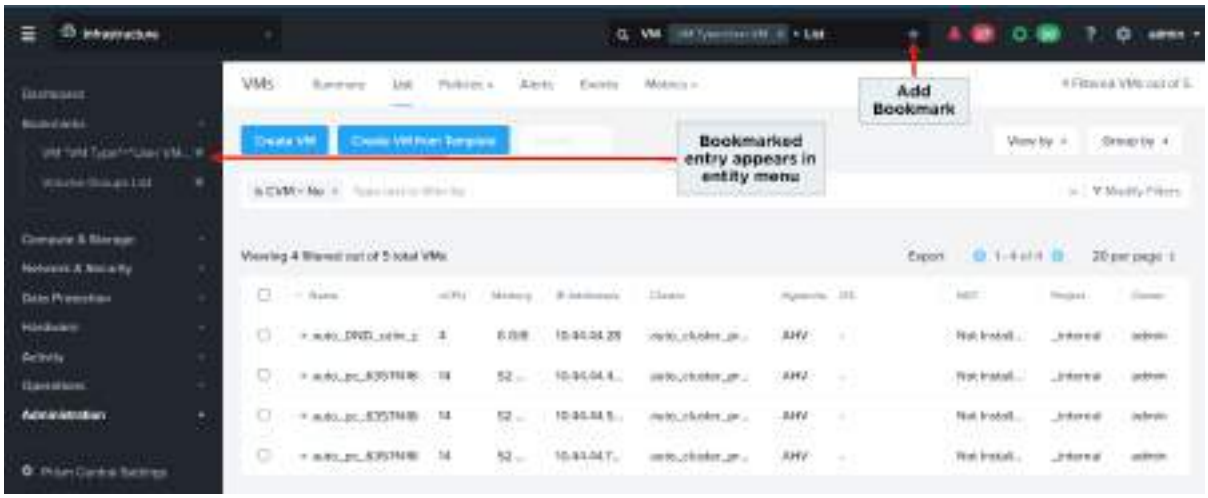


Figure 19: Bookmark Entry

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2544

On some pages, the applied filters are not reflected in the search field. For those pages, a local filters field appears. When you select one or more filters on such a page, the applied filters appear in the local filters field.

You can do the following from this field:

- Remove all filters by clicking **Clear** (on the right).
- Remove a filter by clicking *X* for that filter.
- Bookmark the filter list by clicking the Bookmark icon. You can save a maximum of 20 filter lists per entity type.
- Use a saved filter list by selecting from the dropdown menu.

Figure 20: Local Filters Field

Query Syntax

The search field supports a range of simple and complex query options in the following syntax forms:

- [entity|metric]: Enter an entity or metric type such as `cluster`, `vm`, or `alerts` to return information about the instances of that entity or metric across the registered clusters.
- <entity> <metric>: To refine an entity search, add a metric to the query. For example, `vm iops` returns IOPS information for the VMs.
- <entity> <attribute> <metric>: To further refine the search, add an attribute for the metric. For example, `node failure alerts` returns any failure alerts about the nodes.
- [metric|attribute] operator <value>: Enter an expression for a metric or attribute to return instances that match the expression. For example, `"block model"=1050` returns information about the NX-1050 nodes. See the following "Filter Expressions" section for the supported expression operators.
- <complex expression>: Combine the syntax forms to create complex queries. For example, `clusters hypervisor = AHV "cpu usage" < 30` returns information about clusters running the AHV hypervisor with CPU usage below 30%. Complex expressions have an implied AND so only instances that satisfy all conditions are returned.
- <action expression>: In addition to search queries, you can initiate certain actions from the query bar. For example, `<vm_name> launch console` launches a console window for the specified VM (if you are allowed to do so).

The following table describes the syntax rules for search queries.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2545

Table 12: Syntax Rules

Rule	Example
RULES THAT GO TO WELL DEFINED PAGES	
entity type	vms
entity type + metric perspective (io, cpu, memory)	vms io
entity type + alerts	vm alerts
entity type + alerts + alert filters	vm alerts severity=critical
entity type + events	vm events
entity type + events + event filters	vm events classification=anomaly
entity type + filters (both metric and attribute)	vm “power state”=on
entity type + filters + metric perspective (io, cpu, memory)	vm “power state”=on io
entity type + filters + alerts	vm “power state”=on alerts
entity type + filters + alerts + (alert filters)	vm “power state”=on alerts severity=critical
entity type + filters + events	vm “power state”=on events
entity type + filters + events + event filters	vm “power state”=on events classification=anomaly
entity instance (name, ip address, disk serial, ...)	vm1, 10.1.3.4, BHTXSPWRM
entity instance + metric perspective (io, cpu, memory)	vm1 io
entity instance + alerts	vm1 alerts
entity instance + alerts + alert filters	vm1 alerts severity=critical
entity instance + events	vm1 events
entity instance + events + event filters	vm1 events classification=anomaly
entity instance + pages	vm1 nics, c1 capacity
parent instance + entity type	c1 vms
alert title search	disk bad alerts
page name search	analysis, tasks
RULES THAT ONLY GO TO SEARCH RESULT PAGES (exclusively)	
entity type + metric	vm iops
entity type + attribute	vm power state
entity instance + metric	vm1 iops
entity instance + attribute	vm1 power state
entity type + filters + metric	vm “power state”=on iops
entity type + filters + attribute	vm “power state”=on hypervisor

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2546

Rule	Example
help text search	upgrade cluster

Keywords

The following table lists the keywords or phrases you can use when formulating a query.

- The *Object* column identifies the type of object.
  - *Entities*: Lists the entities you can specify. The list is limited. For example, you cannot search for information about remote sites or network switches.
  - *Fields*: Lists the parameters (fields) you can specify.
  - *Alerts*: Lists the alert conditions you can specify.
  - *Events*: Lists the event conditions you can specify.
  - *Actions*: Lists the actions you can specify.
- The *Entity* column specifies the entities for which you can use that keyword in a query. For example, Alert queries can apply to any entity, but Fields has multiple rows broken down by entity type (such as cluster, VM, and disk) because there are select keywords that apply to each entity type.
- The *Keywords* column is a comma-separated list of the keywords or phrases you can use in a query for the specified object/entity type.

Table 13: Search Keywords

Object	Entity	Keywords
Entities	(n/a)	vm, cluster, node, container, disk
Fields	(not specified)	cpu usage, memory usage, disk usage, free physical storage, storage logical usage, saving ratio, savings, iops, read iops, write iops, io bandwidth, read io bandwidth, write io bandwidth, io latency, read io latency, write io latency, memory capacity, hypervisor
	Cluster	cluster name, ip address, version, number of hosts, cpu count, memory capacity, runway, storage runway, cpu runway, memory runway
	VM	vm name, ip address, host ip, virtual cpus count, power state, reserved memory, os, virtual hardware version
	Disk	serial, tier, mode, iops
	Container	container name, rf, on disk deduplication, perf-tier deduplication, compression, erasure coding
	Node	host name, ip address, service vm, hypervisor name, cpu capacity, cpu model, cpu sockets count, cpu cores count, cpu thread count, serial number, block model

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2547

Object	Entity	Keywords
Alerts	(any)	alert, alert title • Severity levels: critical, warning, info • Categories (impact types): capacity, performance, configuration, availability, system indicator • Dispositions types: resolved, unresolved, acknowledged, unacknowledged
Events	(any)	event type, title
Actions	VM	clone, migrate, delete, power on, power off, suspend, create vm, launch console, create network config, resume, snapshot, update, configure vm host affinity
	Cluster	launch prism element, unregister

Filter Expressions

You can use any of the following operators in an expression.

Table 14: Query Operators

Description	Operator
contains	~
does not contain	!~
starts with (“starts with” x)	=x*
ends with (“ends with” x)	=*x
equal to	=
not equal to	!=
greater than	>
greater than or equal to	>=
less than	<
less than or equal to	<=
a metric range, for example CPU usage between 10 and 30	=[10 to 30]

The following implicit operator rules apply to expressions:

- In most cases, an AND is applied to all filters in an expression. For example, *hypervisor=AHV iops>100* means the hypervisor is AHV and IOPS are over 100.
- If the filters are on the same attribute, an OR is applied. For example, *hypervisor=AHV hypervisor=ESXi* means the hypervisor is either AHV or ESXi.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2548

- If the filters are on the same metric, an AND is applied to create a range. For example, *iops>100 iops<500* means IOPS in the range 100-500.
- If multiple range filters are defined in a single query, an OR is applied across the ranges. For example, *iops>100 iops<500 cpu>20 cpu<40* means IOPS in the 100-500 range or CPU in the 20-40 range.

Search Units

The data for search queries comes from the following parameters.

Table 15: Data Parameters

Data Type	Unit	Parameter
bytes usage related properties	GiBiBytes	memory_capacity_bytes, storage.usage_bytes, storage.free_bytes, storage.logical_usage_bytes, data_reduction.saved_bytes, storage.usage_bytes, storage.user_container_own_usage_bytes, data_reduction.saved_bytes, memory_size_bytes
runway properties	days	capacity.runway, capacity.storage_runway, capacity.cpu_runway, capacity.memory_runway
disk capacity related properties	TebiBytes	storage.capacity_bytes, storage.user_capacity_bytes
CPU/memory usage properties	percent	hypervisor_cpu_usage_ppm, hypervisor_memory_usage

Example Queries

Here are examples of various query types.

- Entity queries:

```
<cluster_name>
<cluster_ip_address>
<disk_serial#>
VMs "Power State"=On List
VMs Hypervisor=AHV List
powered on vms "memory capacity" > 32
```

- Performance queries:

```
clusters running out of cpu
clusters hypervisor = AHV "cpu usage" < 30
vm iops
```

- Alert queries:

```
node failure alerts
<cluster_name> alerts
<cluster_name> critical availability alerts
<alert title>
Alerts "Create Time"="08-Nov-2018 9:46 AM to 08-Nov-2018 10:46 AM" Severity=Critical
```

- Action queries:

```
<vm_name> launch console
<cluster_name> launch prism element
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2549

```
create vm
```

- Exploration queries:

```
clusters hypervisor=AHV
vm os=Linux
<cluster_name> vms
"block model"=1050
"cpu model"=Intel
containers Rf > 2
clusters version=4.6.2
hosts iops < 1000
<cluster_name> powered off vms
disks tier=ssd
vms "cpu usage"
vms “power state”
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2550

MAIN DASHBOARD - INFRASTRUCTURE

The **Main Dashboard** provides a dynamic summary view of all the registered clusters in Prism Central.

To view the **Main Dashboard** at any time, select **Infrastructure** application from the Application Switcher Function on page 45, and click **Dashboard** in the **Navigation Bar** .

> **Important:** Nutanix recommends using Google Chrome web browser to access Prism Central. The display of dashboard and widgets is optimized for Google Chrome browser.

Dashboard Layout

The **Dashboard** provides a collection of widgets that appear as tiles with targeted information about the registered clusters in each tile. The **Dashboard** includes the following options:

- **Main Dashboard** tab: Displays the Infrastructure dashboard. The additional tabs appear if you create any custom dashboards.
- **Manage Dashboard**: Enables you to create a custom dashboard, edit the custom dashboard, or delete a custom dashboard. For more information about how to create a custom dashboard and modify the custom dashboard, see Creating a New (Custom) Dashboard on page 85 and Modifying a Dashboard on page 87.
- **Reset Dashboard**: Enables you to reset the dashboard to the default set of widgets.
- **Generate Report**: Enables you to generate the complete **Main Dashboard** and **Custom Dashboard** widgets as a report of all the registered clusters. For information about how to generate the dashboard report, see Generating a Dashboard Summary Report on page 92.

  > **Note:** Generating a report requires a valid license - Prism Pro, Prism Ultimate, or any edition of NCM. For more information, see License Manager Guide. The **Generate Report** option does not appear if the appropriate license is not available.

- **Add Widget**: Enables you to add a widget to the displayed dashboard. For information about how to add a widget to a dashboard, see Adding Dashboard Widgets on page 98.

  > **Note:** Adding a widget to a dashboard requires a Prism Pro license. The **Add Widgets** does not appear if Prism Pro is disabled.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2551

- **Data Density** - Enables you to select the density of data representation in the widgets. Select one of the following three options:
  - **Light**: The information is lightly packed in the widget with more spacing between the elements.
  - **Default**: The information is moderately packed with sufficient spacing between the elements. This scheme of data density is based on user research by Nutanix.
  - **Dense**: The information is densely packed with minimal spacing between the elements for essential legibility.

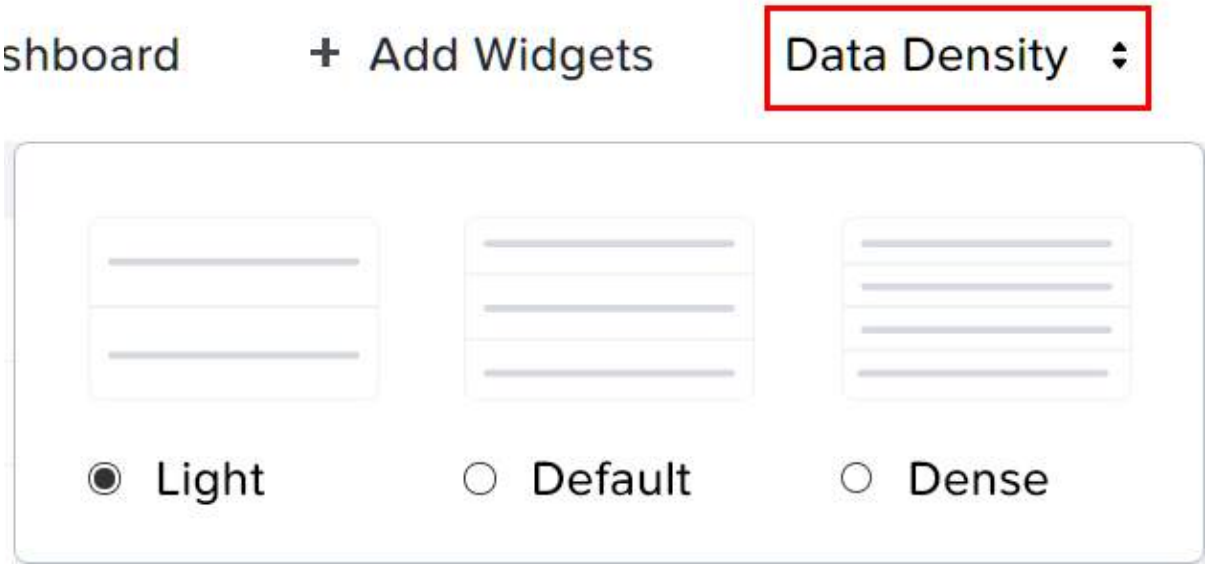


Figure 21: Data Density

Note: The **Manage Dashboards** and **Add Widget** are Prism Pro license features. If Prism Pro is disabled, these options disappear, and you cannot customize or add custom dashboards. Any custom dashboards created before Prism Pro was disabled exists, but clicking the **Reset All** (which replaces the **Reset Dashboard** when custom dashboard exists) deletes all custom dashboards and returns the **Main Dashboard** to the default state.

The following is an example showing the main dashboard:

Figure 22: Main Dashboard

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2552

Dashboard Management

The **Main Dashboard** displays an array of information tiles (widgets) by default. You can customize this view by adding or deleting widgets as desired. For information about how to modify a dashboard, see Modifying a Dashboard on page 87.

The widgets are lined up in rows of four widgets per row. The default widgets are described in this section as they appear from left to right, top to bottom on the **Main Dashboard** page.

The following is an example view of the **Main Dashboard** page with the default widgets:

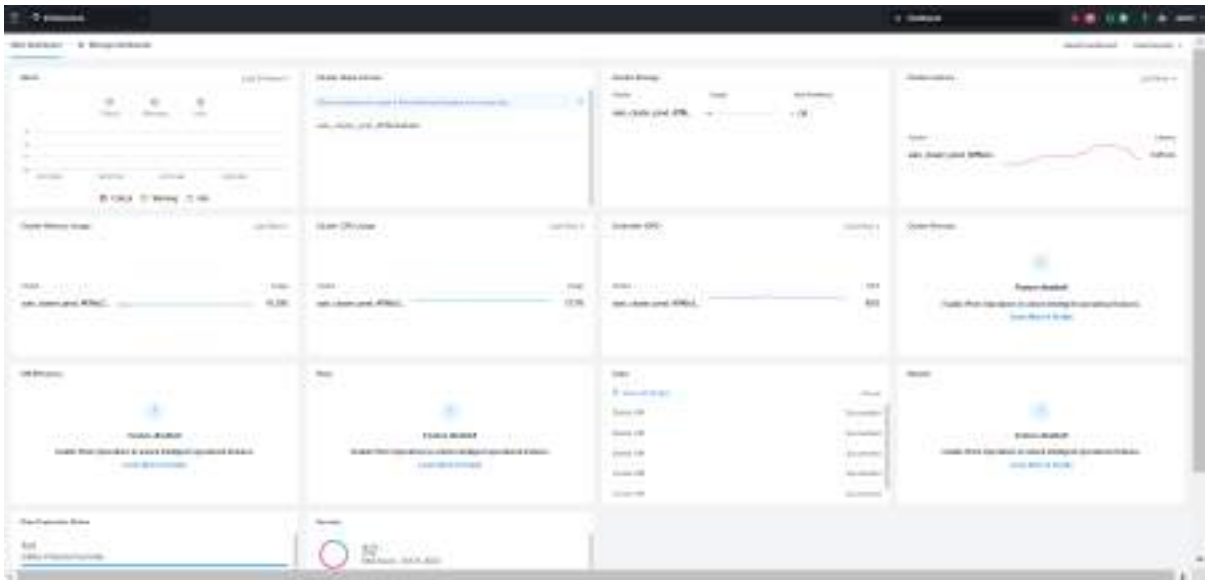


Figure 23: Main Dashboard with Default Widgets

The following is an example displaying a widget with a period (time) selection:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2553

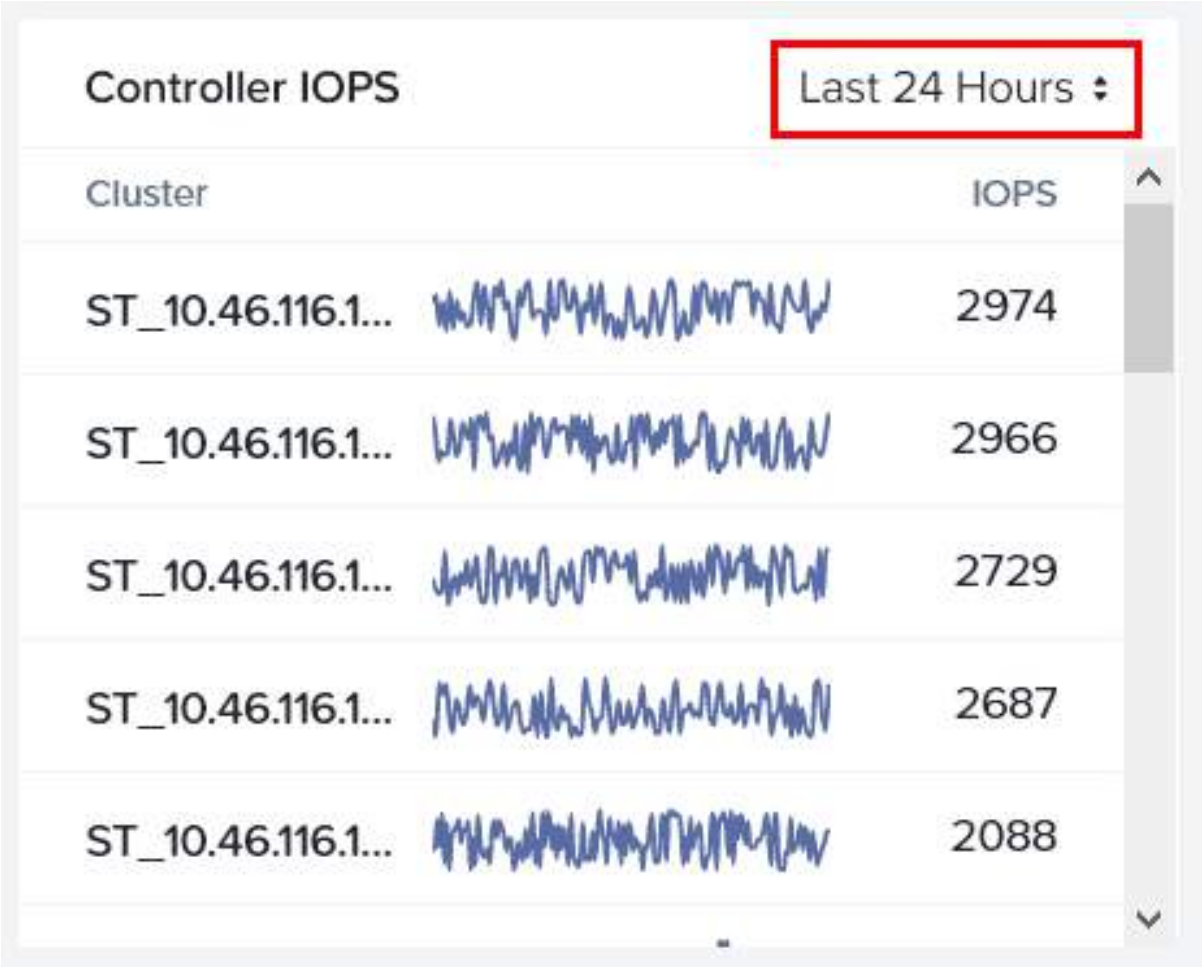


Figure 24: Sample Widget

- **Alerts**: This widget displays colored bar graph representing the alerts raised in the selected period. You can select the period on the drop down list at the top right corner of the widget. Each category of alerts is represented as a colored bar. Click any bar on the graph to see a list of the alerts represented in the bar. Click **View All Alerts** link to see all the alerts on the **Alerts** page.

  The Alerts are categorized as **Critical**, **Warning** and **Info**, and are represented as red, yellow, and blue bars respectively in the graphs.

- **Cluster Quick Access**: This widget displays a list of the clusters managed by the Prism Central. It allows you to open the Prism Element for a registered cluster in a new window when you click the name of the cluster. The cluster **Home** page appears in Prism Element. For more information about the **Home** page of Prism Central, see Prism Central Web Console Guide.

- **Cluster Storage**: This widget displays storage and resiliency information for the highest usage clusters. Each line includes the cluster name, a usage column with a bar that visually indicates how much capacity is used currently, and a data resiliency column that displays the current status (critical, warning, OK, or unknown). The cluster list is ordered by data resiliency status with critical clusters at the top of the list. Click the cluster name to view the **Summary** page for that cluster. Clicking the arrow button displays a dialog box with usage details including data reduction ratio, usage percentage, used space, total space, fault domain (disk, node, or rack), and fault tolerance level (0, 1, or 2). The data reduction ratio indicates the data savings due to data reduction techniques such as de-duplication, compression, and erasure coding. (A 1:1 ratio indicates none of these data reduction techniques are in use currently.)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2554

- **Cluster Latency**: This widget displays the total (read and write) IO latency average for the highest latency clusters. Click <*cluster name*> to display the **Summary** page for that cluster.
- **Cluster Memory Usage**: This widget displays the percentage of total memory in use currently for the highest usage clusters. Click <*cluster name*> to display the **Summary** page for that cluster.
- **Cluster CPU Usage**: This widget displays the percentage of total CPU in use currently for the highest usage clusters (or all clusters if there are fewer than five). Click <*cluster name*> to display the **Summary** page for that cluster.
- **Controller IOPS**: This widget displays the total (read and write) controller IOPS for the highest volume clusters. Click <*cluster name*> to display the **Summary** page for that cluster. The IOPS number comes from the controller when the hypervisor is AHV or Hyper-V and from the hypervisor when the hypervisor is ESXi.
- **Cluster Runway**: This widget alerts you to potential storage, CPU, or memory resource constraints across the clusters and provides an estimated *runway* (time remaining) before the resources are maxed out based on current usage. Click <*cluster name*> to display the **Capacity** page for that cluster.
- **VM Efficiency**: This widget displays the number of VMs that are considered inefficient and are broken down by category: over-provisioned, inactive, constrained, and bully. It provides a link to the VMs dashboard. For information about these VMs, see VMs Summary View on page 104.

  For more information, see Behavioral Learning Tools information in *Intelligent Operations Guide*.
- **Plays**: This widget displays a list of plays running on the cluster. The list is categorised into completed, failed, and paused plays. The completed plays are displayed in the center widget. The number for each category is linked to the **Plays** page.
- **Tasks**: This widget displays a list of recent tasks with the current status of each task. Click the **View All Tasks(s)** link to view the **Tasks** page. For more information, see Tasks View on page 452.
- **Reports**: This widget displays a table that lists the number of total and scheduled reports with a link to the **Reports** page. For more information, see Reports Management in *Intelligent Operation Guide*.
- **Data Protection Status**: This widget displays the protection summary and recovery plans if created. If no recovery plan is created, it displays a **How to setup?** link to create a create recovery plan.
- **Security**: This widget displays the summary of **Security Dashboard**. Click the **View All Issues** link to view the **Security Dashboard** page. For more information, see Security Dashboard on page 394.

Resetting Dashboard

This section describes how to reset an existing dashboard in Prism Central.

About this task

Perform the following steps to reset a dashboard:

Procedure

1. Log in to Prism Central, and select the **Infrastructure** application from the Application Switcher Function on page 45.
   The infrastructure dashboard is displayed.
2. Click **Reset Dashboard** to reset the main dashboard to the default set of widgets.
   The system prompts you to confirm the reset dashboard action.
3. Click **OK** to confirm.
   The main dashboard is reset to default.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2555

Setting Data Density

This section describes how to set up the data density in Prism Central.

About this task

Perform the following steps to set up the data density:

Procedure

1. Log in to Prism Central, and select the **Infrastructure** application from the Application Switcher Function on page 45.
   The infrastructure dashboard is displayed.
2. Click **Data Density** option to select the density of data representation in the widgets.
   The system prompts you to select the data density option.

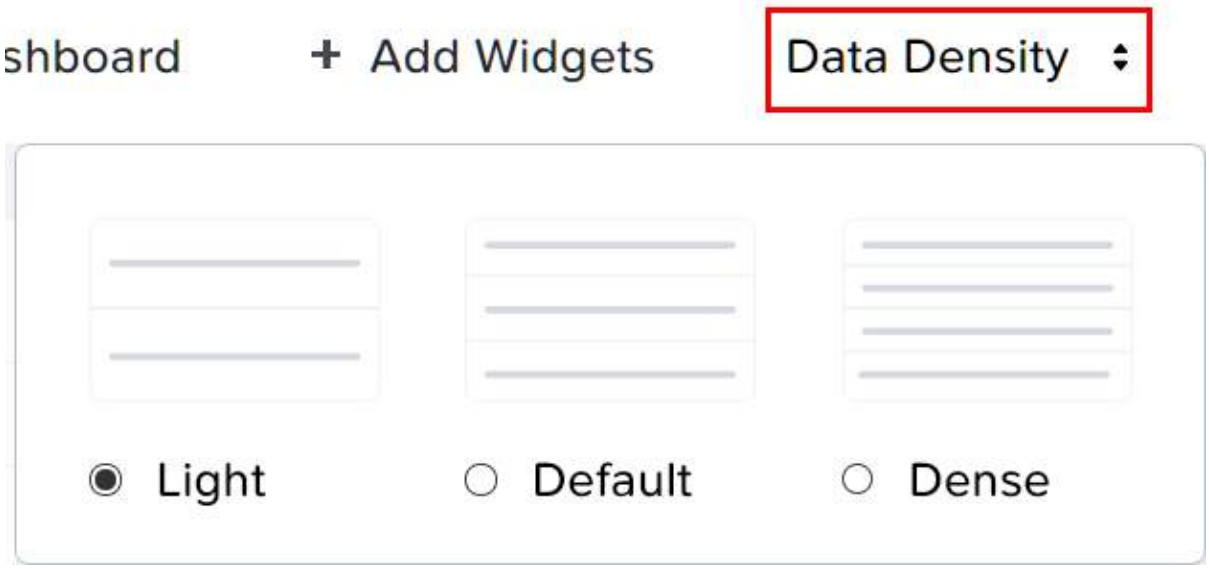


Figure 25: Data Density Options

Select one of the following three options:

Light: The information is lightly packed in the widget with more spacing between the elements.

Default: The information is moderately packed with sufficient spacing between the elements. This scheme of data density is based on user research by Nutanix.

Dense: The information is densely packed with minimal spacing between the elements for essential clarity.

Creating a New (Custom) Dashboard

About this task

The **Main Dashboard** provides a default view into the clusters, but you can add custom views by creating custom dashboards. To create a custom dashboard, do the following:

> **Note:** Creating a dashboard requires a valid NCM license. For more information, see License Manager Guide.
> The **Manage Dashboards** does not appear if the appropriate license is not available.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2556

Procedure

1. Log in to Prism Central, and select the **Infrastructure** application from the Application Switcher Function on page 45.
   The infrastructure dashboard is displayed.
2. Click **Manage Dashboards**, and perform the following steps:
   a. Click **New Dashboard**.
   b. Enter a name for the dashboard in the displayed field.
   c. Click **Save**.

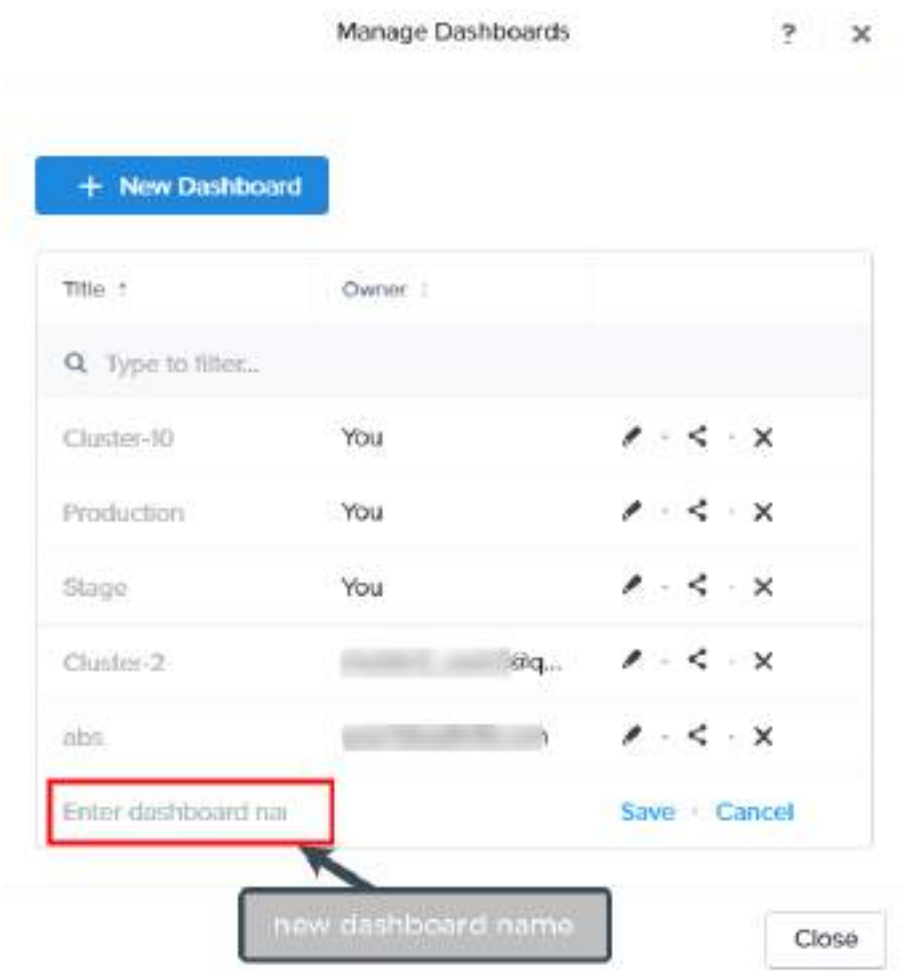


Figure 26: Manage Dashboards Windows (new dashboard)

3. Click **Close** to close the **Manage Dashboards** window.
   A new dashboard tab appears next to the **Main Dashboard** (or other custom dashboard) tab.

   Note: The new dashboard is empty (no widgets) initially.

4. Click the new dashboard tab, and then click the **Add Widgets**.
   The system displays the **Add Widgets** window.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2557

5. In the **Add Widgets** window, select a widget and add it to the dashboard. For more information on how to add a widget, see Adding Dashboard Widgets on page 98.

   Repeat this step for all the desired widgets to be added to the new dashboard.

Modifying a Dashboard

About this task

The **Main Dashboard** provides a default view into the registered clusters, but you can customize that view at any time. To modify the Main dashboard or any other dashboard you create, do the following:

> **Note:** Customizing a dashboard requires a Prism Pro license. The **Add Widgets** and **Manage Dashboards** do not appear if Prism Pro is disabled.

Procedure

1. Log in to Prism Central, and select the **Infrastructure** application from the Application Switcher Function on page 45.
   The infrastructure dashboard is displayed.
2. Click **Main Dashboard** tab or previously added custom dashboard tab.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2558

3. Perform either of the following operations:

   - To add a widget to the displayed **Main Dashboard** or custom dashboard, click **Add Widgets**, select a widget from the **Add Widgets** window, and add it to the **Main dashboard** or custom dashboard.

     For information about how to add a widget, see Adding Dashboard Widgets on page 98.

   - To delete a widget, click *X* in the upper right of the displayed tile. The system prompts you to confirm the delete action.

     Click **OK**. The widget disappears from the dashboard.

   - To reset the **Main Dashboard** to the default set of widgets (after you have previously added or deleted widgets), click **Reset Dashboard**. The system prompts you to confirm the reset action.

     Click **OK**. The **Main Dashboard** returns to its default view.

   - To rename a custom dashboard, perform the following steps:

     1. Click **Manage Dashboards**.
     2. Click the Edit icon for that dashboard.
     3. Enter a new name in the displayed field.
     4. Click **Save**.

   - To delete a custom dashboard, click **Manage Dashboards** and then click *X* for that dashboard. The system prompts you to confirm the delete action.

     Click **OK**. The tab for that custom dashboard disappears from the **Dashboard** page.

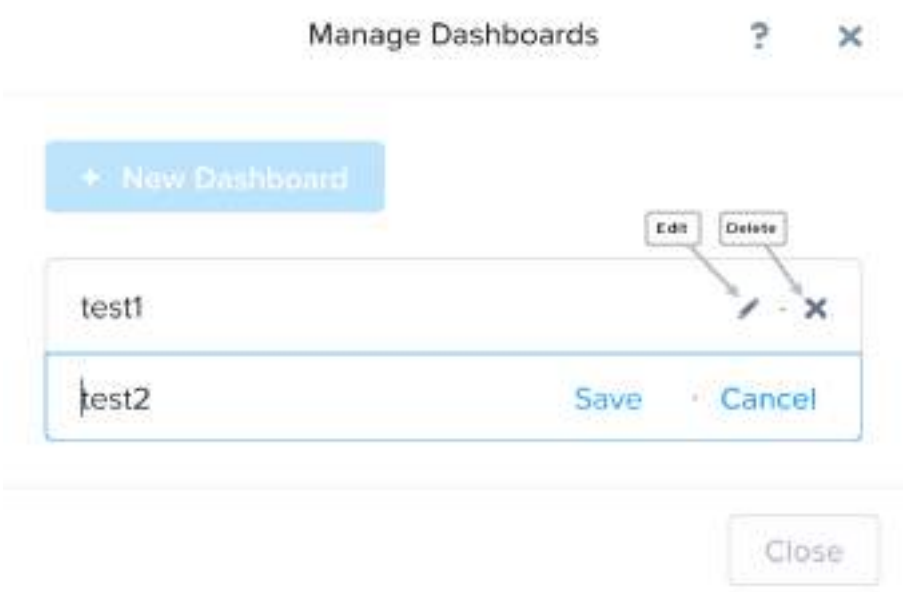


Figure 27: Manage Dashboards Window

Sharing a Dashboard

About this task

Any user with edit permission can share a custom dashboard with other users and provide view or edit access to them.

Note: Enable CMSP to use this feature.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2559

Procedure

1. Log in to Prism Central, and select the **Infrastructure** application from the Application Switcher Function on page 45.
   The infrastructure dashboard is displayed.
2. Click **Manage Dashboard**.
   The systems displays the **Manage Dashboard** window. This window lists all the existing custom dashboards.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2560

3. Select the custom dashboard you want to share, and click the Share icon.

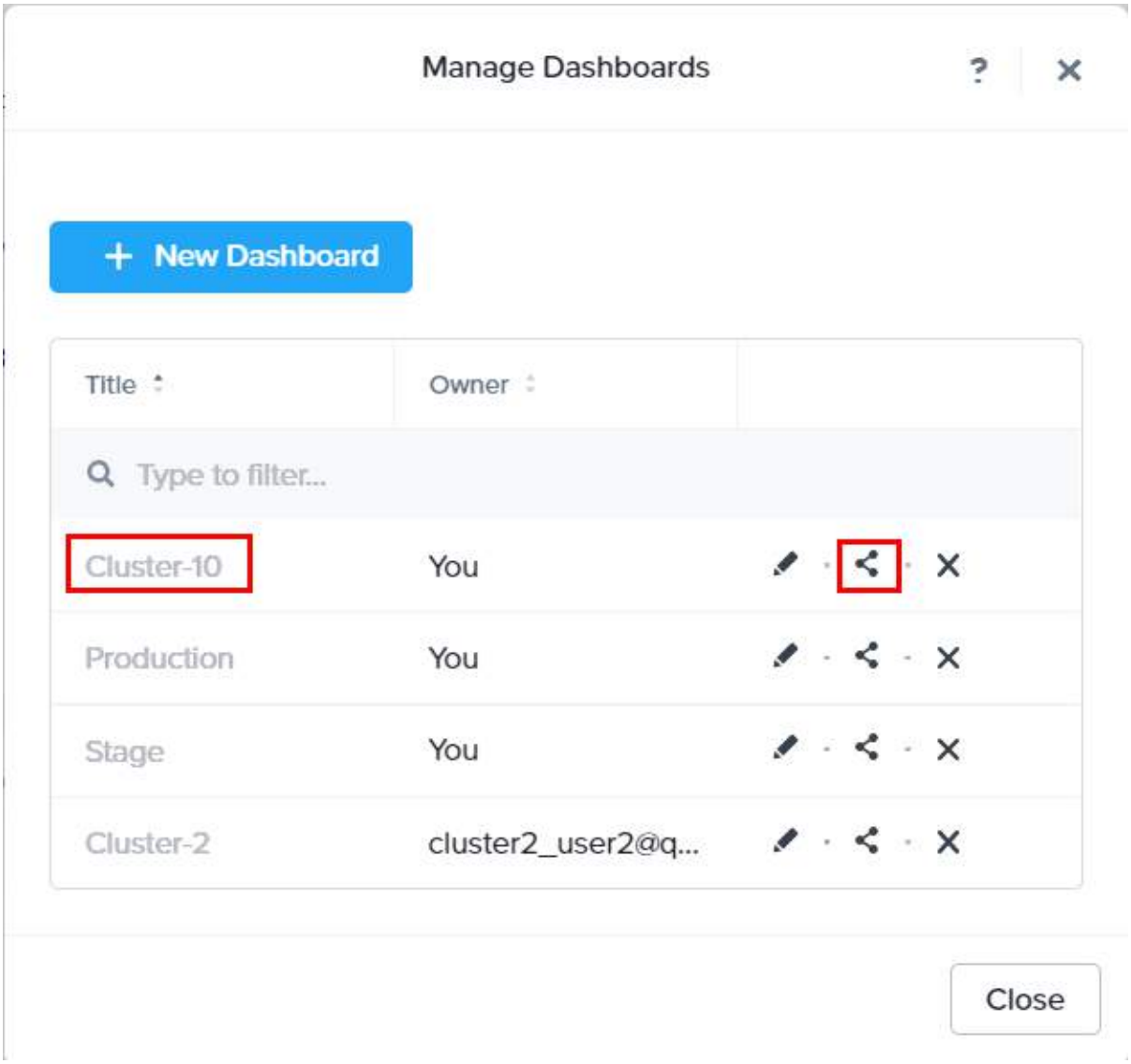


Figure 28: Manage Dashboards

The **Sharing Dashboard** window appears.

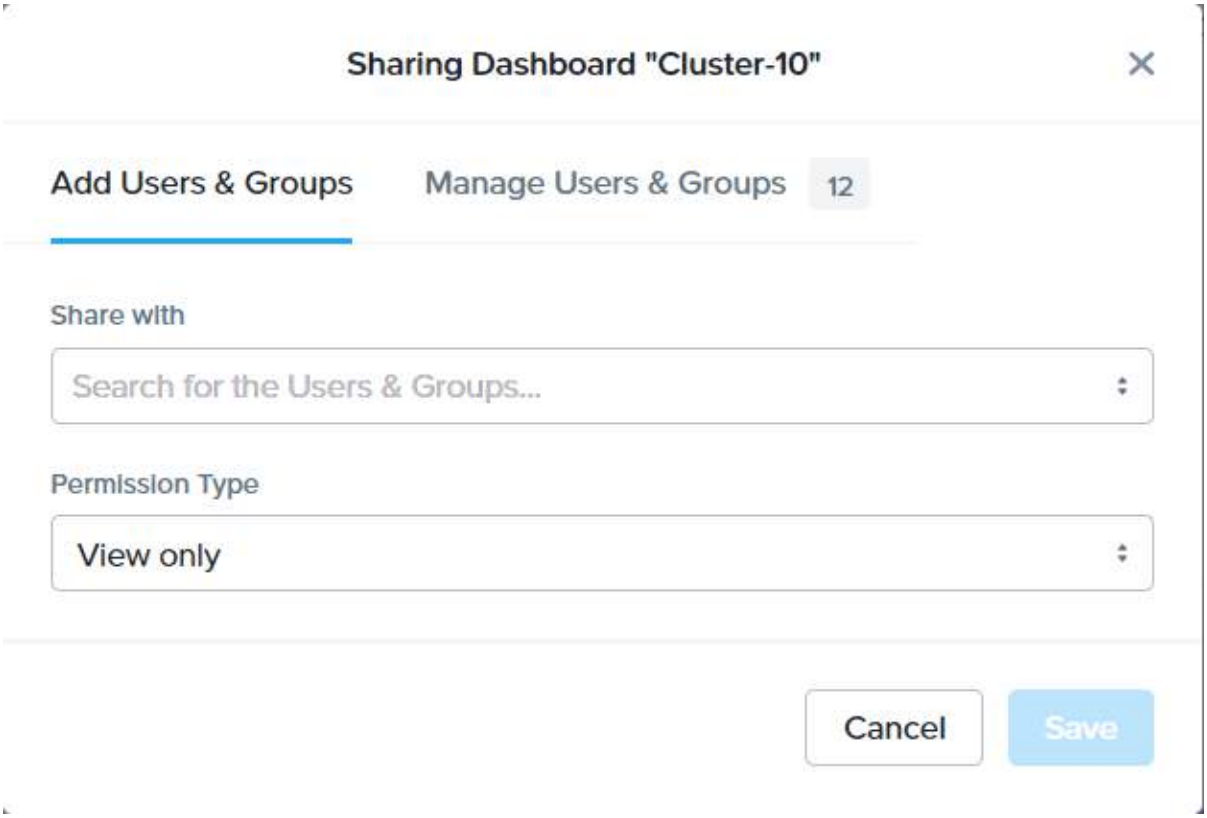


Figure 29: Sharing Dashboard

4. In the **Add Users & Groups** tab, perform the following steps:

   a. In **Share with** field, add the users or groups to share the custom dashboard. You can type a first few characters of a user or group, and as you type, a dropdown menu appears based on the typed keywords. Select the user or group to be added from the displayed list.

   > **Note:** The system also allows you to add more than one user or group.

   b. In the **Permission Type** dropdown menu, select the permission as **View only** or **Edit**.

   The system assigns the selected permission to the user or group entered in the **Share with** field.

   > **Note:**
   >
   > - Only the user with **Edit** permission can view, edit and share the custom dashboard. The user with **View only** permission can only view the custom dashboard.
   > - The **Manage Users & Groups** tab allows you to change the permission type for users or groups with whom you have shared the dashboard earlier. You can also remove the users or groups as per the requirement.

5. Click **Save**.
   A message appears that indicates the dashboard is shared successfully.

   After you share the dashboard, wait for few minutes for changes to take effect.

   > **Note:** You cannot view any information about entities in the dashboard chart without entity permissions.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2562

Generating a Dashboard Summary Report

In Prism Central, you can monitor infrastructure widgets by visualizing the data on the dashboards. However, the data is available only in the Prism Central interface. Generating a Report feature allows you to export the infrastructure data as a report for further analysis, archival, compliance, and other purposes.

> **Note:** Generating a report requires a valid license - Prism Pro, Prism Ultimate, or any edition of NCM. For more information, see License Manager Guide. The **Generate Report** option does not appear if the appropriate license is not available.

You can generate a report in the following ways:

- Download the dashboard data as a report in PDF format or CSV format.
- Email the dashboard data as a report to the recipients in PDF format or CSV format, or both, as an attachment.
- Save the dashboard data as a report configuration to schedule, share, and export reports.

The following is an example showing the dropdown menu of the **Generate Report** option from the Main Dashboard:

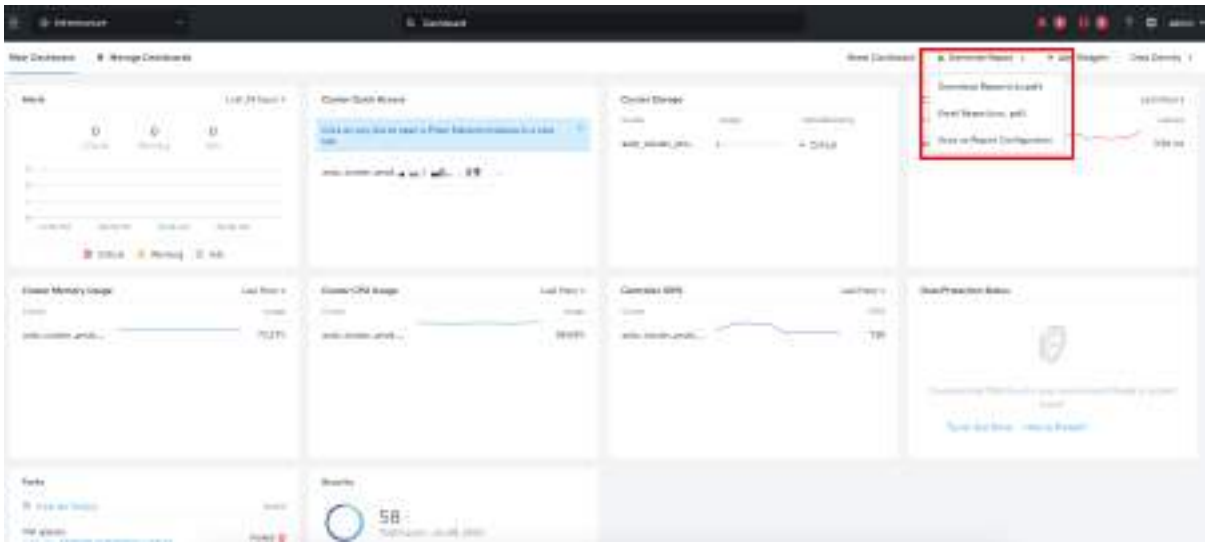


Figure 30: Main Dashboard - Generate Report Dropdown Menu

The following table describes the dropdown menu list of the **Generate Report** option:

Table 16: Generate Report Dropdown List

Options	Description
Download Report (csv, pdf)	Click this action to download the report. For more information, see Downloading a Report on page 93.
Email Report (csv, pdf)	Click this action to email the report. For more information, see Emailing a Report on page 93.
Save as Report Configuration	Click this action to save the report as a configuration. For more information, see Saving as a Report Configuration on page 94.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2563

Downloading a Report

This task describes how to download the main and custom dashboard widgets data as a report, either in PDF format or CSV format.

About this task

Downloading a report has the following workflow:

- The report instance is generated in your preferred format and notified on the main and custom dashboards.
- The generated report instance is available for you to download under **Generated Reports** tab of the Reports page.

> **Important:**
>
> - You can also resend the generated report instance as an email from the **Generated Reports** tab of the Reports page. For more information, see Resending a Report Instance.
> - You must download or resend the report within 24 hours from the time you generated the report instance. After 24 hours, Prism Central removes the report instance from the **Generated Reports** tab.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from **Application Switcher** function.
   The infrastructure dashboard is displayed.
3. Click **Main Dashboard** tab or previously added custom dashboard tab.
4. Click **Generate Report**.
5. Select **Download Report (csv, pdf)** and enter the following information:
   a. **Report Name**: Enter the report name.
   b. **Report Format**: Select PDF format or CSV format.
6. Click **Download**.
   Prism Central displays a confirmation message on the dashboard screen that the report was generated.

What to do next

Select the **Intelligent Operations** application from **Application Switcher** function, and navigate to **Reports** from the **Navigation Bar**. Select **Generated Reports** tab to view and download the generated report instance. For more information, see Downloading a Report Instance.

Emailing a Report

This task describes how to email the main and custom dashboard widgets as a report.

About this task

You can email the main and custom dashboard reports as an attachment in PDF format, CSV format, or both. After you email the report, it is also available as a report instance under **Generated Reports** tab of the Reports page to resend or download the report.

> **Important:** Ensure to resend or download the report within 24 hours from the time you generated the report instance. After 24 hours, Prism Central removes the report instance from the **Generated Reports** tab.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2564

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from **Application Switcher** function.
   The infrastructure dashboard is displayed.
3. Click **Main Dashboard** tab or previously added custom dashboard tab.
4. Click **Generate Report**.
5. Select **Email Report (csv, pdf)** and enter the following information:
   a. **Recipients**: Enter the recipients (comma-separated) email address of the report.
   b. **Subject**: Enter the subject of the email.
   c. **Body**: Enter the desired text.
   d. **Report Format**: Select the **PDF** checkbox or **CSV** checkbox or both to set a report format.
6. Click **Send**.

What to do next

Select the **Intelligent Operations** application from **Application Switcher** function, and navigate to **Reports** from the **Navigation Bar**. Select **Generated Reports** tab to view and manage the generated report instance. For more information, see Managing a Report Instance from Generated Reports Tab.

Saving as a Report Configuration

This task describes how to save the main and custom dashboards data as a report configuration.

About this task

You can save the main and custom dashboards data as a report configuration. The configuration of the report that you save is available under **Configurations** tab of the Reports page to perform report management actions.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from **Application Switcher** function.
   The infrastructure dashboard is displayed.
3. Click **Main Dashboard** tab or previously added custom dashboard tab.
4. Click **Generate Report**.
5. Select **Save as Report Configuration** and enter the following information:
   - **Report Configuration Name**: Enter the report configuration name.
6. Click **Send**.

What to do next

Select the **Intelligent Operations** application from **Application Switcher** function, and navigate to **Reports** from the **Navigation Bar**. Select **Configurations** tab to view and manage the saved report configuration. For more information, see Managing a Custom Report Configuration.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2565

Widgets Management

Widgets provides a quick access to the fault, security, and performance-related data for a cluster such as Alerts, memory usage, CPU usage, CVM IOPS, VM efficiency, Reports, Plays, canceled and succeeded Tasks, Data Protection status, and Security dashboard. Each widget provides unique information, and can be added to the dashboard based on the observation requirements.

Resize the Widgets

You can click and drag down the resize handle at the bottom of the widget to vertically resize a widget.

> **Note:** You cannot resize a widget horizontally.

The following is an example of the resize handle:

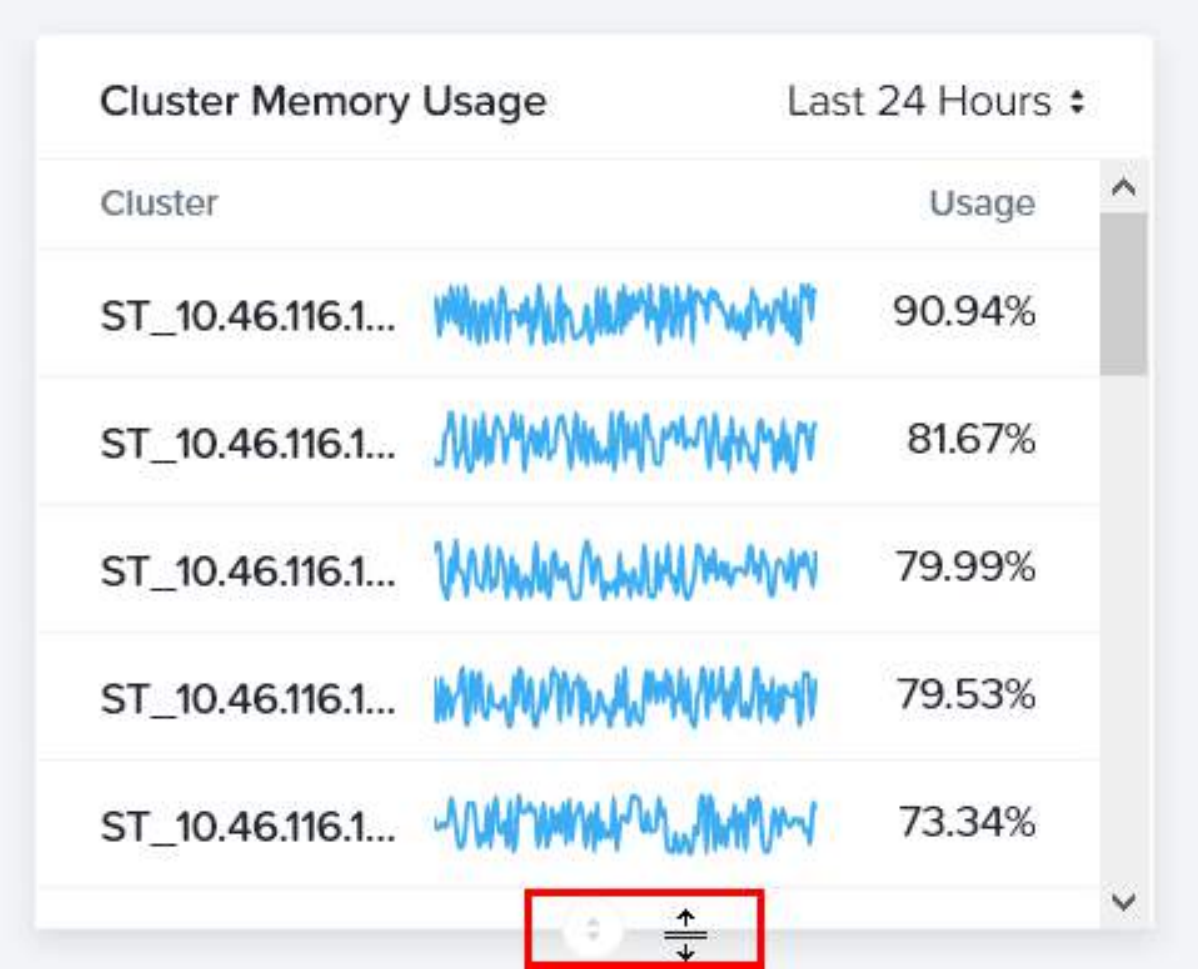


Figure 31: Vertically Resizing the Widget

When you click and drag up or down the resize handle to resize a widget, the widget placed below the resized widget shifts upward or downward.

You can resize (increase or decrease) a widget length in multiples of half of the default length of the widget, such as half, one-and-half, twice, and two-and-half times the default length. Even if you attempt to resize it in any other variation of the default length, the widget auto-sizes itself to the nearest half length.

The following is an example of widget resizing:

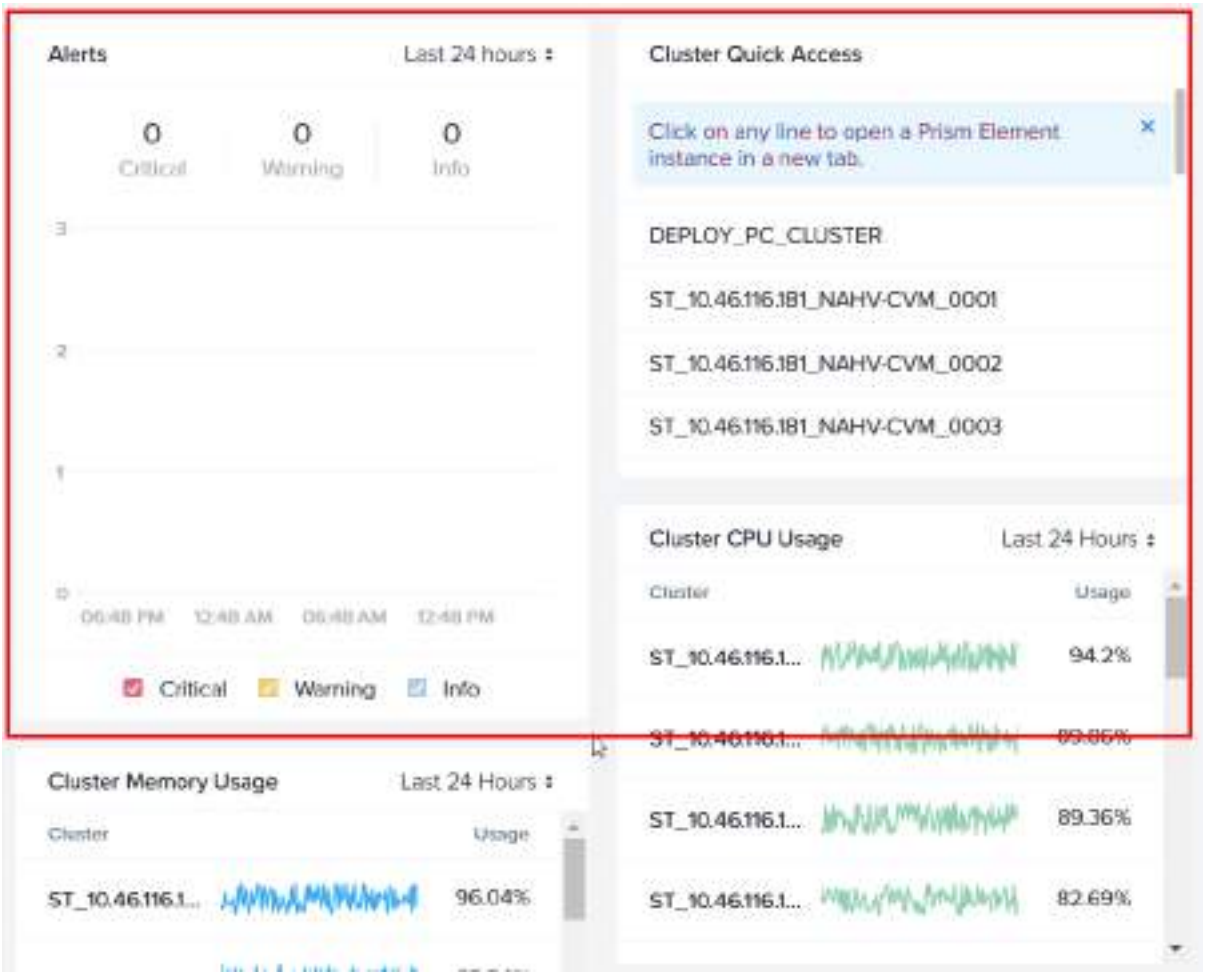


Figure 32: Widget Resize to One-and-half Times the Default Length

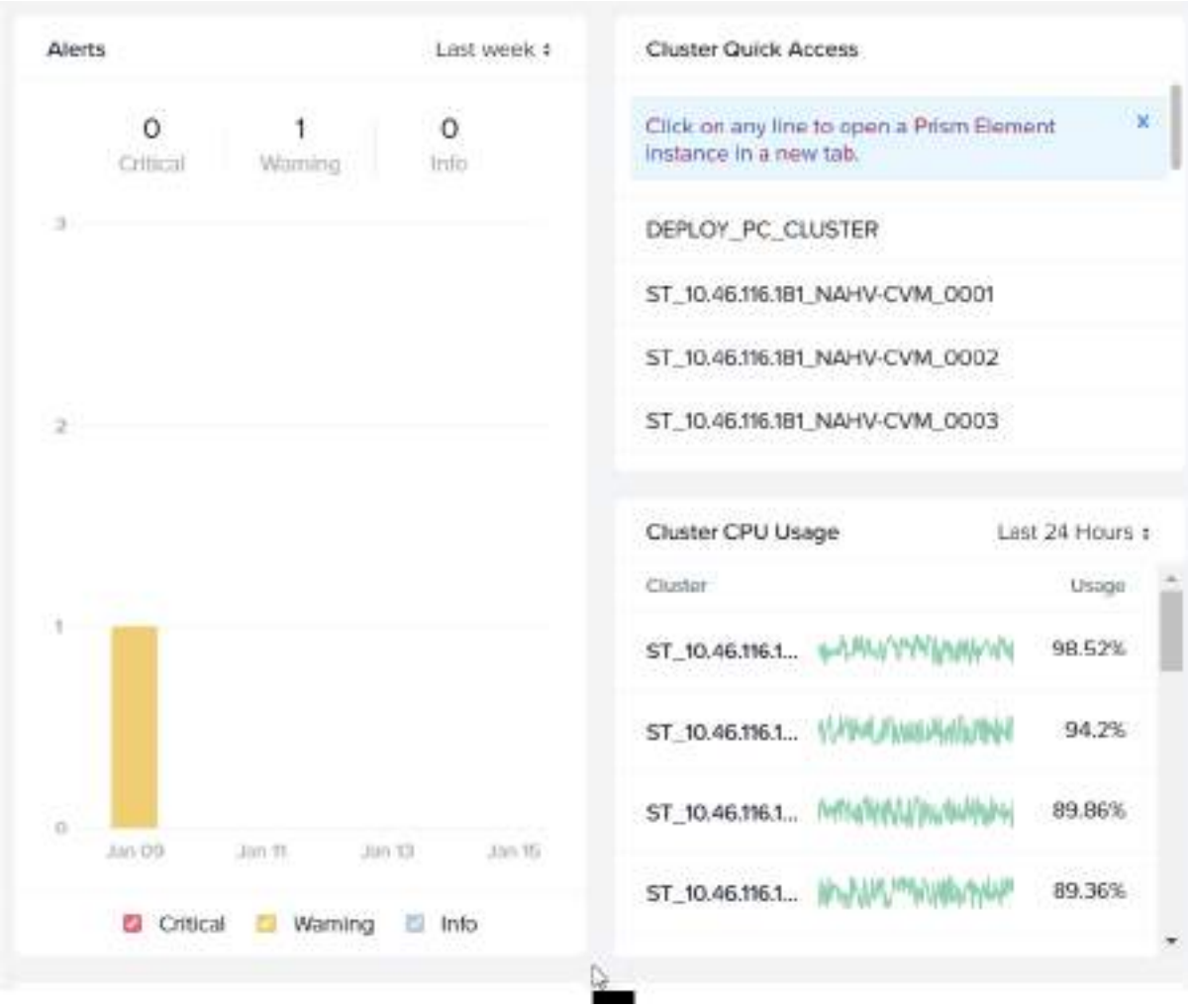


Figure 33: Widget Resize to Twice the Default Length

Drill-down or Expanding Data Elements in a Widget

You can click the data element of a widget to expand or drill-down the information presented in the widget.

Note:

- Expanding a data element in a widget is not possible in all widgets.
- In widgets that provide a list, if you select the list item or row, the system opens an entity page in Prism Central or another application such as Prism Element web console in a new browser tab. For example:
  - In the **Cluster Quick Access** widget, if you click *<cluster name>*, the system opens the Prism Element Web Console for that cluster in a new browser tab.
  - In the **Cluster Storage** widget, if you click *<cluster name>*, the system displays the cluster details view for that cluster.
- In widgets that provide numbers, if you click a number, the system opens the respective entity page in Prism Central. For example:

  In the **Reports** widget, if you click **Total Reports** or the **Scheduled Reports** number, the system displays the **Reports** page.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2568

- In widgets that display charts, if you click the chart, the system displays an expanded or drill-down view of the chart.

  Note: If you click the entity name (such as <*cluster name*>), instead of displaying the drill-down view of the chart, the system displays the entity details page.

- The following is an example of expanding a chart in a widget.

Figure 34: Widget Data Drill-down

At the bottom of the drill-down view, you can select **Full View** to open the details page of the selected entity (cluster or VM). Click **Add To Analysis** to add the chart to the **Analysis** dashboard. For more information, see Analysis Dashboard in *Intelligent Operation Guide*.

Hover Details in Drill-down Views

After you select a chart in a widget, the drill-down view of the chart is displayed. You can hover on any point on the time chart to display the parameters at that point.

In the same example as presented in the Drill-down or Expanding Data Elements in a Widget on page 97, if you hover over the chart, the sample details are displayed.

Adding Dashboard Widgets

Prism Central provides a selection of widgets that can be added to the **Main Dashboard** or a custom dashboard. Each widget provides information about a specific resource or usage topic that is displayed in a tile on the dashboard.

To add a widget to a dashboard, perform the following steps:

Note: Adding a widget to a dashboard requires a Prism Pro license. The **Add Widgets** does not appear if Prism Pro is disabled.

1. Log in to Prism Central, and select **Infrastructure** application from Application Switcher Function on page 45. The infrastructure dashboard is displayed.
2. In the **Main Dashboard** or custom dashboard, click **Add Widgets**.
3. In the **Add Widgets** window, select the desired widget from the left column.

   Note: To find a widget, enter the name in the search field. The system displays a preview of the selected widget.

4. Enter values for the configurable parameters in the right column.

   Note: The parameters vary by widget; some widgets do not have any configurable parameters.

5. Click **Add to Dashboard** (or **Add & Return to Dashboard**) to add the widget to the dashboard.

The following table describes the widgets that you can add to the **Main dashboard**:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2569

Table 17: Widget Parameters

Widget	Description	Parameter	Values
Custom Widgets			
Custom Alerts Widget	Displays a custom list of alerts.	**Widget Name**: Enter a name for the widget. A name (which you can keep or overwrite) is provided after selecting the other options.	(user entered name or settings-based name)
		Select a Cluster: Select the cluster(s) to monitor from the dropdown menu. The default is all clusters.	All Clusters, <cluster name>
		Choose Size: Select the size (width/height dimensions) of the widget. The default is 1 x 1.	1 x 1, 2 x 1, 2 x 2, 2 x 3, 2 x 4, 4 x 4
		Severity. The default is critical.	Critical, Warning, Info
		Entity: Select the entity of interest. The default is cluster.	Cluster, Storage, VM, Hardware, DR
Top Lists Widget	Displays a list of the top performers for a selected metric.	**Widget Name**: Enter a name for the widget that you can keep or overwrite.	(user entered name or settings-based name)
		Select a Cluster: Select the cluster(s) to monitor from the dropdown menu. The default is all clusters.	All Clusters, <cluster name>
		Choose Size: Select the size (width/height dimensions) of the widget. The default is 2 x 1.	2 x 1, 2 x 2, 2 x 3
		Entity: Select the entity of interest. The default is host.	host, VM
		Metric: Select the metric of interest. The default is IOPS.	IOPS, Memory Usage, CPU Usage, Bandwidth, Latency
Custom Chart Widget	Displays a performance graph for a selected entity and metric pair.	**Widget Name**: Enter a name for the widget. The default is *New Chart Widget*.	(name)
		Entity Type: The default is host.	Host, Disk, Storage Pool, Storage Container, Virtual Machine, Virtual Disk

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2570

Widget	Description	Parameter	Values
		Entity: There is no default value. The system displays the list of entity items based on the **Entity Type** field.	(entity name)
		Metric: There is no default value. For information about metrics available for the selected entity item, see the information available in **Metrics Tab** section of that individual entity . For example, for VM-related metrics information, see **Metrics Tab**section in VMs Summary View on page 104 and VM Details View on page 117.	(metric name)
Cluster Info Widget	Displays cluster summary information about alerts, anomalies, runway, and inefficient VMs.	**Widget Name**: Enter a name for the widget. The default is *New Widget*.	(n/a)
		Select a Cluster: Select the target cluster from the dropdown menu.	(registered cluster names)
Virtual Infrastructure Widgets: These widget appears on the **Main dashboard** by default. For details, see Main Dashboard - Infrastructure on page 80.			
VM Efficiency	Displays the number of overprovisioned, inactive, constrained, and bully VMs in the cluster with links to the details.	(no customizable parameters)	(n/a)
Storage Over-provisioning	Displays the configured threshold for storage over-provisioning	Storage Over-provisioning Ratio	
Hardware Widgets: All these widgets (except **Impacted Cluster** and **Performance**) appear on the Main dashboard by default. For details, see Main Dashboard - Infrastructure on page 80.			
Cluster CPU Usage	Displays the percentage of total CPU in use currently for the highest usage clusters.	(no customizable parameters)	(n/a)
Cluster Latency	Displays the total (read and write) IO latency average for the highest latency clusters.	(no customizable parameters)	(n/a)
Cluster Memory Usage	Displays the percentage of total memory in use currently for the highest usage clusters.	(no customizable parameters)	(n/a)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2571

Widget	Description	Parameter	Values
Cluster Quick Access	Displays a list of registered clusters. Health and alert icons appear for each cluster. Clicking the cluster line opens Prism (element) for that cluster in a separate tab or window.	(no customizable parameters)	(n/a)
Cluster Runway	Displays storage, CPU, and memory runway estimates (time remaining before the resource reaches capacity). For more information, see Capacity Runway Summary View in *Intelligent Operation Guide*.	(no customizable parameters)	(n/a)
Cluster Storage	Displays storage statistics for the highest usage clusters.	(no customizable parameters)	(n/a)
Controller IOPS	Displays the total (read and write) controller IOPS for the highest volume clusters.	(no customizable parameters)	(n/a)
Impacted Cluster	Displays information about any clusters that are impacted (performance, capacity, or other potential issues) and may need attention.	(no customizable parameters)	(n/a)
Performance	Displays latency, bandwidth, and IOPS statistics for the highest usage clusters.	(no customizable parameters)	(n/a)
Alerts	Displays colored bar graph that represents the alerts raised in the period selected. Click **View All Alerts** link to see all the alerts on the **Alerts** page. For more information about the alerts generated in Prism Central, see Prism Central Alerts and Events Reference Guide.	(no customizable parameters)	(n/a)
Activity Widgets: The **Tasks** widget appears on the **Main Dashboard** by default. For more information, see Main Dashboard - Infrastructure on page 80.			
Tasks	Displays a list of recent tasks with the current status of each task and a link to the **Tasks** page.	(no customizable parameters)	(n/a)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2572

Widget	Description	Parameter	Values
Discovered Apps	Displays the number of applications discovered in a specified set of monitored clusters. Click the **App instances** number to display the application discovery page. Click the **Identified** or **Unidentified** number to display the application discovery page filtered for that condition. This widget displays the discovered apps information only if you enable App Discovery.	(no customizable parameters)	(n/a)
Operations Widgets: These widgets appear on the **Main Dashboard** by default. For more information, see Main Dashboard - Infrastructure on page 80.			
Plays	Displays a list of the Plays running on the cluster. The list is categorised into completed, failed and paused plays. The completed plays are displayed in the center widget. The number for each category is linked to the **Plays** page.	(no customizable parameters)	(n/a)
Reports	Displays a table that lists the number of total and scheduled reports with a link to the **Reports** page.	(no customizable parameters)	(n/a)
Nutanix Disaster Recovery Widgets: These widgets appear on the **Main Dashboard** by default. For more information, see Main Dashboard - Infrastructure on page 80.			
Data Discovery Status	Displays the Protection summary and recovery plans if created. If no recovery plan is created, it displays a **How to setup?** link to create a create recovery plan.	(no customizable parameters)	(n/a)
Security Widgets: These widgets appear on the **Main Dashboard** by default. For more information, see Main Dashboard - Infrastructure on page 80.			
Security	Displays the summary of **Security Dashboard**. Select the **View All Issues** link to view the **Security Dashboard** page. For more information, see Security Dashboard on page 394.	(no customizable parameters)	(n/a)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2573

COMPUTE ENTITIES

You can access the following entity items from the **Compute** entity of the **Infrastructure** application:

- VMs (see VM Management on page 103)
- Templates (see VM Template Management on page 196)
- Kubernetes Clusters (see Kubernetes Clusters Management on page 210)
- OVAs (see OVA Management on page 219)
- Images (see Image Management on page 242)
- Catalog Items (see Catalog Management on page 266)
- vCenter Datastores (see External vCenter Server Integration on page 326)

For information about how to access the entities items available in **Compute** entities, see Application-specific Navigation Bar on page 66.

VM Management

You can perform the following actions to manage a VM from Prism Central:

- Create and manage VMs directly from Prism Central when the hypervisor is either ESXi or AHV. For more information, see the following sections:
  - Creating a VM through Prism Central (ESXi) on page 170.
  - Managing a VM through Prism Central (ESXi) on page 172.
  - Creating a VM through Prism Central (AHV) on page 130.
  - Managing a VM through Prism Central (AHV) on page 143.
- Create and manage a VM from Prism Central using Prism Self Service. For more information, see the following sections:
  - Creating a VM (Self Service) on page 532.
  - Managing a VM (Self Service) on page 539.
  - Creating a VM from Catalog Items (Self Service) on page 532

  For more information about Prism Self service setup, see Prism Self Service Setup on page 530.
- Add multiple vGPUs to the same VM, and perform a live migration of vGPU-enabled VMs within or outside the cluster. For more information, see the following sections:
  - Adding Multiple vGPUs to the Same VM on page 156
  - Live Migration of vGPU-enabled VMs on page 163
- Export VM as an OVA. For more information, see Exporting a VM as an OVA on page 222.
- Manage NGT. For more information, see Nutanix Guest Tools Overview on page 173.
- Define the QoS for Storage. For more information, see Storage Quality of Service (QoS) on page 194.
- Perform Memory Overcommit for new and existing VMs. For more information, see Memory Overcommit Management on page 196.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2574

- Define VM-Host Affinity, VM-VM Anti-affinity, and NGT Policies for VM Management. For more information, see Policies for VM Management on page 196.

VMs Summary View

The **Summary** tab on the **VMs** page provides a dashboard of all the VMs across registered clusters.

To access the summary view of all VMs, perform the following steps:

1. Log in to the Prism Central web console.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment.
3. Click the **Summary** tab.

   The system displays the **Summary** view of all the VMs across registered clusters:

   Note: To access the summary view of all the non-nutanix VMs that are managed by an external *vCenter*, select **Non-Nutanix** environment from the dropdown menu in the **VMs** page.

   The **Summary**, **Alerts**, and **Events** tabs display the same information as for Nutanix-managed VMs. The **Metrics** tab displays a subset of the full list (10 of the 12 metrics). The **List** tab displays fields for name, node name, hypervisor, memory, IP addresses, power state, and cluster name. While displaying the VM name, vCenter encodes any special characters included in the VM name to utf-8.

   Using playbooks, you can manage the VMs in **Non-Nutanix** environment. For more information about playbooks, see Task Automation - Playbooks in *Intelligent Operations Guide*.

Figure 35: Summary View - All VMs

The **VMs** page includes six tabs on the left (**Summary**, **List**, **Policies**, **Alerts**, **Events**, and **Metrics**) with a display area below the selected tab.

Note: This section describes the information and options that appear in the **Summary** page for all VMs. For instructions on how to view and organize that information in various ways, see Prism Central GUI Organization on page 54.

The **Summary** tab for all VMs displays the following three widgets:

- **Highlighted Entities**: Displays a list of the VMs with the highest usage of the <*parameter*> you select from the dropdown menu on the right of the widget. The <*parameter*> involves **CPU Usage**, **IO Latency**, **Memory Usage**, and **IOPS**. Click **View All XX VMs** link at the bottom to display the **List** tab.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2575

- **Alerts**: Displays a list of VM-related alerts that are generated during the specified <*interval*> you select from the dropdown menu on the right of the widget. The <*interval*> involves **Last week**(default), **Last 24 hours**, and **Last 1 hour**. When an alert appears, you can click the graph to view a list of those alerts. Click any alert to display the details page for that alert.
- **Anomalies**: Displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified <*interval*> you select from the dropdown menu on the right of the widget. The <*interval*> involves **Last week** (default), **Last 24 hours**, and **Last 1 hour**. When an anomaly appears, you can click the graph to view a list of those anomalies. Click any anomaly to display the event page for that anomaly.

List Tab

The **List** tab displays the list of VMs across all registered clusters.

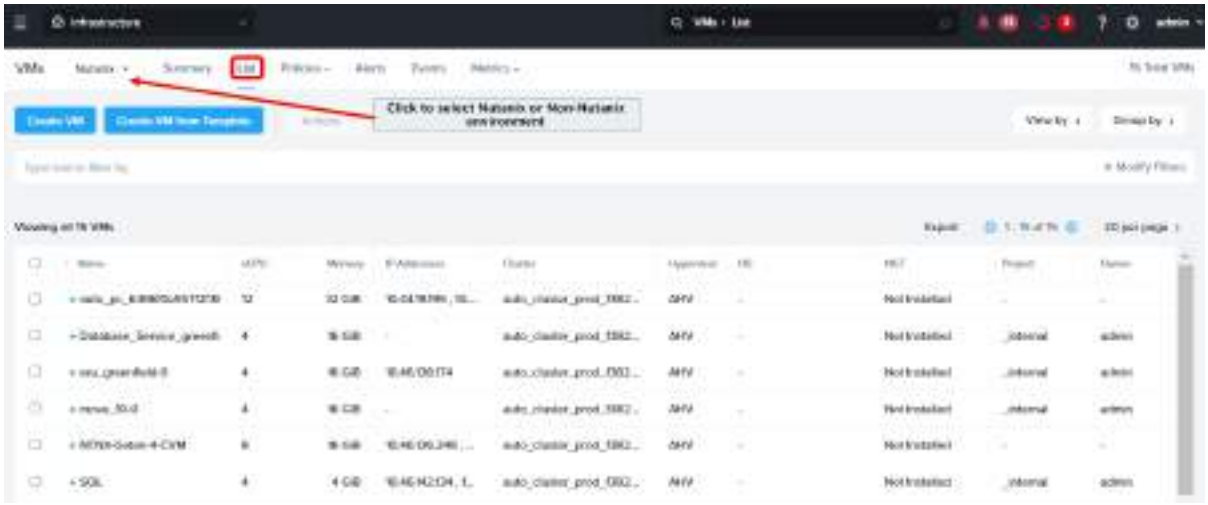


Figure 36: VMs List Tab

The following table describes the fields that appear in the VMs **List** tab.

> **Note:** The fields vary based on the **View by** and **Group by** options. A dash (-) is displayed in a field when a value is not available or applicable. For more information about **View by** and **Group by** options, see Prism Central GUI Organization on page 54.

Table 18: VMs List Tab - Field Description

Field	Description	Values
Select **General** from **View by** option.		
Name	Displays the VM name. You can click the VM name to view the detailed information for that VM. For information about VM details view, see VM Details View on page 117.	(VM name)
vCPU	Displays the virtual CPU count of the VM.	(vCPU count)
Memory	Displays the total amount of memory available to this VM.	xxx [MB|GiB]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2576

Field	Description	Values
IP addresses	Displays one or more VM IP addresses.	(IP address)
Cluster	Displays the name of the cluster in which the VM resides.	(cluster name)
Hypervisor	Displays the hypervisor type on which the VM is running.	AHV, ESX, or Hyper-V
OS	Displays the guest operating system of the VM.	(OS)
NGT	Displays whether Nutanix Guest Tools is installed on the VM.	Installed, Not Installed
Project	Displays the name of the project to which this VM belongs.	(project name)
Owner	Displays the owner (user name) of this VM.	(user name)
Select **Performance** from **View by** option.		
Name	Displays the VM name.	(VM name)
Memory Overcommit	Displays the Memory Overcommit state of the VM.	Enabled / Disabled
Memory Usage	Displays the percentage of allocated memory capacity currently being used by this VM.	0 -100%
CPU Usage	Displays the percentage of allocated CPU currently being used by this VM	0 -100%
Read IOPS	Displays read I/O operations per second (IOPS) for this VM.	(number)
Write IOPS	Displays write I/O operations per second for this VM.	(number)
IO Bandwidth	Displays I/O bandwidth used per second for this VM.	xxx [MBps|KBps]
IO Latency	Displays the average I/O latency for this VM.	xxx [ms]
Cluster	Displays the name of the cluster in which the VM resides.	(cluster name)
Select **Anomalous Behavior** from **View by** option.		
Name	Displays the VM name.	(VM name)
Anomaly Count	Displays the Anomaly count for Memory, I/O, CPU, Network, and Disks	(Integer number)
Anomaly Disabled	Displays whether Anomaly reporting is Disabled.	Yes/No
Select **Efficiency** from **View by** option.		
Name	Displays the VM name.	(VM name)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2577

Field	Description	Values
Efficiency	Displays the assessed efficiency of the VM. If a VM is performing in an expected range, the efficiency is listed as *Good*. If not, the type of inefficiency is displayed as determined by the VM behavioral learning engine. For more information, see Behavioral Learning Tools in *Intelligent Operations Guide*.	Good, Constrained, Overprovisioned, Inactive, Bully; (*NA* if insufficient baseline data for categorization, which is typically 21 days)
Reason	Displays the reason why a VM is considered inefficient. A dash (-) appears for a *Good* VM.	(text message)
Project	Displays the name of the project to which this VM belongs.	(project name)
Owner	Displays the owner (user name) of this VM.	(user name)
Cluster	Displays the name of the cluster in which the VM resides.	(cluster name)
Select **GPU** from **View by** option.		
Name	Displays the VM name.	(VM name)
GPU Configuration	Displays the GPU board (in case of Passthrough mode), vGPU software, type and number of vGPU instances in brackets (in case you configured the vGPU mode).	(GPU board/software-type name) Example: Passthrough - Nvidia Tesla M60 Example: vGPU - Nvidia GRID M60-8Q (2)
GPU Type	Displays the GPU configuration made as Passthrough or vGPU or if you did not configure GPU then a dash (-) appears.	[Passthrough|vGPU|-]
GPU Usage	Displays the percentage of GPU capacity being used by the VM.	(percentage)
GPU Framebuffer Usage	Displays the percentage of GPU framebuffer (RAM) capacity being used by the VM.	(percentage)
Select **Data Protection** from **View by** option.		
Name	Displays the VM name. You can click the VM name to view the detailed information for that VM. For information about VM details view, see VM Details View on page 117.	(VM name)
Categories	Displays the category mapped to the VM. For information about categories in Prism Central, see Category Management on page 456.	String (Category name)
Consistency Group	Displays the consistency group of the VM. For information about Consistency Groups in Prism Central, see Consistency Groups information in *Nutanix Disaster Recovery Guide* .	(Yes/No)
Protection Status	Displays the Protection Status of the VM.	(Protected/Unprotected)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2578

Field	Description	Values
Sync Status	Indicates the VM synchronization status between the Availability Zones in the Disaster Recovery setup.	(Sync Status)
Protection Type	Displays the type of protection defined for the VM.	(Protection Policy/ Legacy Protection Domain)
Protection Policy	Displays the protection policy that is applicable for the VM. For more information about protection policies, see Nutanix Disaster Recovery Guide.	(String) Protection Policy Name
Recovery Plans	Displays the recovery plans that is applicable for the VM. For more information about VM recovery plans, see Nutanix Disaster Recovery Guide.	(String) Recovery Plans Name
Select **Storage Configuration** from **View by** option.		
Name	Displays the VM name.	(VM name)
Replication Factor	Displays the Replication Factor setting for the VM in the storage policy applied to the VM.	Inherit from Container or 2 or 3
Encryption	Displays the Encryption setting for the VM in the storage policy applied to the VM.	Enabled or Inherit from Cluster
Compression	Displays the Compression setting for the VM in the storage policy applied to the VM.	Inline or Post Process (if enabled) , Disabled or Inherit from Cluster
Throttled Throughput (IOPS)	Displays the throttled throughput value in terms of IOPS set for the VM in the storage policy applied to the VM.	(Integer number)
Throttled Throughput (MB/s)	Displays the throttled throughput value in terms of MB/s set for the VM in the storage policy applied to the VM.	(Integer number)
Associated Policy	Displays the name of the storage policy applied to the VM.	(String) Storage Policy Name

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2579

Field	Description	Values
Compliance State	Displays the compliance state of the VM based on realization of the storage policy applied to the VM. **Note:** The compliance state is displayed as **In Progress** until the extent groups are synchronized by the Curator service at full scan intervals. Full scan intervals are intervals of 6 hours. Depending up on the time elapsed in the full scan interval at the time when the Replication Factor was set or updated, it may take up to 6 hours for the **In Progress** state to change to **Compliant** or **Non Compliant**.	**In Progress**, **Compliant** or **Non Compliant**
Cluster	Displays the name of the cluster that the VM resides in.	(String) Cluster Name
Select **Add custom** from **View by** option.		
Acropolis VM	Displays whether the VM is running on the AHV host.	(Yes/No)
Anomalies (Last 24 hours)	Displays the sum of all the anomaly counts for 20 metrics such as memory, I/O, CPU, network, and disks in the last 24 hours.	(Integer number)
AZ Name	Displays the availability zone specified to the VM.	AZ name
Cluster UUID	Displays the UUID of the cluster in which the VM resides.	(cluster UUID)
Constrained Level	Displays the VM constrained level along with the metric that constrains the VM.	“high”:”memory”, “moderate”:cpu” or “high”:”cpu”, “moderate”:memory”
Controller IOPS	Displays the total (read and write) I/O operations per second (IOPS) for the VM.	(Integer number)
Controller Read IO Bandwidth	Displays the read I/O bandwidth of the VM.	(Integer number (KBps))
Controller Read I/O Latency	Displays the read I/O latency of the VM.	(Integer number (ms))
Controller Write IO Bandwidth	Displays the write I/O bandwidth of the VM.	(Integer number (KBps))
Controller Write IO Latency	Displays the write I/O latency of the VM.	(Integer number (ms))
Created Timestamp	Displays the date and time of VM creation.	(date and time), Timestamp in MM DD, YYYY, hh: mm AM/PM format. For example, Oct 27, 2023, 06:51 AM
Description	Displays the description specified for the VM.	(description text)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2580

Field	Description	Values
Disk Capacity	Displays the total disk capacity of the VM.	(Integer number (GiB))
Disk Usage	Displays the disk usage percentage for the VM.	(0 - 100%)
Disk Usage Bytes	Displays the amount of used disk space.	(Integer number (GiB))
Efficiency Detail	Displays the reason why a VM is considered inefficient.	(text message)
Health	Displays the health state of the VM.	(Critical/Warning/Good)
Host	Displays the host name. This field might be blank if the VM is powered off and a host is not assigned.	(hostname)
Host IP	Displays the host IP address.	(IP address)
Host UUID	Displays the UUID of the host.	(host UUID)
Hypervisor IOPS	Displays the total (read and write) I/O operations per second (IOPS) from the hypervisor for the VM.	(Integer number)
IS CVM	Displays whether the VM is a CVM or not.	(Yes/No)
Network Adapters	Displays the number of network adapters in the VM.	(Integer number)
Network Rx Bytes	Displays the number of bytes received from the network.	(Integer number)
Network Rx Packets Dropped	Displays number of packets received from the network and dropped.	(Integer number)
Network Tx Packets Dropped	Displays number of packets sent to the network and dropped.	(Integer number)
NGT communication status	Displays the NGT communication status between CVM and guest VMs. For more information, see Nutanix Guest Agent and Controller VM Communication on page 189.	(Active/Inactive)
NGT communication type	Displays the transport channel established between CVM and guest VMs. For more information, see Verifying Communication Type Using Prism Central on page 191.	(IP-based/IP-less)
NGT Installed Version	Displays if NGT is installed in the VM. For more information, see Installing NGT on page 176.	(Installed/Not Installed/ Latest)
Overprovisioned	Displays the type of over-provisioned VMs. **Note:** This and the following field filters based on a VM efficiency algorithm, which is part of the VM behavioral learning capabilities (see Behavioral Learning Tools).	(Good/High/Moderate)
Overprovisioned level	Displays the VM overprovisioned level along with the metric that overprovisions the VM.	“high”:”memory”, “moderate”:cpu” or “high”:”cpu”, “moderate”:memory”

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2581

Field	Description	Values
Power State	Displays whether the VM is powered off or powered on.	(Off/On)
Services Enabled	Displays the name of the NGT services enabled in the VM.	(file_level_restore, vss_snapshot)
Shared Usage	Displays the shared data usage by the VM.	(Integer number (GiB))
Snapshot Usage	Displays the amount of storage used for snapshots.	(Integer number (GiB))
Total Working Set Size	Displays the total working set size of the VM. Working set is the amount of memory that a VM requires in a given time interval.	(Integer number (GiB/MiB))
Virtual NICS	Displays the name of the virtual NIC that allows the VM to connect to a network	(NIC name)
VM Type	Displays the type of VM.	(Guest, PCVM, MSP, AFS)
VPC Name	Displays the VPC Name specified for the VM.	(VPC name)
Working Set Size Read	Displays the read working set size of the VM.	(Integer number (GiB/MiB))
Working Set Size Write	Displays the write working set size of the VM.	(Integer number (GiB/MiB))

You can perform the following actions for the VMs in the **List** tab:

- Access the detailed information about an individual VM. For more information, see VM Details View on page 117.
- Filter the VMs list based on available parameter values using **Filters** pane. For more information, see Filters Pane - VMs Page on page 112.
- Export the table that contains the list of VMs and their information to a file in a CSV format. For more information, see Export on page 59.
- Group the VMs based on pre-defined criteria. For information about how to group the VMs, see Group by on page 56.
- View VMs based on pre-defined criteria or create a custom view. For information about available views and how to create a custom view, see View by on page 56.
- Assign a label to the filtered criteria. For information about how to define a label, see Label on page 59.
- Create a VM. For more information about how to create a VM, see Creating a VM through Prism Central (AHV) on page 130 or Creating a VM through Prism Central (ESXi) on page 170.
- Perform the VM-specific actions on a single or multiple VMs using the **Actions** dropdown menu. For instructions on how to perform these actions, see Managing a VM through Prism Central (AHV) on page 143 or Managing a VM through Prism Central (ESXi) on page 172.

> **Note:** The available actions appear in bold; other actions are grayed out. For grayed out options, a tool tip explaining the reason is provided. The available actions depend on the current state of the selected VM(s).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2582

Filters Pane - VMs Page

The following table describes the fields available in the **Filters** pane:

Table 19: Filter Pane Fields

Parameter	Description	Values
Labels	Filters based on label name. Select one or more labels from the **Labels** dropdown menu. If there are no labels currently, the system displays a message about how to create labels.	(label names)
Name	Filters based on the VM name. Select a condition from the dropdown menu and enter a string in the field. The system returns a list of VMs that satisfy the VM name condition/string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	(VM name string)
Description	Filters based on the description specified for the VM. Enter a string in the field to filter the result. The system returns a list of VMs that satisfy the description string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	(Description string)
IP Addresses	Filters based on the IP address specified for the VM. Enter a valid IP address in the field to filter the result. The system returns a list of VMs that satisfy the IP address string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	(A Valid IP Address)
VPC Name	Filters based on the VPC Name specified for the VM. Enter a string in the field to filter the result. The system returns a list of VMs that satisfy the VPC string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	(VPC name string)
Host	Filters based on the host name. Select a condition from the dropdown menu and enter a string in the field. The system returns a list of VMs that satisfy the host name condition/string.	(host name string)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2583

Parameter	Description	Values
Cluster	Filters based on the cluster name. Select a condition from the dropdown menu and enter a string in the field. The system returns a list of VMs that satisfy the cluster name condition/string.	(cluster name string)
Categories	Filters based on category names. Enter a category name in the field and then check the box. As you type a dropdown menu appear to help you select the correct category. A new field appears where you can add more categories to the filter. The number of VMs tagged to each selected category are displayed in the **List** tab.	(category name)
Quarantined	Filters based on the Quarantined mechanism. Select either **Strict** or **Forensics** or both the checkboxes. The system displays the number of VMs currently quarantined as Strict or Forensics.	Strict, Forensics
Hypervisor	Filters based on the hypervisor type. Select one or more of the checkboxes to filter on those hypervisors. The system displays the number of VMs currently on each hypervisor type.	AHV, ESX, Hyper-V
Health	Filters based on the VM health state (good, warning, or critical). Select one or more states to return a list of VMs in that state(s). The system displays the number of VMs currently in each state.	Critical, Warning, Good
Nutanix Guest Tools	Filters based on the NGT status. Select one or more NGT status to return a list of VMs with selected NGT status. For more information on **Nutanix Guest Tools** filters, see Installing NGT on page 176.	Installed, SSR, VSS, VSS and SSR, Not installed
Power State	Filters based on the VM power state. Select one or more states to return a list of VMs in that state(s). The system displays the number of VMs currently in each state.	On, Off, Suspended, Paused, Unknown
Is CVM	Filters based on the whether the VM is a CVM or not. The system displays the number of CVMs, if filter selected is **Yes**.	No, Yes
VM Type	Filters based on the type of VM. Select either Guest, PCVM, MSP, AFS or multiple checkboxes. The system displays the number of VMs of each type.	Guest, PCVM, MSP, AFS
Memory Overcommit	Filters based on the Memory Overcommit status. Select one or more Memory Overcommit status to return a list of VMs with selected status.	Enabled, Disabled, Not Available
Memory Usage	Filters based on the amount of memory capacity being used. Select the checkbox(es) for the desired percentage range or enter a percentage range in the ***from <low> to <high> %*** field. The system returns a list of VMs utilizing memory in that range.	([xx] to [yy]% range)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2584

Parameter	Description	Values
CPU Usage	Filters based on the processor usage. Select the checkbox(es) for the desired percentage range or enter a percentage range in the ***From <low> to <high> %*** field. The system returns a list of VMs utilizing memory in that range.	([xx] to [yy]% range)
Read IOPS	Filters based on the read IOPS. Select the checkbox(es) for the desired range or enter a range in the ***From <low> to <high> IOPS*** field. The system returns a list of VMs with read IOPS in that range.	([xx] to [yy] IOPS range)
Write IOPS	Filters based on the write IOPS. Select the checkbox(es) for the desired range or enter a range in the ***From <low> to <high> IOPS*** field. The system returns a list of VMs with write IOPS in that range.	([xx] to [yy] IOPS range)
I/O Bandwidth	Filters based on the I/O bandwidth used. Select the checkbox(es) for the desired range or enter a range in the ***From <low> to <high> Mbps*** field. The system returns a list of VMs with I/O bandwidth usage in that range.	([xx] to [yy] Mbps range)
I/O Latency	Filters based on the average I/O latency. Select the checkbox(es) for the desired range or enter a range in the ***From <low> to <high> ms*** field. The system returns a list of VMs with average I/O latency in that range.	([xx] to [yy] ms range)
Over Provisioned	Filters for over-provisioned VMs. Select the checkbox(es) for the desired type (high and moderate). **Note:** This and the following two fields filter based on a VM efficiency algorithm, which is part of the VM behavioral learning capabilities. For more information, see Behavioral Learning Tools in *Intelligent Operations Guide*.	High, Moderate
Constrained	Filters for constrained VMs. Select the checkbox(es) for the desired type (high and moderate).	High, Moderate
Efficiency	Filters for certain VM profiles. Check the boxes for the desired profile types. There is one for efficient VMs (good) and four for inefficient VMs (bully, over-provisioned, constrained, and inactive).	Bully, Over Provisioned, Constrained, Inactive VM, Good
GPU Configuration	Filters for GPU configuration information such as model name. Enter the GPU configuration information in the field and then select the checkbox. As you type, a dropdown menu appears to help you select the correct configuration information.	(configuration info)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2585

Parameter	Description	Values
GPU Type	Filters based on GPU operational mode. Select the checkbox for one or more of the GPU types.	vGPU, Passthrough, Passthrough(Compute)
vCPU	Filters based on the number of vCPUs allocated to the VM. Select one or more numeric checkboxes to return a list of VMs with selected number of vCPUs.	vCPU Integer value
GPU Usage	Filters based on the amount of GPU capacity being used. Enter a percentage range in the ***from <low> to <high> %*** field. The system returns a list of GPUs in that range.	([xx] to [yy]% range)
GPU Framebuffer Usage	Filters based on the amount of GPU framebuffer (RAM) capacity being used. Enter a percentage range in the ***from <low> to <high> %*** field. The system returns a list of GPUs in that range.	([xx] to [yy]% range)
Storage Configuration	Filters based on the storage policy configuration parameters set for VM. This view displays the storage configurations parameters set for the VMs by storage policies applied to the VMs. For more information about storage policies, see Storage Policies Summary View on page 511.	Storage policy name
vGPU Guest driver Version	Filters on the guest driver version. Enter the guest driver version number in the field.	(guest driver version number)
AZ Name	Filters based on the availability zone specified of the VM. Enter a string in the field to filter the result. The system returns a list of VMs that satisfy the AZ string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	AZ String
NGT Communication Status	Filters based on the NGT communication status between CVM and guest VMs. Select the communication status to filter the result. The system returns a list of VMs that satisfy the selected status.	Active, Inactive
NGT Communication Type	Filters based on the transport channel established between CVM and guest VMs. Select the required transport channel checkbox to filter the result. The system returns a list of VMs that satisfy the selected transport channel.	IP-Less, IP-Based

Policies Tab

The **Policies** tab displays **VM-Host Affinity Policies**, **VM-VM Anti-affinity Policies**, and **NGT Policies**.

For more information about how to configure **VM-Host Affinity Policies**, **VM-VM Anti-affinity Policies**, and **NGT Policies**, see VM-Host Affinity Policies Defined in Prism Central on page 463, VM-VM Anti-Affinity Policies Defined in Prism Central on page 474, and NGT Policies on page 484.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2586

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options that are available on the **Activity** > **Alerts** page, however it only displays the VM-related alerts across the registered clusters. For more information about alerts, see Prism Central Alerts and Events Reference Guide.

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options that are available on the **Activity** > **Events** page, however it only displays the VM-related events across the registered clusters. For more information about events, see Prism Central Alerts and Events Reference Guide.

Metrics Tab

The **Metrics** tab allows you to view performance metrics across the VMs. Click the **Metrics** tab to display dropdown menu of available metrics, and select the metric name to display the relevant performance information.

> **Note:** The **Metrics** dropdown menu is hypervisor-specific, and might vary based on the hypervisors used in the cluster.

The following table describes the dropdown menu list of the **Metrics** tab:

Table 20: Metrics Tab Fields

Metric	Description
CPU Usage	Displays a CPU usage table that lists the current values and total VMs (number). The current values are split into percentile intervals (for example, less than 25%, 25-50, 50-75, more than 75%). You can click a percentile interval to view the **Summary** tab filtered with selected VMs. **Note:** The same format also applies to the other metrics in this table with either percentile or quantity intervals.
CPU Ready Time	Displays a CPU ready time percentage usage table.
Memory Usage	Displays a memory percentage usage table.
Memory Swap	Displays memory swap-out and swap-in rate tables.
IOPS	Displays total, read, and write IOPS tables.
IO Latency	Displays total, read, and write I/O latency rate tables.
I/O Bandwidth	Displays total, read, and write I/O bandwidth rate tables.
Storage Usage	Displays total, snapshot, and shared storage size tables.
Working Set Size	Displays total, write, and read working set size tables. Working set is the amount of memory that a VM requires in a given time interval.
Network Packets Dropped	Displays tables for the number of transmitted and received packets dropped.
Network Bytes	Displays tables for the amount of transmitted and received bytes (in GiB).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2587

Metric	Description
Disk Usage	Displays a disk usage table that lists the current values and total VMs (number). The current values are split into percentile intervals, for example, l3.68% - 4.1%, more than 4.93%. Click a percentile interval to display the **Summary** tab filtered to just those VMs. **Note:** The same format also applies to the other metrics in this table with either percentile or quantity intervals.

VM Details View

To access the details view of an individual VM, perform the following steps:

1. Log in to the Prism Central web console.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment. For information about how to access the list of VMs in **Non-Nutanix** environment (non-nutanix VMs managed by external *vCenter*), see VMs Summary View on page 104.
3. Click the target <*VM_Name*> to view the **Summary** tab of an individual VM.

   Note: Replace <*VM_Name*> with the actual VM name at your site.

The following is an example showing the **Summary** tab of an individual VM:

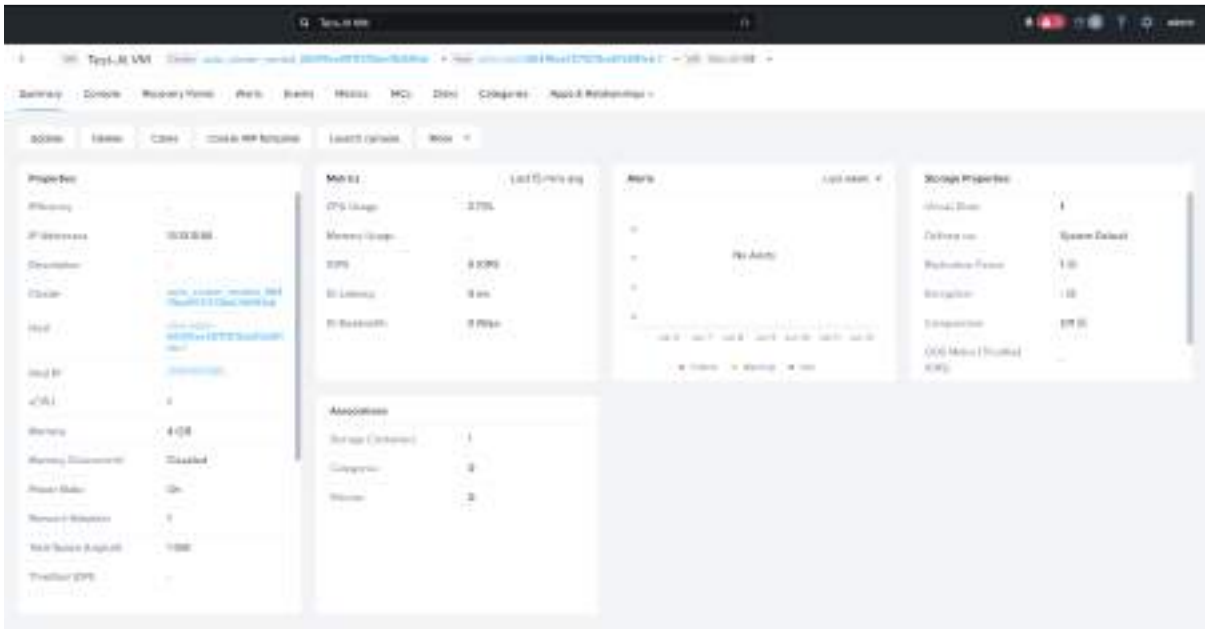


Figure 37: Summary Tab - Individual VM

Note: VirtIO must be installed in a VM for AHV to display correct VM memory statistics. For more information about VirtIO drivers, see Nutanix VirtIO for Windows in *AHV Administration Guide*.

The **Summary** tab of an individual VM provides the following widgets:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2588

- **Properties**: Displays summary information about the VM. For information about the fields available in **Properties** widget, see Properties Widget - Parameter Details on page 118.
- **Alert**: Displays a list of related alerts that occurred during the specified interval. Select either **Last week** (default), **Last 1 hour**, or **Last 24 hours** from the dropdown menu on the top right corner of the widget.
- **Anomalies**: Displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified interval. Select either **Last week** (default), **Last 1 hour**, or **Last 24 hours** from the dropdown menu on the top right corner of the widget. When an anomaly appears, you can click the graph to display a list of those anomalies. If you click an individual anomaly, the system displays the event page for that anomaly.
- **Storage Properties** : Displays the storage properties of the VM as defined in the storage policy associated with the VM. The storage properties involve the actual values for Replication Factor, Encryption, and Compression that is applied to the VM. For information about the fields available in **Storage Properties** widget, see Storage Properties Widget - Parameter Details on page 120.
- **Associations**: Displays the other entities associated with the VM such as Virtual Disks, Storage Containers, Categories and policies (storage policies). For information about the fields available in **Associations** widget, see Associations Widget - Parameter Details on page 121.

  Note: In the **Storage Properties** widget, for any storage property, even if the "i" symbol specifies **Inherited from Cluster**, but the **Association** widget always displays the actual inherited values.

  The following is an example showing the VM Storage Properties and Associations Widget:

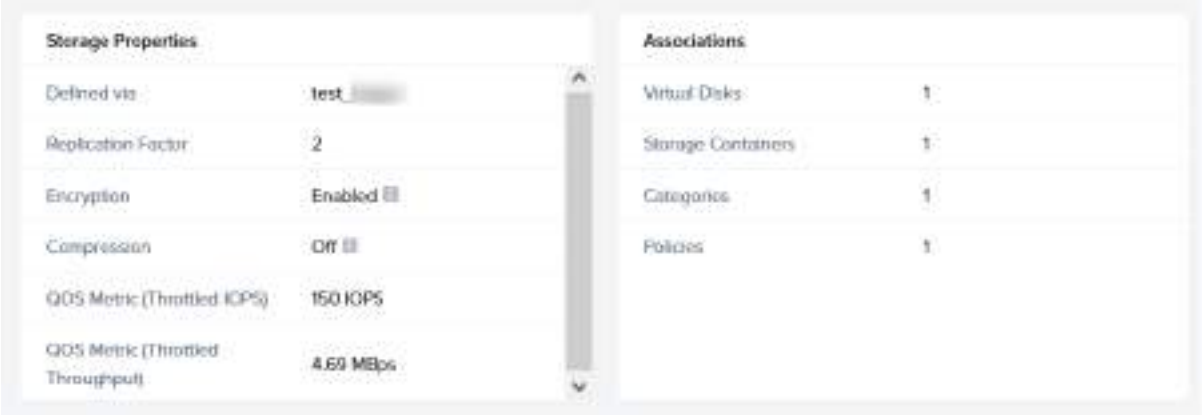


Figure 38: VM Storage Properties and Associations Widget

<*Action*> available above the widgets and under **More** dropdown menu. Click the appropriate <*Action*> to run that administrative action on the VM. The available <*Action*> appear in bold, and the other actions are grayed out. The available actions depend on the current state of the VM. For more information about how to perform any <*Action*>, see Managing a VM through Prism Central (AHV) on page 143.

Note: You can perform administrative actions on VMs in Acropolis-managed clusters only.

Properties Widget - Parameter Details

The following table describes the fields available in the **Properties** widget.

Note: A dash (-) in a field indicates that there is not enough data to evaluate or a value is not assigned.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2589

Table 21: VM Properties - Parameter Details

Parameter	Description	Values
Efficiency	Displays the efficiency state for this VM. If the efficiency is not good, an additional field may appear that specifies the problem. For example, if the VM is constrained, a Constrained field appears that identifies the constrained resource such as the CPU or memory. **Note:** The Anomalies, Efficiency, Over provisioned, and Constrained parameters relate to the VM behavioral learning feature. For more information, see Behavioral Learning Tools in *Intelligent Operations Guide*.	Bully, Over Provisioned, Constrained, Inactive VM, Good
IP Addresses	Displays one or more IP addresses assigned to the VM.	(IP address)
Description	Displays the description specified for the VM	*<Description Text>*
Cluster	Displays the name of the cluster in which the VM resides.	(cluster name)
Host	Displays the host name. This field may be blank if the VM is powered off and a host is not assigned.	(host name)
Host IP	Displays the host IP address.	(IP address)
vCPU	Displays the number of virtual CPUs assigned to this VM.	(number)
Memory	Displays the amount of memory available to this VM.	xxx [MB|GB]
Memory Overcommit	Displays whether Memory Overcommit is enabled or disabled. For more information on Memory Overcommit feature, see Memory Overcommit	Enabled -
Power State	Displays whether the VM is powered on or powered off	On, Off
Network Adapters	Displays the number of network adapters available to this VM.	(# of adapter ports)
Total Space (Logical)	Displays the total disk capacity available to this VM.	xxx [GB|TB]
Throttled IOPS	Displays the throttled throughput value in IOPS. For more information about Throttled IOPS, see Storage Quality of Service (QoS) on page 194.	-
NGT Status	Displays if NGT is installed	Installed, Not Installed, Latest
Services Enabled	Displays the services enabled for this VM.	*<Services>* such as NCM Self-Service (formerly known as Calm), Karbon, and so on.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2590

Parameter	Description	Values
NGT	Displays the NGT version installed on the VM	*<NGT version>* such as 21.5
NGT Cluster Version	Displays the NGT version available on the cluster	*<NGT version>* such as 21.5
Owner	Displays the VM owner name.	admin (if VM is created by Prism Central admin user.
Project	Displays the name of the project to which the VM is mapped.	*<Project Name>* such as *_Internal*for projects created by admin user.
(the following fields appear when the VM is allocated to a GPU)		
GPU Type	Displays the GPU operational mode. If it is vGPU, the following fields also appear.	vGPU, Passthrough, None
GPU Configuration	Displays the vGPU profile used.	(vGPU profile name)
Framebuffer	Displays the size of the GPU framebuffer (RAM).	xxx GiB
Virtual Slice	Displays the virtual slice applied. The "virtual slice" reflects the approximate amount of physical GPU resources that the vGPU can receive. **Note:** The Virtual Slice and vGPU Guest Driver Version fields do not appear for passthrough GPUs.	(slice amount)
vGPU Guest Driver Version	Displays the version number of the vGPU guest driver.	(version number)

Storage Properties Widget - Parameter Details

The following table describes the fields available in the **Storage Properties** widget.

Note: A dash (-) in a field indicates that there is not enough data to evaluate or a value is not assigned. For more information about the Storage properties, see Storage Policy Details View on page 514.

Table 22: Storage Properties Widget - Parameter Details

Parameter	Description	Values
Defined via	Displays the name of the storage policy that the VM is associated with.	Storage policy name
Replication Factor	Displays the Replication Factor setting for the VM in the storage policy applied to the VM.	Inherit from Container or 2 or 3
Encryption	Displays the status of encryption that the storage policy applies to the VM.	Enabled or Inherit from Cluster

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2591

Parameter	Description	Values
Compression	Displays the status and type of compression that the storage policy applies to the VM.	Inline, Post Process, Off or Inherit from Cluster
QOS Metric (Throttled IOPS)	Displays the type of QOS metric that the storage policy applies to the VM with the throttled throughput value in IOPS.	(Integer) IOPS
QOS Metric (Throttled Throughput)	Displays the type of QOS metric that the storage policy applies to the VM with the throttled throughput value in MBps.	(Integer) MBps

Associations Widget - Parameter Details

The following table describes the fields available in the **Associations** widget.

> **Note:** A dash (-) in a field indicates that there is not enough data to evaluate or a value is not assigned.

Table 23: Associations Fields

Parameter	Description	Values
Virtual Disks	Displays the number of virtual disks associated with the VM.	(number)
Storage Containers	Displays the number of storage containers associated with the VM.	(number)
Categories	Displays the number of categories associated with the VM.	(number)
Policies	Displays the number of policies like storage policies and Image Placement policies that are associated with the VM.	(number)

Entity Relationship Information

The entity relationship involves relationship between related entities like clusters, hosts, and VMs instances. It allows quick access between the related entities. You can directly navigate to a target cluster, host, or VM instance through the respective dropdown menus.

Example: Displaying Relationship between Entities

The following example indicates that VM *auto_pc_611cd08373101ab68d756c9a0* resides on host *cool-07-2* and cluster *auto_cluster_prod_rohan_bajaj_1ab68d756c98*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2592

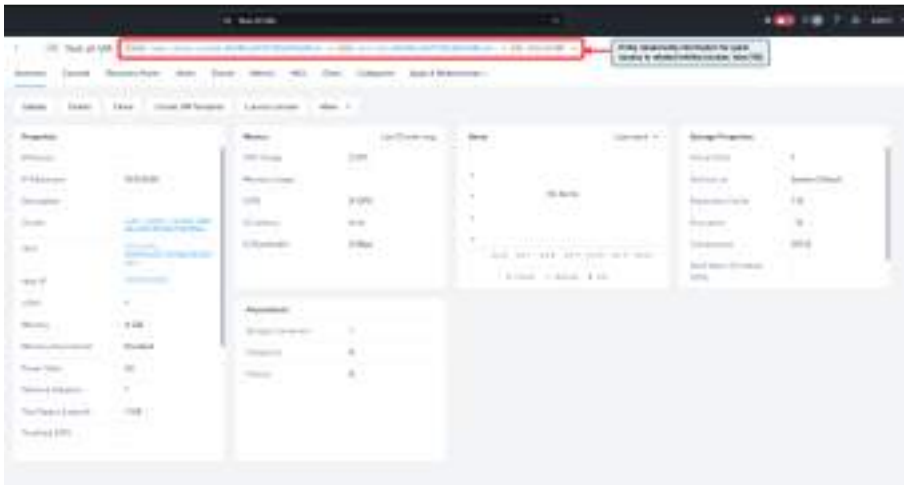


Figure 39: VM Summary: Entity Relationship Information

Example: Viewing VMs on a Cluster

Click the **VM** dropdown menu to view the list of VM instances in the selected cluster. Alternatively, you search the VM instance name residing on the target cluster.

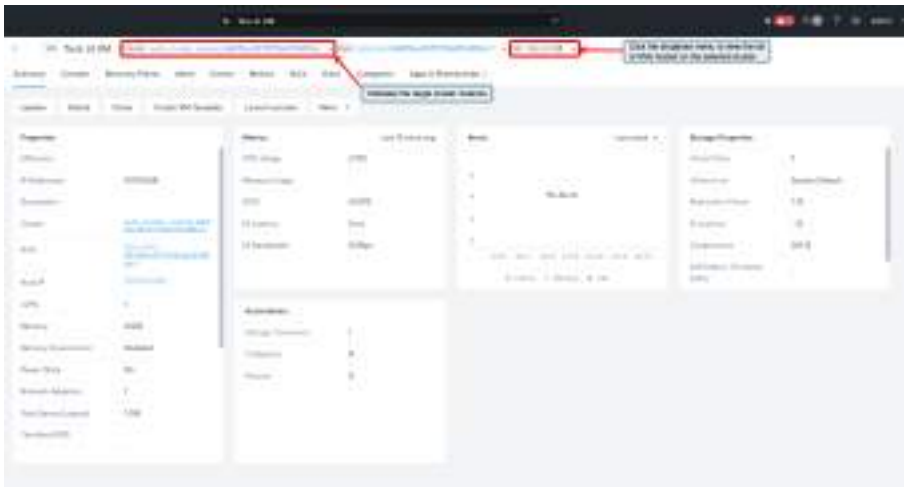


Figure 40: VMs on a Cluster

Example: Viewing VM Instances on a Host

Click the **VM** dropdown menu to view the list of VM instances on the selected host. Alternatively, you can search the VM instance name belonging to the target host.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2593

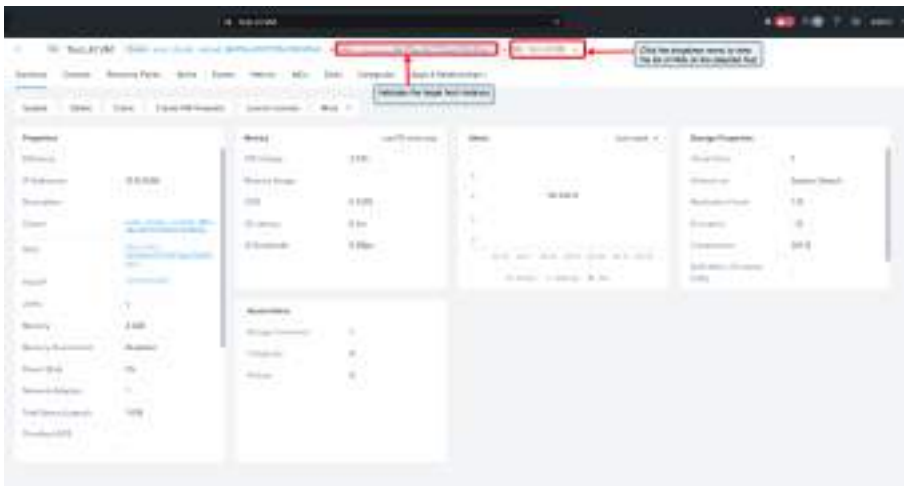


Figure 41: VMs on a Host

Note:

- The **Recent** label indicates the last accessed entity instances. The system displays a maximum of three recently accessed entity instances.
- The filtered list of VMs display only the powered-on VM instances.
- If the VMs are not filtered on a host instance, all VMs on the selected cluster are displayed.

Console Tab

The **Console** tab displays the VM console screen. There are three icons available on the top right corner of the console screen).

- Click the Reboot icon to send a **Control-Alt-Delete** command to the console.
- Click the Screenshot-capture icon to take a screen shot of the console display.
- Click the Launch icon to open the console in a new window.

Recovery Points Tab

The **Recovery Points** tab displays a list of recovery points (backup snapshots) when recovery points are created for the selected VM.

For information about how to create a recovery point, see Managing a VM through Prism Central (AHV) on page 143.

The protection policy associated with the VM also creates the VM recovery points for Disaster Recovery. For more information about VM recovery points, see Nutanix Disaster Recovery Guide.

The list is blank if there are no recovery points available. The total number of recovery points and the latest and oldest recovery points are listed on the left. A list of all recovery points appears in a table on the right with the create time, location, expiry time, and recovery point type provided for each recovery point.

You can restore or replicate a VM from a recovery point. Select the recovery point and click the required action from the **Actions** menu:

- Click **Clone** to create a new cloned VM from the selected recovery point.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2594

- Click **Replicate** to replicate a VM from the selected recovery point either locally or remotely in a state of a chosen recovery point.
- Click **Restore** to restore the VM from the selected recovery point.
- Click **Delete** to delete the recovery point.

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options as the Alerts dashboard, however it is filtered to display the alerts only for the selected VM (individual VM). For more information about alerts, see Prism Central Alerts and Events Reference Guide.

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options as the Events dashboard, however it is filtered to display the events only for the selected VM (individual VM). For more information about events, see Prism Central Alerts and Events Reference Guide.

Metrics Tab

The **Metrics** tab allows you to view usage metrics for the selected VM.

Click the **Metrics** tab to view the graphs for all the metrics . The graph is a rolling time interval performance or usage monitor. The baseline range appears as a blue band in the graph.

> **Note:** The baseline range and identified anomalies are based on sophisticated machine-learning capabilities. For more information, see Behavioral Learning Tools in *Intelligent Operations Guide*. The machine-learning algorithm uses 21 days of data to monitor and predict performance. A graph or baseline band may not appear if less than 21 days of data is available.

You can perform the following actions in the **Metrics** tab:

- Place the cursor anywhere on the horizontal axis to display the value at that time.
- Select the duration (time interval) from the dropdown menu on the right (last 1 hour, last 24 hours, or last week).
- Click the **Filters** option to select one or more appropriate metric checkboxes to display the selected metrics in the **Metrics** page. For more information, see Table 24: Metrics Tab Fields on page 125.
- From the **Actions** dropdown menu that appears on the top-right corner of each metrics widget, you can perform the following operations:
  - Select **Alert Settings** to create an alert policy for the selected metric. For more information about how to create alert policies, see Prism Central Alerts and Events Reference Guide.
  - Select **Add to Analysis** to add the selected metric to **Analysis** dashboard. For more information, see Analysis Dashboard in *Intelligent Operation Guide*.

The following table describes the metrics available in **Metrics** tab:

> **Note:** Metrics are hypervisor-dependant, and might not be available on all hypervisors.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2595

Table 24: Metrics Tab Fields

Metric	Description
CPU Usage	Displays the percentage of CPU capacity currently being used by the VM (0–100%).
CPU Ready Time	Displays the current, high, and low percentage of CPU wait time (0–100%).
Memory Usage (%)	Displays the percentage of memory capacity currently being used by the VM (0–100%).
IOPS related metrics	Displays separate graphs for total, write, and read I/O operations per second (IOPS) for the VM.
IO Latency related metrics	Displays separate graphs for total, write, and read average I/O latency (in milliseconds) for physical disk requests by the VM.
IO Bandwidth related metrics	Displays separate graphs for total, write (only), and read (only) I/O bandwidth used per second (MBps or KBps) for physical disk requests by the VM.
Usage related metrics	Displays separate graphs for disk, snapshot, and shared data usage (in GiBs) by the VM.
Working Set Size related metrics	Displays separate graphs for total, write, and read storage usage (in GiBs) for the VM working set size.
Disk Usage (%)	Displays the disk usage percentage for the VM.
Dropped Network Packets related metrics	Displays separate graphs for the number of transmitted and received packets dropped.
Network Bytes related metrics	Displays separate graphs for the amount of transmitted and received bytes (in GiBs).

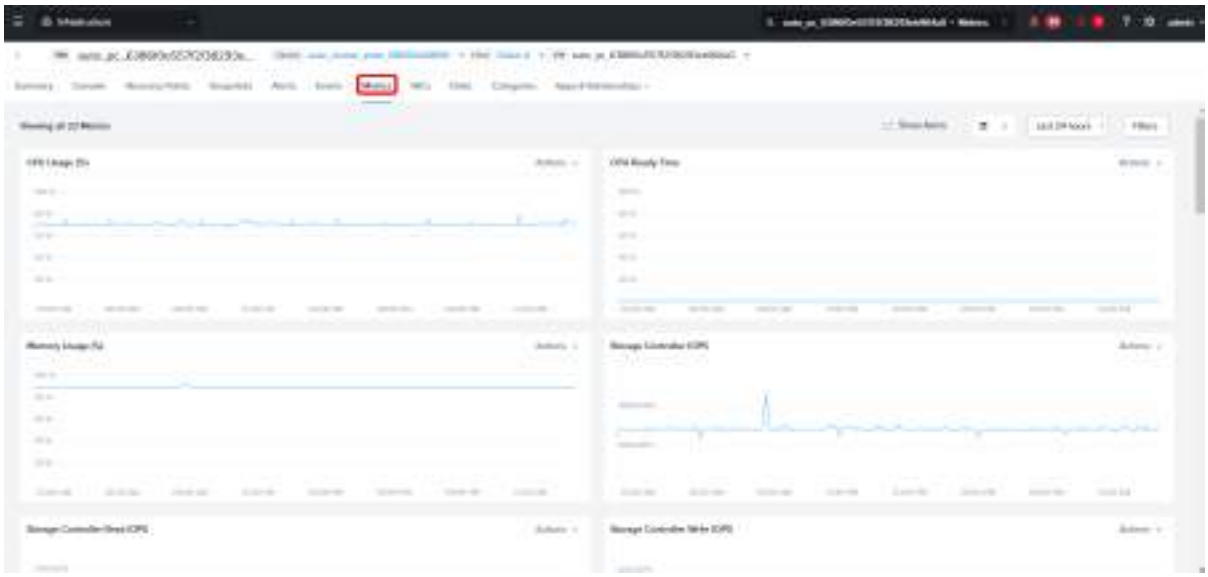


Figure 42: Metrics Tab

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2596

NICs Tab

The **NICs** tab displays information in tabular form about the virtual NICs in the VM. Each line represent a virtual NIC, and the following table describes the fields.

Table 25: NIC Fields

Parameter	Description	Values
VLAN ID	Displays the VLAN ID of the NIC.	(VLAN ID
MAC Address	Displays the virtual NIC MAC address.	(MAC address)
Network Connection State	Displays whether the NIC is connected to the network currently.	Connected, Disconnected
VPC	Displays the Virtual Private Cloud (VPC) of the NIC. For more information about VPC, see Virtual Private Clouds on page 356.	(VPC name)
Virtual Switch	Displays the virtual switch of the NIC. For more information about how to create a virtual switch, see Creating a Virtual Switch on page 349.	(Virtual Switch Name)
IP Address	Displays the virtual NIC IP address	(IP address)
Action	Displays the available actions you can perform on the NIC.	Delete

Disks Tab

The **Disks** tab displays information in tabular form about the virtual disks in the VM. Each line represents a virtual disk, and includes the following fields.

- **Disk Address**: Displays the disk address (such as ide.0 or scsi.1).
- **Capacity**: Displays the disk capacity (in MiB or GiB).

Categories Tab

The **Categories** tab displays the categories and image placement policies associated with the VM. Each VM can have a one-to-many relationship with categories and the categories can have a many-to-one relationship with image placement policies.

For more information about categories management and image placement policies, see Category Management on page 456 and Image Placement Policies on page 488.

Apps & Relationships Tab

The **Apps & Relationships** tab displays a dropdown menu with two options: **Discovered Apps** and **App Relationships**.

> **Note:** Application Discovery function needs to be enabled to view the **Discovered Apps** and **App Relationships**. For more information about Application discovery function and how to enable it in Prism Central, see Application Discovery in *Intelligent Operations Guide*.

The **Discovered Apps** page displays (up to) the top 20 applications that are communicating with other entities (usually client VMs). The discovered applications are sorted based on the number of clients communicating with the application. This menu option provides similar information as the application discovery dashboard, except it

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2597

is filtered to display the details only for this VM . For more information, see Application Discovery in *Intelligent Operation Guide*.

The **App Relationships** page displays three tabs: **Visualization**, **Incoming List**, and **Outgoing List**. All the three tabs display (up to) the top 20 results with respect to the visualization, incoming or outgoing client communication.

The **Visualization** tab displays a visual representation of the VM and the applications running on it, along with its incoming and outgoing communication with other entities. Data for last 24 hours is fetched to display the information on the visualization tab.

You can perform the following actions in **Apps & Relationships** tab:

- Hover on an entity to see the communication details with the applications.
- Hover on an application to see the incoming communication of the application with external entities and outgoing communications of the VM on which the application is running.

> **Note:** In case of dual NIC VMs, click and expand the App listing to view the specific IP that is being used by the application.

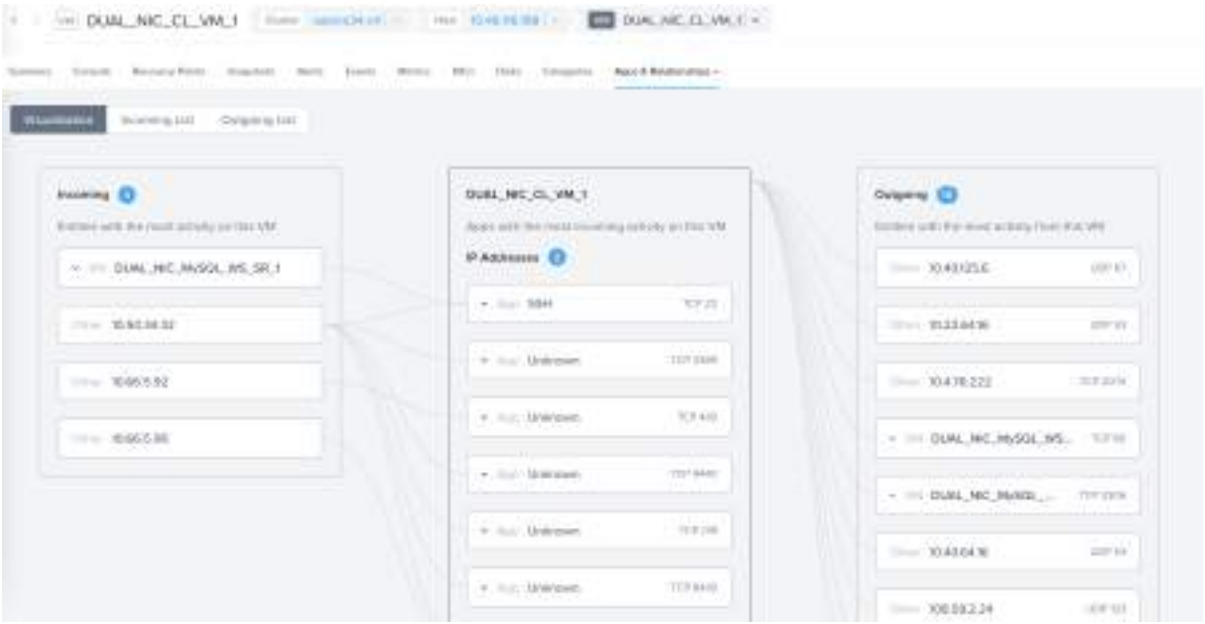


Figure 43: Visualization Tab

Incoming List: Displays a list of entities having incoming communication with this VM. Each line represents an incoming communication and includes the following fields.

Table 26: Incoming List Fields

Parameter	Description	Values
Source Entity Name	Displays the name of the communicating entity. If the entity is not identified by Prism Central (through registered PE or through vCenter using monitoring configurations feature), the name is displayed as unknown.	(VM name), Unknown

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2598

Parameter	Description	Values
Source IP Address	Displays the IP Address of the communicating entity.	(IP Address)
Destination App	Displays the name of the application that is being communicated to. If the application is not an identified one, the Destination App is displayed as Unknown.	(application name), Unknown
Destination IP Address	Displays the IP Address of the VM.	(IP address)
Destination Port	Displays the port used by the application for communication.	(port number)
Destination App Identification Status	Indicates whether the application is an identified application type. An identified application is one that is a known type.	Identified, Unidentified

Click **Modify Filters** option to view the **Filters** pane. You can use the **Filters** pane to select a filter option.

You can apply filters with multiple fields. The filters fetch the latest discovery and communication data and accordingly display the result set, to a maximum of 20 results.

The following table describes the filter options for **Incoming List**.

Table 27: Filters Pane - Incoming List

Field	Description	Values
Source Entity Name	Filters based on the source entity name. Select a condition from the dropdown menu (**Contains**, **Equal to**, **Not equal to**, **Doesn't contain**, **Starts with**, **Ends with**) and enter a string in the field.	(source entity name string)
Entity Type	Filters based on the entity type. A VM belongs to a cluster managed by Prism Central or vCenter (only if using monitoring configurations feature). An Unknown entity is one that is not identified by Prism Central.	VM, Unknown
Source IP Address	Filters based on the source IP address.(same options as Source Entity Name).	(source IP address string)
Destination App	Filters based on the destination app (same options as Source Entity Name).	(Destination App string)
Destination IP Address	Filters based on the destination IP address (same options as Source Entity Name).	(destination IP address string)
TCP Port	Filters based on the TCP port number.	(TCP port number)
UDP Port	Filters based on the UDP port number.	(UDP port number)
Time Range	Filters based on the time range.	Last 30 Mins, Last 1 Hour, Last 12 Hours, and Last 24 Hours

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2599

Outgoing List: Displays a list of entities having outgoing communication from this VM. Each line represents an outgoing communication and includes the following fields.

Table 28: Field Description - Outgoing List

Field	Description	Values
Destination Entity Name	Displays the name of the entity this VM is communicating to. If the entity is not identified by Prism Central (through registered PE or through vCenter using monitoring configurations feature), the name is displayed as unknown.	(entity name), Unknown
Destination IP Address	Displays the IP Address of the entity this VM is communicating to.	(IP address)
Destination Port	Displays the port on which this VM is communicating with the destination entity.	(port number)
Source IP Address	Displays the IP Address of the VM.	(IP address)
Source App Identification Status	Indicates whether the communicating application is an identified application type. An identified application is one that is a known type.	Identified, Unidentified

You can filter this list by opening the Filter pane to select a filter option. The following table describes the filter options for **Outgoing List**. You can apply filters with multiple fields. The filters fetch the latest discovery and communication data and accordingly display the result set, to the maximum of 20 results.

The following table describes the filter options for **Outgoing List**:

Table 29: Filter Pane - Outgoing List

Fields	Description	Values
Destination Entity Name	Filters based on the destination entity name. Select a condition from the dropdown menu (**Contains**, **Equal to**, **Not equal to**, **Doesn't contain**, **Starts with**, **Ends with**) and enter a string in the field.	(destination entity name string)
Entity Type	Filters based on the entity type. A VM belongs to a cluster managed by Prism Central or vCenter (only if using monitoring configurations feature). An Unknown entity is one that is not identified by Prism Central.	VM, Unknown
Destination IP Address	Filters based on the destination IP address. (same options as Destination Entity Name).	(destination IP address string)
TCP Port	Filters based on the TCP port number.	(TCP port number)
UDP Port	Filters based on the UDP port number.	(UDP port number)
Source IP Address	Filters based on the source IP address (same options as Destination Entity Name).	(source IP address string)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2600

Fields	Description	Values
Time Range	Filters based on the time range.	Last 30 Mins, Last 1 Hour, Last 12 Hours, and Last 24 Hours

Creating a VM through Prism Central (AHV)

You can create virtual machines (VMs) in Acropolis-managed clusters through Prism Central.

About this task

Note:

- For instructions about how to install Nutanix VirtIO on Windows VMs, see Windows VM Provisioning in the *AHV Administration Guide*.
- If you are logged in as the self-service administrator or a project member, see Creating a VM (Self Service) on page 532.

To create a VM in an AHV cluster, perform the following steps:

Procedure

To create a VM in AHV cluster, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and go to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment. For information about how to access the list of non-nutanix VMs managed by an external *vCenter*, see VMs Summary View on page 104.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2601

3. Click **Create VM**, and enter the following information in the **Configuration** step:

   a. **Name**: Enter a name for the VM.

   b. **Description** (optional): Enter a description for the VM.

   c. **Cluster**: Select the target cluster from the dropdown menu on which you intend to create the VM.

   d. **Number of VMs**: Enter the number of VMs you intend to create. The created VM names are suffixed sequentially.

   e. **vCPU(s)**: Enter the number of virtual CPUs to allocate to this VM.

   f. **Number of Cores per vCPU**: Enter the number of cores assigned to each virtual CPU.

   g. **Memory**: Enter the amount of memory (in GiBs) to allocate to this VM.

   h. **Enable Memory Overcommit**: Select this checkbox to enable memory overcommit for the VM.

      Before you turn memory overcommit on or off, see Memory Overcommit in the *AHV Administration Guide*. For more information on configuring memory overcommit, see Memory Overcommit Management on page 196.

      > **Note:** Ensure that the status of the **Memory Overcommit** property under **Configuration** in the **Review** tab is set as **Enabled**.

   i. **Enable Advanced Processor Compatibility**: Select this checkbox to enable advanced processor compatibility for the VM.

      After you select the **Enable Advanced Processor Compatibility** checkbox, the system provides you the option to select the required CPU generation.

      Select the required CPU generation name in the **Select CPU generation** dropdown menu.

      For more information, see Advanced Processor Compatibility in AHV section in the *AHV Administration Guide*.

      > **Note:** Advanced processor compatibility setting for VMs with automatic cluster selection configuration is not supported. For more information on automatic cluster selection, see Automatic Cluster Selection for VM Placement section in the *AHV Administration Guide*.

      The following is an example showing the **Configuration** step:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2602

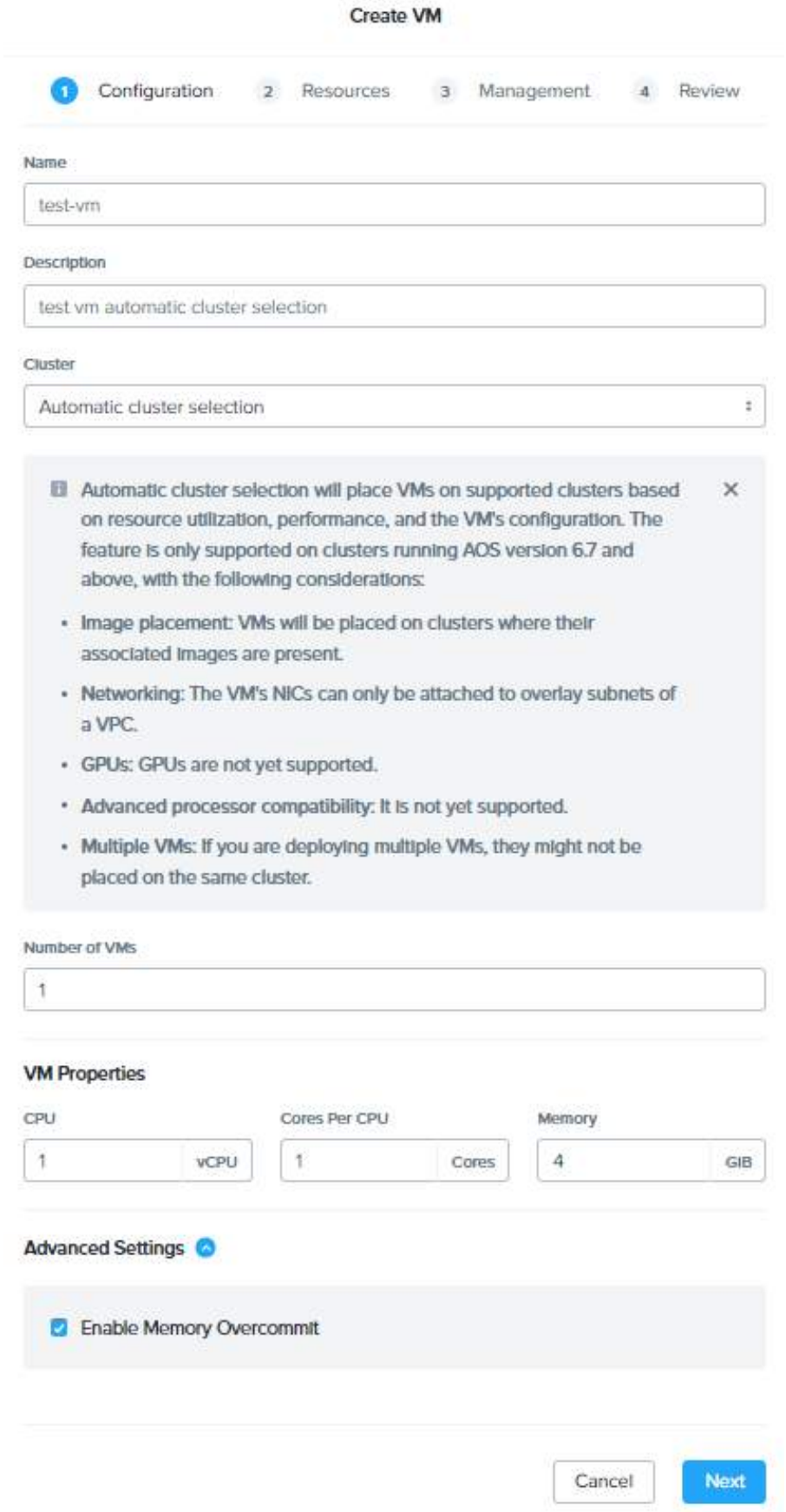


Figure 44: Create VM - Configuration

The following is an example showing the **Configuration** step:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2604

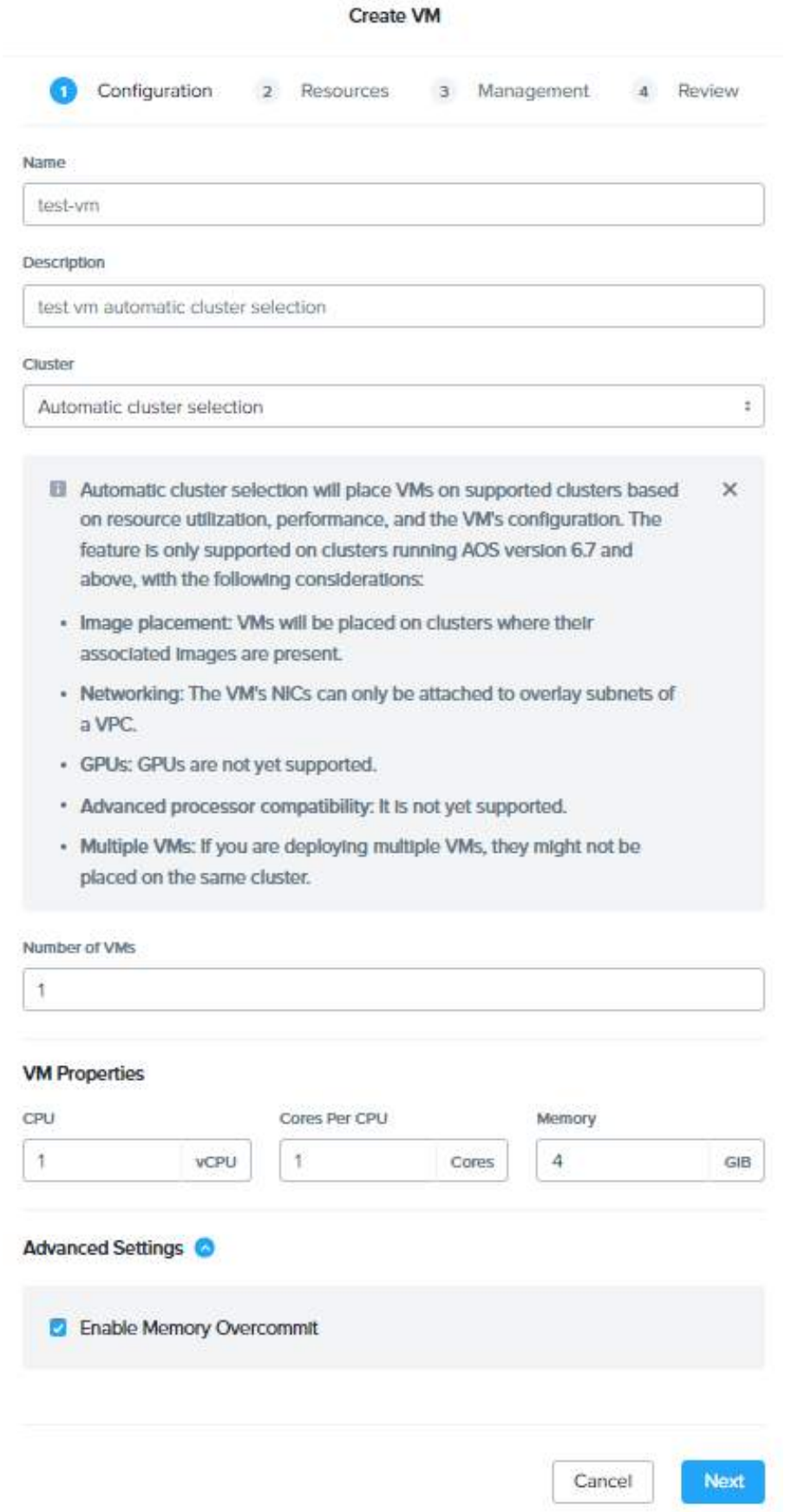


Figure 45: Create VM - Configuration

4. In the **Resources** step, perform the following actions to attach a Disk to the VM:

   Disks: Click **Attach Disk**, and enter the following information:

   a. **Type**: Select the type of storage device, **Disk** or **CD-ROM**, from the dropdown menu.

   b. **Operation**: Specify the device contents from the dropdown menu.

   - Select **Empty CD-ROM** to create a blank CD-ROM device. A CD-ROM device is needed when you intend to provide a system image from CD-ROM.

     Note: The **Empty CD-ROM** option is available only when *CD-ROM* is selected as the storage device in the **Type** field.

   - Select **Allocate on Storage Container** to allocate space without specifying an image. Selecting this option means you are allocating space only. You have to provide a system image later from a CD-ROM or another source.

     Note: The **Allocate on Storage Container** option is available only when *Disk* is selected as the storage device in the **Type** field.

   - Select **Clone from Image** to copy an image that you have imported by using the image service feature onto the disk.

   c. If you select:

   - **Allocate Storage Container** in the **Operation** field, the system prompts you to specify the **Storage Container**.

     Note: If the VM is assigned to a category associated with a storage policy, then the storage container that you select might not govern the storage properties of the VM. The storage properties that the storage policy provides override the storage properties that the storage container provides.

   - **Clone from Image** in the **Operation** field, the system prompts you to specify the **Image**.

   d. Enter either of the following information based on your selection in the **Operation** field:

   - **Storage Container**: Select the appropriate storage container.
   - **Image**: Select the image you created using the image service feature. For information about Image management, see Image Management on page 242.

     Note: The image transfer can trigger image bandwidth throttling if a bandwidth throttling policy is associated with the image. For more information, see Bandwidth Throttling Policies on page 496.

   e. **Bus Type**: Select the bus type from the dropdown menu.

   The options displayed in the dropdown menu vary based on the storage device **Type** selected in the **Type** field.

   If the storage device **Type** is:

   - **Disk**: The available choices are **SCSI**, **SATA**, **PCI**, or **SATA**.
   - **CD-ROM**: The available choices are **IDE**, or **SATA**

   f. **Capacity**: Enter the disk size in GiB.

   g. When all the field entries are correct, click **Save** to attach the disk to the VM and return to the **Create VM** window.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2606

Repeat this step to attach additional devices to the VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2607

5. In the **Resources** tab, perform the following actions to create a network interface for the VM:

   Networks: Click **Attach to Subnet**. The **Attach to Subnet** window appears.

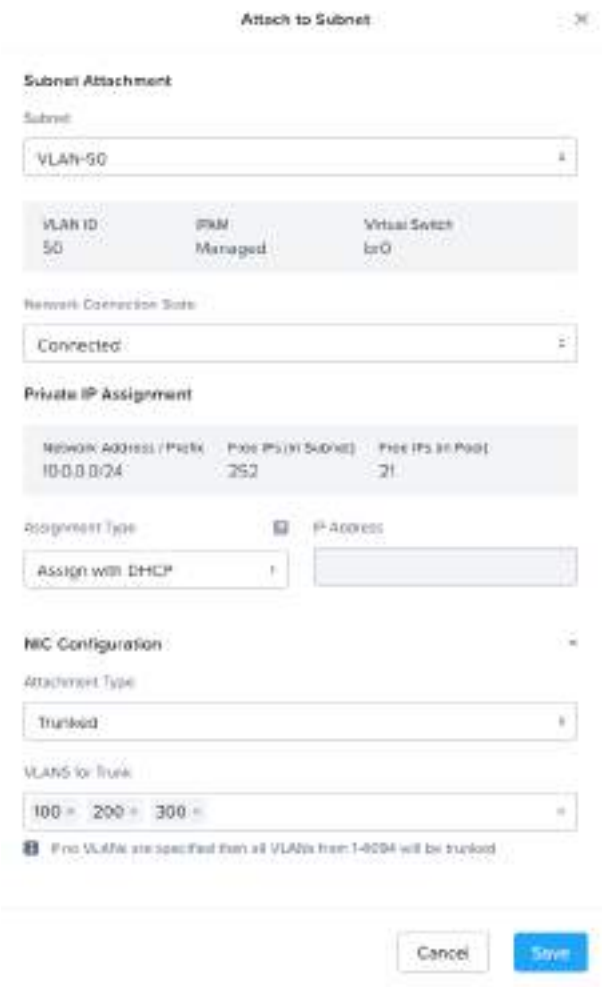


Figure 46: Attach to Subnet Window

   a. **Subnet**: Select the target subnet from the dropdown menu.
      The list includes all the defined networks. For more information on how to perform the network configuration, see Creating VLAN Connections on page 347.

   b. **VLAN ID**: This is a read-only field that displays the VLAN ID.

   c. **IPAM**: This is a read-only field that informs you if the subnet is IPAM managed or not.

   d. **Virtual Switch**: This is a read-only field that displays the name of the virtual switch associated with the subnet.

   e. **Network Connection State**: Select the state for the network after VM creation:

      - *Connected*: If the VM needs to be connected to the network to operate.
      - *Disconnected*: If the VM needs to be in disconnected state after creation.

   f. **Network Address/Prefix**: This is a read-only field that displays the network IP address and prefix.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2608

g. **Free IPs (in Subnet)**: This is a read-only field that displays the free IP addresses in the selected subnet.

h. **Free IPs (in Pool)**: This is a read-only field that displays the free IP addresses in the network IP pool.

i. **Assignment Type**: Select the IP assignment type from the dropdown menu. The options are *Assign with DHCP*, *Assign Static IP*, and *No Private IP*.

j. **IP Address**: Enter the static IP address for VLAN.

This field is enabled only if *Assign Static IP* is selected in the **Assignment Type** field.

k. **Attachment Type**: Select the NIC configuration attachment type from the dropdown menu. The options are *Access* and *Trunked*.

If you select *Trunked* attachment type, **VLANS for Trunk** field appears where you can specify the VLANs ID for the trunk.

l. **VLANS for Trunk**: Specify the VLAN ID for the trunk.

If you do not specify the VLAN ID for the trunked attachment type, then all VLANs from 1- 4094 are trunked.

> **Note:** VLANS for Trunk is available only for basic VLANs.

m. Click **Save** to create a network interface for the VM,and return to the **Create VM** window.

Repeat this step to create additional network interfaces for the VM.

6. (Optional) If you want to add Traffic Mirror Destination NICs, click **Add Mirror Destination NIC**.

> **Note:** NIC MAC Address is assigned after the creation of the VM.

You can add additional Traffic Mirror Destination NICs by clicking **Add New NIC**.

7. In the **Resources** step, perform the following actions for boot configuration.

Boot Configuration: Select one of the following firmware to boot the VM.

» **Legacy BIOS Mode**: Used to start the VM with legacy BIOS firmware.

» **UEFI BIOS Mode**: Used to start the VM with UEFI firmware. UEFI firmware supports larger hard drives, faster boot time, and provides more security features. For more information on UEFI firmware, see UEFI Support for VM information in the *AHV Administration Guide*.

If you select **UEFI BIOS Mode** for **Boot Configuration**, the system enables you to define the **Shield VM Security Settings**:

- **Secure Boot**: Select this check box to enable UEFI secure boot policies for your guest VMs. For more information on Secure Boot functionality, see Secure Boot for VMs information in *AHV Administration Guide*.
- **Attach vTPM**: Select this checkbox to enable vTPM. For information about vTPM functionality, see Securing AHV VMs with Virtual Trusted Platform Module (vTPM) information in *Security Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2609

8. In the **Resources** step, perform the following actions to add a GPU:

   GPUs: Click **Add GPU**. The **Add GPU** dialog box appears. Do the following in the indicated fields:

   > **Note:** This step is applicable

   a. only to AHV clusters with GPU-enabled mode: Select the option for the desired mode, either **vGPU** or **Passthrough**.

   b. If you select **vGPU**, perform the following configuration settings:

   - **NVIDIA Virtual GPU License**: Select a license type from the dropdown menu. This action sets (filters the list of) available profiles. Click the Help icon for information about the license types.

     > **Note:**
     >
     > You can add multiple vGPUs to the VM only if you select the license for NVIDIA Virtual GPU software version 10.1 (440.53) or later.
     >
     > Before you add multiple vGPUs to the VM, see Multiple Virtual GPU Support and Restrictions for Multiple vGPU Support in the *AHV Administration Guide*.

   - **vGPU Profile**: Select the option for the desired profile. Click the help links (Virtual Slice column and end of line) for more information on the profiles.

     > **Note:**
     >
     > Multiple vGPUs are supported on the same VM only if you select the highest vGPU profile type. After you add the first vGPU, to add multiple vGPUs, see Adding Multiple vGPUs to the Same VM on page 156

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2610

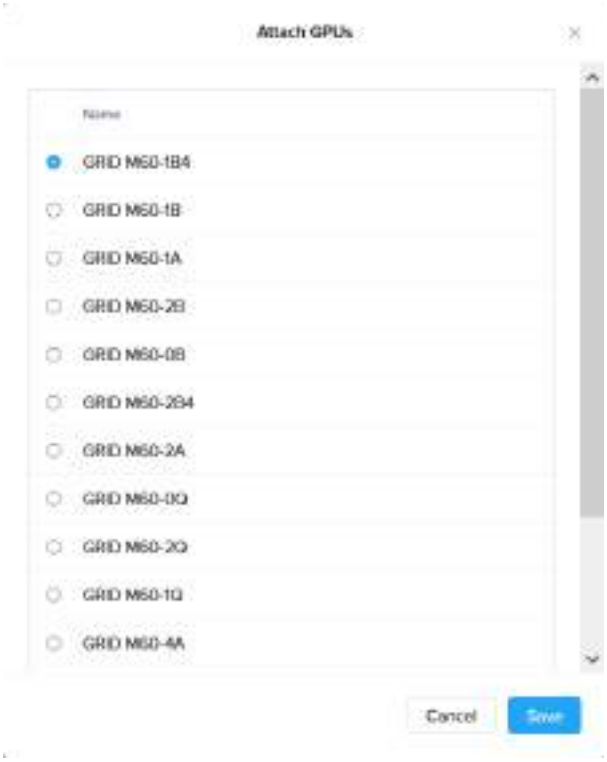


Figure 47: Attach GPUs Window: vGPU

c. If you select **Passthrough**, click the option for the desired type.

Figure 48: Attach GPUs Window: Passthrough

d. Click **Save**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2611

Figure 49: Create VM Window (Resources)

9. In the **Management** step, perform the following actions to define categories and timezone:

   a. Turn on the **Enable 'Default-Storage' policy** switch to apply the default storage policy to the VM that you are creating.

      The **Enable 'Default-Storage' policy** switch is turned off by default.

      For more information on the default storage policy, see Default Storage Policy on page 509.

   b. **Categories**: Search for the category to be assigned to the VM. Select the checkboxes of the categories that you want to assign to the VM.

      If you enabled the **Enable 'Default-Storage' policy** switch for the VM in the previous step, then the **Storage:$Default** is displayed in the **Categories** dropdown menu. To assign more categories to the VM, select the categories from the dropdown menu.

      Note:

      Do not assign any other category that is already associated with another storage policy to the entity, such as a VM or VG, if you want to enable the **Enable 'Default-Storage' policy** switch for that entity. If you enable the **Enable 'Default-Storage' policy** switch for an entity that is already

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2612

associated with another category, the **Storage: $Default** category is enabled, but the storage policy associated with the other category overrides the default storage policy.

c. **Timezone**: Select the local timezone to use from the dropdown menu.

d. **Use this VM as an agent VM**: Select this option to make this VM as an agent VM.

You can use this option for the VMs that must be powered on before the rest of the VMs (for example, to provide network functions before the rest of VMs are powered on the host) and must be powered off and migrated after rest of the VMs (for example, during maintenance mode operations).

Figure 50: Create VM Window (Management)

10. In the **Management** step, perform the following actions for VM customization:

Guest Customization: To customize the VM, select Cloud-init (for Linux VMs) or Sysprep (for Windows VMs).

Script Type: Select the VM script customization type from the dropdown menu. The options are `No Customization`, `Sysprep(Windows)`, or `Cloud-init (Linux)`.

Configuration Method: Select the VM script customization method from the dropdown menu. This field is activated when the **Script Type** is either `Sysprep(Windows)` or `Cloud-init (Linux)`. The options are `Custom Script` or `Guided Script`.

The system displays the options required to configure Cloud-init and Sysprep, such as options to specify a configuration script and options to upload a script

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2613

11. To specify a user data file (Linux VMs) or answer file (Windows VMs) script for unattended provisioning, perform either of the following actions:

    » If the file is available on your local computer, click **Upload Script**, choose and upload the file.

    » Create or paste the contents of the file in the text box below **Upload Script**.

    Note: The script type supports the following file formats.

    - Sysprep: XML
    - Cloud-init (Linux): YAML, JSON, or Shell.

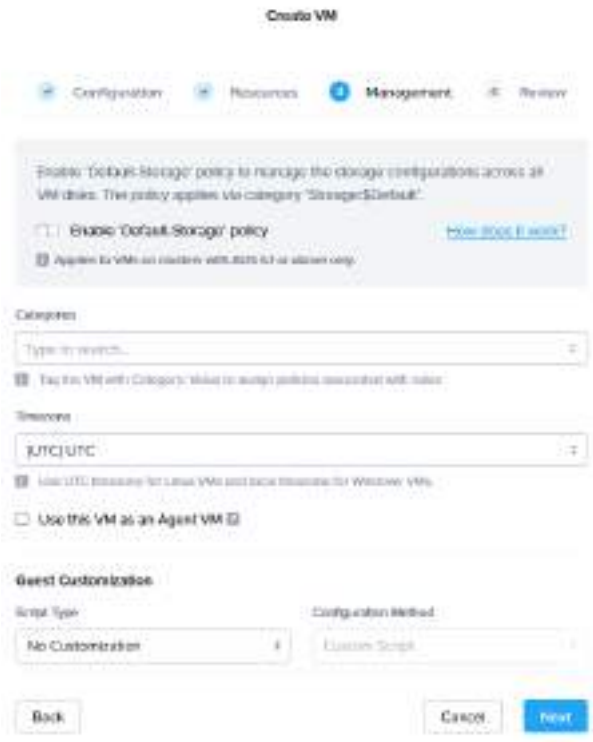


Figure 51: Create VM Window (Management)

12. In the **Review** step, when all the field entries are correct, click **Create VM** to create the VM, and close the **Create VM** window.

    The new VM appears in the VMs **Summary** page and **List** page.

Managing a VM through Prism Central (AHV)

About this task

After you create a VM, you can perform various operations to manage it based on your requirement.

Note:

- You can perform some of the available actions on a single VM at a time, while others can be performed on multiple VMs simultaneously. The available actions appear in bold; the unavailable actions are grayed out. The available actions depend on the current state of the VM and user permissions.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2614

- You can perform only those operations for which you have permissions from the admin.
- Do not install any external software on the Prism Central VM.

To manage a VM, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment. For information about how to access the list of non-nutanix VMs managed by an external *vCenter*, see VMs Summary View on page 104.
3. Select the required action using any of the following methods:
   - Select the target VM checkbox in the **List** tab, and choose the required action from the from the **Actions** dropdown menu.
   - Right-click on the target VM in the **List** tab, and select the required action from the displayed dropdown menu.
   - Select the required action in the **Summary** page of an individual VM. For information about how to access the **Summary** page of an individual VM, see VM Details View on page 117.

The following table provides the information about all the actions that you can perform to manage the VM:

Table 30: VM Actions

Action	Description	Applicable to Multiple VMs
Update	Update the VM configuration. For more information, (see Updating a VM through Prism Central (AHV) on page 147.	No
Delete	Delete the VM.	Yes
Clone	Clone a VM. For more information, see Cloning a VM through Prism Central (AHV) on page 153.	No
Create VM Template	Create a VM template. For more information, see Creating a VM Template on page 201.	No
Launch Console	Launch the VM console. For more information, see Launching a VM Console through Prism Central (AHV) on page 155.	No
Migrate Across Clusters	On-demand migrate the VM across AHV clusters without the need to protect them in synchronous replication schedules or set up Nutanix Disaster Recovery from the Prism Central web console. For more information about on-demand VM migration, see On-Demand Cross-Cluster Live Migration on page 164.	Yes
Power On	Power on the VM.	Yes
Power Off	Power off the VM.	Yes

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2615

Action	Description	Applicable to Multiple VMs
Power Cycle	power off the VM followed by a power on.	Yes
Reset	Perform an ACPI reset action through the BIOS of the VM.	Yes
Guest Shutdown	Perform a graceful shutdown of the operating system of the VM.	Yes
Guest Reboot	Perform a graceful restart of the operating system of the VM.	Yes
Pause/Suspend	Pause or suspend the VM. This option is available only when the VM is powered on.	Yes
Resume	Resume a paused or suspended VM.	No
Disable Efficiency Measurement	Disable machine-learning capability of efficiency measurement for the VM. You can also create a category of VMs and assign the category in **Inefficiency Measurement Exclusion** policy to control this function through operations policies. For more information, see Operations Policy Management in *Intelligent Operations Guide*. **Note:** By default, the efficiency measurement function is enabled for all VMs.	Yes
Enable Efficiency Measurement	Enable machine-learning capability of efficiency measurement. **Note:** If the VM is part of the VM category that is mapped to the **Inefficiency Measurement Exclusion** operations policy, the policy takes precedence and the system does not allow you to enable efficiency measurement. For information about how to assign or remove the VM category in **Inefficiency Measurement Exclusion** policy, see Managing Operations Policies in *Intelligent Operations Guide*. You cannot enable efficiency measurement on individual VMs if the efficiency measurement is disabled on the cluster level.	Yes
Disable Anomaly Detection	Disable machine-learning capability of Anomaly Detection for the VM. You can also create a category of VMs and assign the category in **Anomaly Detection Exclusion** policy to control this function through operations policies. For more information, see Operations Policy Management in *Intelligent Operations Guide*. **Note:** By default, the anomaly detection function is enabled for all VMs.	Yes
Enable Anomaly Detection	Enable machine-learning capability of anomaly detection. **Note:** If the VM is part of the VM category that is mapped to the **Anomaly Detection Exclusion** operations policy, the policy takes precedence and the system does not allow you to enable anomaly detection. For information about how to assign or remove the VM category in **Anomaly Detection Exclusion** policy, see Managing Operations Policies in *Intelligent Operations Guide*.	Yes

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2616

Action	Description	Applicable to Multiple VMs
Protect	Assign the VM to a protection policy. Selecting **Protect** opens a window to specify the protection policy to which this VM should be assigned. You can create a protection policy for a VM or set of VMs that belong to one or more categories by enabling Nutanix Disaster Recovery and configuring the Availability Zone.	Yes
Unprotect	Remove the VM from a protection policy.	Yes
Create Recovery Point	Create VM recovery point. The VM can be restored or replicated from a recovery point either locally or remotely in a state of a chosen recovery point. In the **Create VM Recovery Point** window, enter a name for the VM recovery point. You can choose to create an app consistent VM recovery point by enabling the **App Consistent** checkbox. For more information about app consistent recovery point, see Terminology section in the *Data Protection and Recovery with Prism Element* guide.	No
Migrate	Migrate the VM within the cluster to another host or outside the cluster. In the **Migrate VM** window, choose any of the following options: • **Migrate Within Cluster** to select the target host from the dropdown menu (or select the System will automatically select a host option to let the system choose the host). • **Migrate Outside Cluster (Protected VMs)** to live migrate the VM protected with synchronous replication outside the cluster. **Note:** This option is disabled if the VM is not protected with synchronous replication schedule or VM synchronization is not completed at the recovery AZ. **Note:** Nutanix recommends to live migrate VMs when they are under light load. If they are migrated while heavily utilized, migration may fail because of limited bandwidth. For more information about VM migration, see VM Migration Specifications on page 157.	No
Add to Recovery Plan	Add the VM to a recovery plan you created previously. For more information, see the Adding Guest VMs Individually to a Recovery Plan section in the *Nutanix Disaster Recovery Guide*.	Yes
Run Playbook	Run a playbook you created previously. For more information, see Running a Playbook (Manual Trigger) in *Intelligent Operations Guide*.	Yes
Manage Categories	Assign the VM a category value. For more information, see Assigning a Category on page 460.	Yes
Install NGT	Install Nutanix Guest Tools (NGT). For more information, see Installing NGT on page 176.	Yes

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2617

Action	Description	Applicable to Multiple VMs
Manage NGT Applications	Enable or disable NGT. For more information, see Managing NGT Applications on page 180.	Yes
Upgrade NGT	Upgrade NGT. For more information, see Upgrading NGT on page 180.	Yes
Configure VM Host Affinity	This option is disabled and cannot be used to define VM-Host affinity in Prism Central. The VM-Host affinity policies can be created using VM categories and host categories. For more information about affinity policies Prism Central, see VM-Host Affinity Policies Defined in Prism Central on page 463. For information about how to create an affinity policy, see Creating a VM-Host Affinity Policy on page 471. It is recommended to create an affinity to multiple hosts (at least two) to protect against downtime due to a node failure.	No
Add to Catalog	Add the VM to the catalog. For more information, see Adding a Catalog Item on page 268.	No
Manage Ownership	Specify a project and user who owns the VM. In the **Manage VM Ownership** window, select the target project from the dropdown menu and enter a user name as owner of the VM.	No
Set QoS Attributes	Configure quality of service (QoS) settings. For more information, see Setting QoS for an Individual VM on page 195.	Yes
Export as OVA	Export the VM as OVA. For more information, see OVA Management on page 219 and Uploading an OVA on page 223.	No

4. Check the status of the selected action under tasks widget.

Updating a VM through Prism Central (AHV)

You can use Prism Central to update the VM configuration.

About this task

To update a VM, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default with all the VMs across registered clusters in the **Nutanix** environment. For information about how to access the list of non-Nutanix VMs managed by an external *vCenter*, see VMs Summary View on page 104.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2618

3. Select the **Update** action using any of the following methods:

   - Select the target VM checkbox in the **List** tab, and choose **Update** from the from the **Actions** dropdown menu.
   - Right-click on the target VM in the **List** tab, and select **Update** from the displayed dropdown menu.
   - Click **Update** in the **Summary** page of an individual VM. For information about how to access the **Summary** page of an individual VM, see VM Details View on page 117.

   The **Update VM** window appears, which includes the same fields as the **Create VM** window. For information about how to create a VM, see Creating a VM through Prism Central (AHV) on page 130.

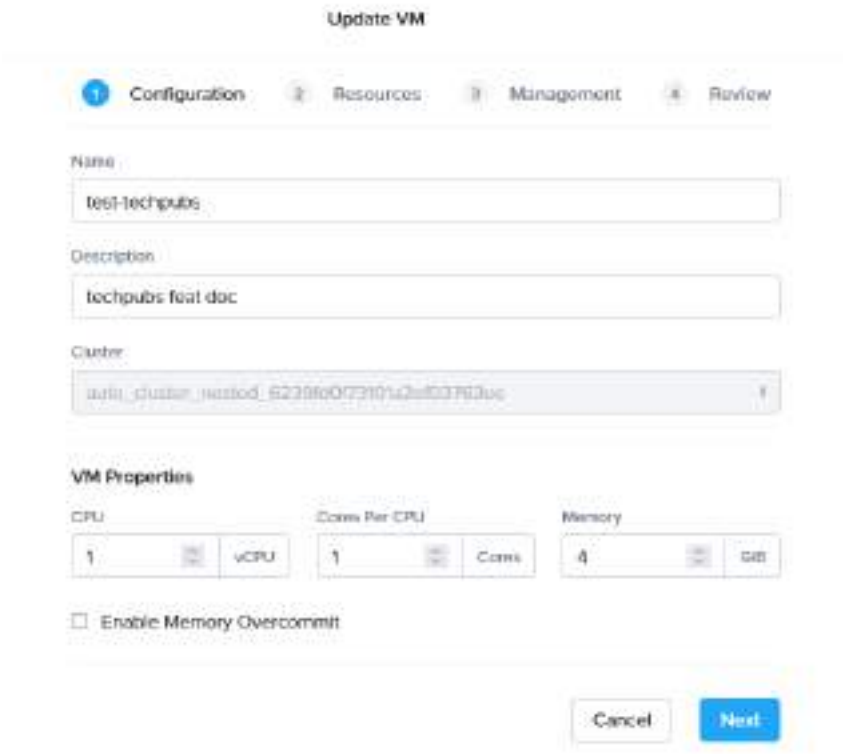


Figure 52: Update VM Window (Configuration)

Modify the VM configuration based on your requirement as indicated in the following steps, and click **Save** in the **Review** step:

4. **Enable Memory Overcommit**: Select this checkbox to enable memory overcommit for the VM.

   Before you turn memory overcommit on or off, see Memory Overcommit in the *AHV Administration Guide*. For more information on configuring memory overcommit, see Memory Overcommit Management on page 196.

   > **Note:** Verify that the status of the **Memory Overcommit** property under **Configuration** in the **Review** tab is set as **Enabled**.

5. **Disks**:

   - You can add new disks to the VM using the **Attach Disk** option. You can also modify the existing disk attached to the VM using the controls under the actions column. See Creating a VM through Prism Central

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2619

(AHV) on page 130 before you modify the disk or create a new disk for a VM. You can turn the flash mode settings for the VM and VM disks on or off.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2620

- You can change the storage container of the disk from the **Storage Container** field:

> **Note:** Starting with Prism Central 2023.4, the individual VM disks can be migrated using Prism Central UI. If more granular control is required, perform the steps through acli as described in Migrating a vDisk to Another Container section in *AHV Administration Guide*.

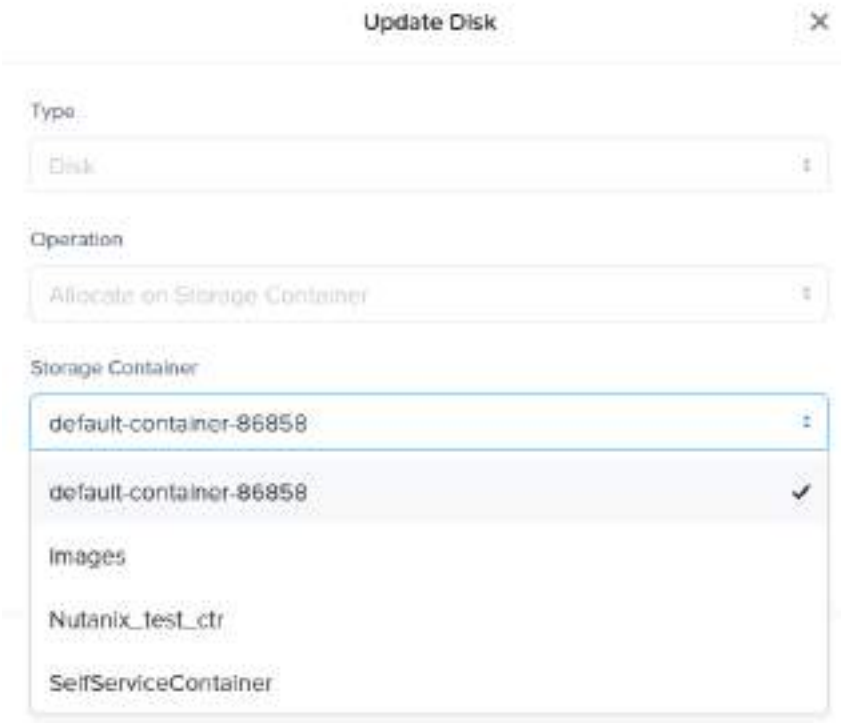


Figure 53: Storage Container Update

a. To enable flash mode on the VM, click the **Enable Flash Mode** checkbox.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2621

Figure 54: Update VM Window (Resources)

» After you enable this feature on the VM, the status is updated in the VM table view. To view the status of individual virtual disks (disks that are flashed to the SSD), click the update disk icon in the **Disks** pane in the **Update VM** window.

» You can turn off the flash mode feature for individual virtual disks. To update the flash mode for individual virtual disks, click the update disk icon in the **Disks** pane and deselect the **Enable Flash Mode** check box.

Figure 55: Update Disk Window (VM Disk Flash Mode)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2622

Note: The flash mode setting is not supported for **CD-ROM** storage devices.

Figure 56: Update VM Window (Resources)

6. **Networks:** You can attach a new network to the VM using the **Attach to Subnet** option. You can use the **Add Mirror Destination NIC** option to use the VM as a Traffic Mirror destination. You can also modify the existing subnet and Traffic Mirror destination NICs attached to the VM. Before you modify the NIC network or create a new NIC for a VM, see Creating a VM through Prism Central (AHV) on page 130 and Limitation for VNIC Hot-Unplugging information in the *AHV Administration Guide*.

7. **Boot Configuration:** You cannot modify the BIOS mode after the VM is created. However, if you have enabled the Secure Boot option under UEFI Mode while creating the VM, you can modify this setting during the VM update.

8. **GPUs:** (For GPU-enabled AHV clusters only) You can add pass-through GPUs if a VM is already using GPU pass-through. You can also change the GPU configuration from pass-through to vGPU or vGPU to pass-through, change the vGPU profile, add more vGPUs, and change the specified vGPU license.

   Note:

   - You must shut down the VM before you perform GPU configuration-related operations.
   - Before you add multiple vGPUs to the VM, see Multiple Virtual GPU Support and Restrictions for Multiple vGPU Support information in the *AHV Administration Guide*.
   - Multiple vGPUs are supported on the same VM only if you select the highest vGPU profile type.
   - After you add the first vGPU, to add multiple vGPUs, see Adding Multiple vGPUs to the Same VM on page 156.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2623

9. Turn on or off the **Enable 'Default-Storage' policy** switch to turn on or off the default storage policy for the VM. The switch is turned off by default.

   The default storage policy uses the **Storage:$Default** category. When you turn on the **Enable 'Default-Storage' policy** switch, the VM is associated with the **Storage:$Default** category.

   For more information on the default storage policy, see Default Storage Policy on page 509.

Cloning a VM through Prism Central (AHV)

You can use Prism Central to clone a VM.

About this task

To clone a VM, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment. For information about how to access the list of non-nutanix VMs managed by an external *vCenter*, see VMs Summary View on page 104.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2624

3. Perform the **Clone** action using any of the following methods:

   - Select the target VM checkbox in the **List** tab, and choose **Clone** from the from the **Actions** dropdown menu.
   - Right-click on the target VM in the **List** tab, and select **Clone** from the displayed dropdown menu.
   - Click **Clone** in the **Summary** page of an individual VM. For information about how to access the **Summary** page of an individual VM, see VM Details View on page 117.

   The **Clone VM** window appears, which includes the same fields as the **Create VM** window. For information about how to create a VM, see Creating a VM through Prism Central (AHV) on page 130.

   A cloned VM inherits most the configurations (except the name) of the source VM.

   Note:

   - You can clone up to 250 VMs at a time.
   - You cannot override the secure boot setting while cloning a VM, unless the source VM already had secure boot setting enabled.

   The following is an example showing the **Clone VM** window:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2625

Figure 57: Clone VM Window

4. Enter a name for the clone, and click **Save**.

   You can optionally override some of the configurations before you click **Save**. For example, you can override the number of vCPUs, memory size, boot priority, NICs, or the guest customization.

   The VM clone is created successfully.

Launching a VM Console through Prism Central (AHV)

You can use Prism Central to launch a VM console.

Procedure

1. Log in to Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2626

2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment. For information about how to access the list of non-nutanix VMs managed by an external *vCenter*, see VMs Summary View on page 104.

3. Select the **Launch Console** action using any of the following methods:

   - Select the target VM checkbox in the **List** tab, and choose **Launch Console** from the from the **Actions** dropdown menu.
   - Right-click on the target VM in the **List** tab, and select **Launch Console** from the displayed dropdown menu.
   - Click **Launch Console** in the **Summary** page of an individual VM. For information about how to access the **Summary** page of an individual VM, see VM Details View on page 117.

   This opens a Virtual Network Computing (VNC) client and displays the console in a new tab or window. This option is available only when the VM is powered on. The VM power options that you access from the **Power On Actions** (or **Power Off Actions**) action link below the VM table can also be accessed from the VNC console window. To access the VM power options, click Power icon at the top-right corner of the console window.

Figure 58: Console Window (VNC)

Note:

- A VNC client may not function properly on all browsers. Some keys are not recognized when the browser is Chrome. It is observed that the VNC client works better on Firefox browser.
- To enable or disable the console support for a VM with one vGPU configured, see Enabling or Disabling Console Support for vGPU VMs.

Adding Multiple vGPUs to the Same VM

About this task

You can add multiple vGPUs of the same vGPU type when you create a new VM or update an existing VM.

- For information on how to create a VM, see Creating a VM through Prism Central (AHV).
- For information on how to update an existing VM, see Updating a VM through Prism Central (AHV).

For more information on multiple vGPU support, see Multiple Virtual GPU Support.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2627

Before you begin

Ensure that the following prerequisites are met before you add multiple vGPUs to the VM:

- Select the license for NVIDIA Virtual GPU (vGPU) software version 10.1 (440.53) or later.
- Observe the guidelines and restrictions specified in Multiple Virtual GPU Support and Restrictions for Multiple vGPU Support.

Procedure

To add multiple vGPUs to the same VM, perform the following steps:

1. Click **Add GPU** in the **Resources** step of create VM workflow or update VM workflow. For more information, see Creating a VM through Prism Central (AHV) or Updating a VM through Prism Central (AHV)
2. In the **Add GPU** window, click **Add**.

   The License field is grayed out and you cannot select a different license when you add a vGPU for the same VM.

   The **VGPU Profile** is auto-selected. The system allows you to select additional vGPU of the same vGPU type as indicated by the message at the top of the **Add GPU** window.

   The newly added vGPU appears in the **Create VM** or **Update VM** window.
3. Repeat the steps for each vGPU addition to the VM.

VM Migration Specifications

VM migration can be performed in the following ways:

- *Live Migration* – This method is used to transfer the VM from one physical host to another host without affecting the normal functions and operations of the VM, and with minimal and often no interruption to the users of the VM.

  Live migration is supported for the following scenarios:

  - Intra-cluster live migration of guest VMs from one host to another host. For more information, see Migrating Within the Cluster in the *Prism Central Infrastructure Guide*.
  - Cross-cluster live migration (CCLM) of guest VMs protected with synchronous replication schedules. For more information, see Cross-Cluster Live Migration in the *Nutanix Disaster Recovery Guide*.
  - On-demand cross-cluster live migration of guest VMs across AHV clusters registered to the same or different Prism Central AZs. For more information, see On-Demand Cross-Cluster Live Migration on page 164.
- *Cold Migration* - This method is used to transfer the VM from one physical host to another host with minimal VM downtime. You can use **Nutanix Move** for Inter-cluster VM migration <Third-Party Hypervisor> to the AHV cluster. For more information, see Move User Guide.

  Note: The <Third-party hypervisors> are Xen (Amazon EC2), Microsoft Hyper-V, and VMware ESXi.

Live Migration Cases

VM live migration is applicable for the following cases:

- Maintenance activity required on the cluster - This scenario is applicable for a planned event (for example, scheduled maintenance of guest VMs) at the primary AZ when you put node into maintenance mode. For information on how to configure a planned failover, see Cross-Cluster Live Migration section in *Nutanix Disaster Recovery Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2628

- AHV or Firmware Upgrades - When you upgrade the AHV or Firmware, the VMs need to be live migrated to another AHV cluster.
- Load balancing or to isolate specific VMs on hosts.
- Changes in Host affinity policy.
- Acropolis Dynamic Scheduling (ADS)- If ADS detects a resource contention in the cluster, it creates a migration plan to eliminate the hotspots in the cluster by migrating VMs from one host to another. For more information about ADS, see Acropolis Dynamic Scheduling in AHV section in *AHV Administration Guide*.
- Defragmentation activity to create resources for VM power-on operation. This activity is performed when the cluster can accommodate resources for VM power-on operation after moving some VMs to another host.

Live Migration Restrictions

This section provides the list of factors that affect VM live migration.

The following conditions affect VM live migration;

- VM is powered off.
- VM is configured as an agent VM.

  You can select or clear the **Use this VM as an agent VM** checkbox to enable or disable this function when you create or update a VM. For more information, see the Creating a VM through Prism Central (AHV).
- For guest VMs with Windows Credential Guard enabled, the VM live migration is only supported between the nodes with Skylake or newer Intel CPU generations. While expanding the cluster, if you add a node with CPU generation prior to Skylake, the system generates an alert *VMs became non-migratable due to node addition* after cluster expansion. Nutanix recommends that you remove the nodes with older CPU generation, power-off, then power-on affected guest VMs to re-enable VM live migration support. For more information, see KB-15227.

  For information about Windows Credential Guard, see the Windows Defender Credential Guard Support section in the *AHV Administration Guide*.
- For guest VMs with WSL2 enabled, VM live migration is only supported between the nodes with Skylake or newer Intel CPU generations. While expanding the cluster, if you add a node with CPU generation prior to Skylake, the system generates an alert *VMs became non-migratable due to node addition* after cluster expansion. Nutanix recommends that you remove the nodes with older CPU generation, power-off, then power-on affected guest VMs to re-enable VM live migration support. For more information, see KB-15227.

  For information about WSL2, see the Windows Subsystem for Linux (WSL2) Support on AHV section in the *AHV Administration Guide*.
- GPU passthrough is enabled.

  For information on how to verify if GPU passthrough is enabled for the VM, see Checking Live Migration Status of a VM on page 159.
- CPU passthrough is enabled.
- VM-Host affinity is set from the Prism Element web console with one host.

  For information on how to verify the VM-Host affinity policy from the Prism Element web console, see Verifying Affinity Policy Association on page 160.
- VM affinity policies are defined from Prism Central using VM categories and host categories.

  For information on how to verify the affinity policies mapped to a VM from Prism Central, see Checking Affinity Policies of a VM From Prism Central on page 161.
- Defragmentation activity to create resources for VM-power-on is in progress.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2629

Note:

- Starting with AOS 6.8 release, AHV supports the live migration of the guest VMs that have Windows Credential Guard enabled. When you upgrade to AOS 6.8 or later release and enable HA reservation for the cluster, the system reserves the resources to accommodate the HA event. However, if you have the existing VMs in the cluster that have Windows Credential Guard enabled, some guest VMs (both with or without Windows Credential Guard enabled) might fail to start due to the unavailability of sufficient resources in the cluster. Ensure that you have sufficient resources available in the cluster to accommodate the HA reservation.

  For more information on Windows Credential Guard, see the Windows Defender Credential Guard Support in AHV section in the *AHV Administration Guide*.

  For more information on how to enable HA reservation, see the Enabling High Availability for the Cluster section in the *Prism Element Web Console Guide*.

- Starting from AOS 7.0 release, with a minimum required AHV version of 10.0, AHV supports the live migration of the guest VMs that have WSL2 enabled. When you upgrade to AOS 7.0 or later release and enable HA reservation for the cluster, the system reserves the resources to accommodate the HA event. However, if you have the existing VMs in the cluster that have WSL2 enabled, some guest VMs (both with or without WSL2 enabled) might fail to start due to the unavailability of sufficient resources in the cluster. Ensure that you have sufficient resources available in the cluster to accommodate the HA reservation.

  For more information on WSL2, see Windows Subsystem for Linux (WSL2) Support on AHV in the *AHV Administration Guide*.

  For information on how to enable HA reservation, see Enabling High Availability for the Cluster section in the *Prism Element Web Console Guide*.

Checking Live Migration Status of a VM

This section describes how to check whether the live migration is allowed for the VM.

Procedure

To check if a VM can be live migrated, perform the following steps:

1. Log on to the CVM as a nutanix user using SSH.
2. Run the following command:

   ```
   nutanix@cvm$ acli vm.get <VM_NAME> | grep 'allow_live_migrate
   ```

   Replace `<VM_NAME>` with the actual VM name at your site.

   The following attribute value confirms the live migration is allowed:

   ```
   allow_live_migrate: True
   ```

What to do next

If `allow_live_migrate: False` is returned for the above command, then check the status of the VM properties that restricts live migration.

The following table provides the information about the verification procedure to check the status of VM properties:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2630

VM Properties	Verification Procedure

WSL2	Log on to the CVM as a Nutanix user using SSH, and run the following command:
	`nutanix@cvm$ acli vm.get <VM_NAME> | grep 'hardware_virtualization`
	Replace `<VM_NAME>` with the actual VM name at your site.
	The following attribute value confirms WSL2 is enabled:
	`hardware_virtualization: True`

GPU	1. Log in to Prism Central. 2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information on the **Navigation Bar**, see Application-specific Navigation Bar. The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment. 3. Apply the **GPU TYPE** filter from the **Modify Filter** option. The system displays the VMs based on the selected GPU criteria.

Figure 59: GPU TYPE Filter

Verifying Affinity Policy Association

This section describes how to verify the VM-Host affinity from Prism Element web console and affinity policies mapped to the VM from Prism Central.

Procedure

To verify affinity policy association for a VM, perform the following checks:

- Checking VM-Host Affinity From Prism Element on page 160.
- Checking Affinity Policies of a VM From Prism Central on page 161.

Checking VM-Host Affinity From Prism Element

About this task

Using Prism Element, you can define the VM-host affinity policy that controls the placement of a VM. You can use this policy to specify that a selected VM can only run on the members of the affinity host list.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2631

Procedure

To verify the VM-Host affinity, perform the following steps:

1. Log in to Prism element web console.
2. Navigate to **VM** > **Table**, and double-click the target VM name. The system displays the **Update VM** window.
3. Under **VM Host Affinity**, check the hosts specified for the VM.

> **Note:**
>
> VMs with Host affinity policies can only be migrated to the hosts specified in the affinity policy during an HA event. If only one host is specified, the VMs cannot be migrated.

Checking Affinity Policies of a VM From Prism Central

About this task

Using Prism Central, you can define the affinity policy based on VM Categories and Host categories.

Procedure

To verify the affinity policy associated with a VM, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.

   The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment.
3. Click the target VM name.
   The system displays the details view of the target VM.
4. Click the **Categories** tab in the target VM's details view.
   The system displays the Categories and Affinity Policy associated with the VM.

Defining Behaviour for Non-migratable VMs (GPU/CPU/PCI/Host Affinity configured VMs)

About this task

When a host is put in maintenance mode, VMs are moved from that host to other hosts in the cluster. After exiting maintenance mode, those VMs are automatically returned to the original host, eliminating the need to manually move them. However, some VMs cannot be migrated to other hosts. For more information, see Non-Migratable VMs.

When an attempt is made for a host to enter maintenance mode, the VMs with GPU passthrough, CPU passthrough, and PCI passthrough are not migrated to the other hosts in the cluster and therefore may block the attempt to enter maintenance mode.

> **Note:** VMs with host affinity policies are also not migrated to other hosts in the cluster, if any of the following condition is met:
>
> - The hosts that are configured as part of VM-Host affinity policy are not available.
> - The hosts that are part of VM-Host affinity policy does not have the sufficient resources to run the VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2632

To overcome this situation, Nutanix recommends you define either of the following behavior for these non-migratable VMs when host enters the maintenance mode:

- Automatically shutdown these non-migratable VMs.
- Set a block migration indication for these non-migratable VM.

Procedure

To define the above behaviors for non-migratable VMs, perform the following steps:

1. Log on to CVM with SSH.
2. Run the following command to put the host into maintenance mode with default action set for non-migratable VMs:

   ```
   nutanix@cvm$ acli host.enter_maintenance_mode <Hypervisor-IP-address> [wait="{ true | false }" ]
   [non_migratable_vm_action="{ acpi_shutdown | block }"
   ```

   Replace:

   - `<Hypervisor-IP-address>` - with the actual host name at your site.
   - `wait`: Set the wait parameter to true to wait for the host evacuation attempt to finish.
   - `non_migratable_vm_action`: By default, this parameter is set to *block*, which means the non-migratable VMs are shut down when you put a node into maintenance mode. For more information on non-migratable VMs, see Non-Migratable VMs.

     If you want to automatically shut down such VMs for the duration of the maintenance mode, set this parameter to *acpi_shutdown*.

Migrating Within the Cluster

You can live-migrate a VM to another host within the cluster.

About this task

The **Migrate Within Cluster** option in the **Migrate VM** window allows you to migrate VMs to other hosts within the cluster.

Before you begin

Ensure that you observe the prerequisites as described in Live Migration of vGPU-enabled VMs on page 163 section, and the limitations described under Limitations for Live Migration information in *AHV Administration Guide*.

Procedure

To live migrate the VMs within the cluster, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment. For information about how to access the list of non-nutanix VMs managed by an external *vCenter*, see VMs Summary View on page 104.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2633

3. Select the target VM checkbox in the **List** tab, and choose **Migrate** from the **Actions** dropdown menu.
   The system displays the **Migrate VM** window with **Migrate Within Cluster** option selected as default.

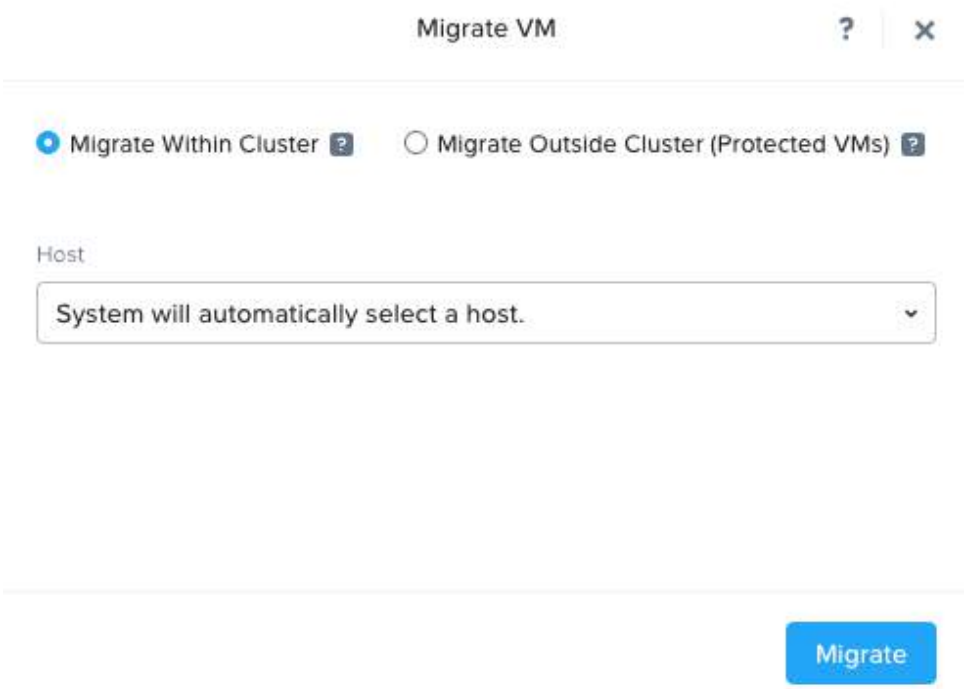


Figure 60: Migrate VM window

4. In the **Host** dropdown menu, perform either of the following actions:

   - Retain the *`System will automatically select a host`* default option if you want to migrate the VM to a host selected by the system.

     The system selects a host based on the GPU resources available with the host as appropriate for the VM to be migrated live.

   - Select the target host from the dropdown menu to which you want to migrate the VM.

5. Click **Migrate**.

   Prism submits the task and displays the following message:

   ```
   Successfully submitted migrate operation.
   Task details
   ```

   Task details is a link to the **Tasks** page. Click the **Task details** link to monitor the migration task in the **Tasks** page.

   The host name of the VM in the **List** view changes to the host name to which you migrated the VM.

Live Migration of vGPU-enabled VMs

You can live-migrate a vGPU-enabled VM to another host within the cluster.

You can perform live migration of VMs enabled with virtual GPUs (vGPU-enabled VMs) only on commercially reasonable effort, if the destination node is equipped to provide enough resources to the vGPU- enabled VMs. However, if the destination node is not equipped with the enough resources, the vGPU-enabled VMs are shut down and you might experience a downtime.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2634

In a successful migration case, the vGPUs can continue to run while the VMs that are running the vGPUs are seamlessly migrated in the background.

When you perform the LCM update, the vGPU-enabled VMs are listed as Non-HA-protected VMs. LCM also migrates the Non-HA-protected VMs on commercially reasonable effort to the destination node if the following requirements are met:

- Destination node is equipped with the required resources for the VM.
- The VM GPU drivers are compatible with the AHV host GPU drivers.

If the destination node is not equipped with the enough resources or there is any compatibility issue between the VM GPU drivers and AHV host GPU drivers, the LCM forcibly shuts down the Non-HA-protected VMs.

Prerequisites

Ensure the following prerequisites are met before you live migrate the vGPU-enabled VMs:

- The VM is not powered off.
- The host affinity is not set for the VM.

  If the host affinity of the VM is set to only one host, you cannot migrate the VM. However, based on the GPU resources required, if the host affinity is set to multiple hosts with the same or similar GPU resources, you can migrate the VM among the hosts with which the affinity is set.
- You have another host in the same cluster that supports the resources necessary to support the vGPU-enabled VM that you want to live migrate.

Limitations

For limitations applicable to live migration of vGPU-enabled VMs, see Limitations for Live Migration in *AHV Administration Guide*.

On-Demand Cross-Cluster Live Migration

On-demand cross-cluster live migration (OD-CCLM) enables you to migrate guest VMs (and all of their associated metadata like VM categories) across AHV clusters registered to the same or different Prism Central instances spanning availability zones (AZs). To ensure zero downtime of the guest VMs, you can live migrate without the need to protect the guest VMs with synchronous replication schedules or set up Nutanix Disaster Recovery from the Prism Central web console.

> **Note:** AHV Metro Availability also provides cross-cluster live migration (CCLM) capability that is based on the Nutanix Disaster Recovery workflows. With AHV Metro CCLM, you can live migrate only the guest VMs protected with synchronous replication schedules. For more information on AHV Metro CCLM, see Cross-Cluster Live Migration in the *Nutanix Disaster Recovery Guide*.

You can live migrate a VM in the following situations:

- In an overlay subnet in a Prism Central AZ to an overlay subnet in another Prism Central AZ
- In an overlay subnet in a virtual private cloud (VPC) in a Prism Central AZ to an overlay subnet in another VPC in the same Prism Central AZ
- Within the same VPC in a Prism Central AZ
- In a VLAN subnet in a Prism Central AZ to a VLAN subnet in another Prism Central AZ
- In a VLAN subnet in a Prism Central AZ to another VLAN subnet in the same Prism Central AZ

A Layer 2 (L2) network extension creates a tunnel between the source and destination subnets so that the VMs in these subnets can communicate with each other. To ensure that dependent VMs on the source cluster and the

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2635

destination cluster can communicate with the migrating VM throughout the live migration process, connect the source and the destination subnets using an L2 network extension before you live migrate a VM in the following scenarios:

- From an overlay subnet in a Prism Central AZ to an overlay subnet in another Prism Central AZ
- From an overlay subnet in a VPC in a Prism Central AZ to an overlay subnet in another VPC in the same Prism Central AZ
- From a VLAN subnet in a Prism Central AZ to a VLAN subnet in another Prism Central AZ
- From a VLAN subnet in a Prism Central AZ to another VLAN subnet in the same Prism Central AZ

> **Note:** An L2 network extension is not required between the source and the destination subnets if you live migrate a guest VM within the same VPC subnet.

For successful live migration, Nutanix recommends that the round-trip latency between the clusters must be 40 ms or less. The data copy time during live migration is dependent on the data to be copied between the clusters and the available network bandwidth.

On-Demand Cross-Cluster Live Migration (OD-CCLM) Requirements

This section describes the requirements for live migrating guest VMs.

Table 31: Nutanix Software Requirements

Nutanix Software	Software Version Required
AOS	• 6.7 or later. While upgrading the AOS version from 6.6 to 6.7, ensure that the upgrade is completed before performing on-demand migration of the guest VM. • For OD-CCLM of vTPM-enabled guest VMs, 6.8 or later. Both the source and destination clusters must be running AOS 6.8 and later.
Prism Central	• pc.2023.3 or later. • For OD-CCLM of vTPM-enabled guest VMs pc.2024.1 or later.

Table 32: Prism Central User Requirements

Prism Central User	Permissions
Administrator	Only the administrator (local admin user account in Prism Central) can perform on-demand live migration between the clusters registered to different Prism Central deployments.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2636

Prism Central User	Permissions
Non-administrator	Non-administrators can perform on-demand live migration only between the clusters registered to the Prism Central deployment. The user must have the following permissions: • View_Prism_Central • View_Virtual_Machine • View_Subnet • View_Availability_Zone • Allow_Cross_Cluster_VM_Migration • View_Cluster For more information on user management, see User Management in *Security Guide*.

- Both the source and the destination subnet must have the same IP network prefix.
- If you did not enable the advanced processor compatibility feature for the guest VM, ensure that the destination Nutanix cluster supports all of the CPU feature sets (set of CPU flags) that are supported on the source Nutanix cluster. Otherwise, live migration fails. For more information, see Advanced Processor Compatibility in AHV Administration Guide.

  Live migration can happen even when the CPU types of the source and destination clusters do not match exactly. The destination cluster must support the superset of the CPU features of the source cluster.
- If the VM in the source cluster has NGT enabled, then the VM must have at least one empty IDE or SATA CD-ROM to attach the ISO required for reconfiguration on the destination cluster.
- Both the source and the destination clusters must run on the same AHV version.
- Both the source and the destination clusters must have the same storage container name for the guest VMs.

  A storage container with the same name as the one on the source cluster must exist on the destination cluster. For example, if a *SelfServiceContainer* storage container exists on the source cluster, the destination cluster must also have a *SelfServiceContainer* storage container.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2637

- If the source and the destination cluster (Prism Element) are in different subnets, open the ports listed on Ports and Protocols for communication.

  > **Tip:** If the source and the destination cluster (Prism Element) are in the same subnet, you do not need to open the ports manually.

  - To open the ports for communication from the source cluster to the destination cluster, run the following command on all CVMs of the source cluster:

    ```
    nutanix@cvm$ allssh 'modify_firewall -f -r remote_cvm_ip,remote_virtual_ip -p
     2030,2036,2073,2090 -i eth0'
    ```

    Replace *remote_cvm_ip* with the IP address of the destination cluster CVM. For multiple CVMs, replace *remote_cvm_ip* with the IP addresses of the CVMs separated by comma.

    Replace *remote_virtual_ip* with the virtual IP address of the destination cluster.

  - To open the ports for communication from the destination cluster to the source cluster, run the following command on all CVMs of the destination cluster:

    ```
    nutanix@cvm$ allssh 'modify_firewall -f -r source_cvm_ip,source_virtual_ip -p
     2030,2036,2073,2090 -i eth0'
    ```

    Replace *source_cvm_ip* with the IP address of the source cluster CVM. For multiple CVMs, replace *source_cvm_ip* with the IP addresses of the CVMs separated by comma.

    Replace *source_virtual_ip* with the virtual IP address of the source cluster.

    > **Note:**
    >
    > - Use the *eth0* interface only. *eth0* is the default CVM interface that shows up when you install AOS.
    > - For Nutanix Disaster Recovery on Network Segmentation enabled Nutanix cluster, use the *ntnx0* interface and run the following command:
    >
    >   ```
    >   nutanix@cvm$ allssh 'modify_firewall -f -r remote_cvm_ip,remote_virtual_ip
    >    -p 2030,2036,2073,2090 -i ntnx0'
    >   ```
    >
    >   Replace *remote_cvm_ip* with the IP address of the cluster CVM where you want to migrate the guest VMs. For multiple CVMs, replace *remote_virtual_ip* with the IP addresses of the CVMs separated by comma.

- The destination cluster must have sufficient storage capacity to host the migrating guest VMs.
- The destination cluster must be reachable from the source cluster.
- IP address management must be manually set up on both the source and the destination cluster.
- The guest VM to be live migrated must be powered on.

  The Prism Central web console filters out the guest VMs that are powered off.

On-Demand Cross-Cluster Live Migration (OD-CCLM) Limitations

Consider the following limitations before performing OD-CCLM of your guest VMs:

- Currently, on-demand live migration of guest VMs is not supported when Windows Defender Credential Guard is enabled.
- On-demand live migration to clusters on Nutanix Cloud AZ (DRaaS) is not supported.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2638

- On-demand live migration to Nutanix Cloud Cluster AZ (NC2) is not supported.
- On-demand live migration of up to 60 guest VMs in parallel is supported.

  While no limit exists to the number of parallel migrations, the time required for successful migration depends on the guest VM size.
- On-demand live migration of guest VMs fails in the following scenarios:
  - Guest VMs are part of Flow Network Security policies.
  - Guest VMs are part of consistency groups.
  - You cannot migrate VMs that have volume groups attached to them.
  - Guest VMs have Replication Factor 1 (RF1).
  - GPU passthrough is enabled on guest VMs.

    For information on GPU passthrough verification, see Checking Live Migration Status of a VM.

    For information on GPU passthrough verification using acropolis CLI (acli), see vm in the Command Reference Guide.
  - Guest VMs are vNUMA VMs.
  - Guest VMs are in a paused state or have NVMe disks attached.
  - Memory overcommit is enabled on guest VMs.
  - Guest VMs are connected to a managed VLAN (IPAM-enabled).
  - Guest VMs are connected to Open Virtual Network (OVN) LAN.
  - Guest VMs are upgraded before on-demand live migration starts.

    When on-demand live migration is in progress, do not perform hotplug upgrades to the memory or CPU. Updates to NIC, disk, memory, and CPU are fatal while data is copied during migration.
  - Prism Central upgrade is in progress.
  - AHV upgrade is in progress.

    Similarly, if on-demand live migration is in progress, upgrading AHV fails.
  - LCM upgrade is in progress.
- After migrating a guest VM in an overlay subnet in a virtual private cloud (VPC) to an overlay subnet in another VPC, Prism Central does not retain the floating IP address of the guest VM if the VPCs are attached to different external subnets. Therefore, you must reassign the floating IP address to the migrated guest VM to access the guest VM from the external network.

  If the VPCs share the same external subnets, Prism Central retains the floating IP address of the guest VM.
- After migration to the recovery cluster, VM categories are not preserved if those categories do not exist on the recovery cluster.
- Data over the wire is not encrypted during the live migration.
- Automatic defragmentation on the recovery cluster is not supported.
- Guest VMs running on ESXi are not supported.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2639

On-Demand Cross-Cluster Live Migration (OD-CCLM) Best Practices

Nutanix recommends the following best practices for live migrating your guest VMs (and all of their associated metadata like VM categories):

- Ensure that you set up the relevant user permissions. For more information, see On-Demand Cross-Cluster Live Migration (OD-CCLM) Requirements on page 165.
- Enable the advanced processor compatibility feature for the guest VM and select the oldest CPU generation to maximize the migration capability of the guest VM. For more information, see Advanced Processor Compatibility in AHV.
- Do not protect the guest VM with a DR protection policy when on-demand live migration is in progress.
- Do not perform Nutanix software upgrades when on-demand live migration is in progress. For more information, see On-Demand Cross-Cluster Live Migration (OD-CCLM) Limitations on page 167.
- Do not perform on-demand live migration when Nutanix software upgrades are in progress. For more information, see On-Demand Cross-Cluster Live Migration (OD-CCLM) Limitations on page 167.
- Do not change the IP addresses or other network configurations of the guest VMs when on-demand live migration is in progress.
- Ensure that a 10G network link is available in the infrastructure setup.
- When an administrator user live migrates the guest VMs created by a non-administrator to a Nutanix cluster registered to a different Prism Central deployment, the administrator user becomes the owner of the guest VM after the VM migration. The ownership remains the same irrespective of who migrated the guest VM when the live migration happens between the Nutanix clusters registered to the same Prism Central deployment.

Performing On-Demand CCLM

If, due to a failure event (for example, scheduled maintenance of guest VMs) at the primary cluster, you must migrate your applications to another AHV cluster without VM downtime, perform an on-demand live migration to the recovery cluster.

Before you begin

See On-Demand Cross-Cluster Live Migration (OD-CCLM) Requirements on page 165, On-Demand Cross-Cluster Live Migration (OD-CCLM) Limitations on page 167, and On-Demand Cross-Cluster Live Migration (OD-CCLM) Best Practices on page 169.

About this task

To live migrate the guest VMs, follow these steps at the primary AZ:

Procedure

1. Log in to the Prism Central web console.
2. From **Application Switcher Function**, select the **Infrastructure** application, and navigate to **Compute** > **VMs** from the **Navigation Bar**.
3. Select the guest VMs to live migrate.

   Warning: To see the guest VM configurations that cannot be migrated, see On-Demand Cross-Cluster Live Migration (OD-CCLM) Limitations on page 167.

4. Click **Migrate Across Clusters** from the **Actions** drop-down menu.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2640

5. Do the following in the **Destination Cluster** tab:
   a. From the dropdown menu, under **Destination Location**, select the AZ to live migrate your guest VMs.
   b. From the dropdown menu, under **Destination Cluster**, select the AHV cluster to live migrate your guest VMs.
   c. Click **Next**.
6. Do the following in the **Network** tab:
   a. From the dropdown menu under **Destination Subnets**, select the network to map the subnet of the migrated guest VMs.
   b. Click **Next**.
7. Do the following in the **Migration Checks** tab:
   a. Review the status of the selected guest VMs after the prechecks run automatically.
      If any precheck fails, resolve the issue that is causing the failure and click **check again**.
   b. When all the **Checks** under the **Selected VMs** show OK, click **Migrate**.

   The selected guest VMs migrate to the recovery cluster with zero VM downtime.

Creating a VM through Prism Central (ESXi)

You can create virtual machines (VMs) in ESXi clusters through Prism Central.

Before you begin

Ensure that the following prerequisites are met before you create a VM in ESXi cluster:

- All the requirements, rules, and guidelines are considered, and the limitations are observed. For more information, see External vCenter Server Integration on page 326 and .
- The vCenter Server is registered with your cluster. For information on how to register a vCenter Server, see Registering External vCenter Server (Prism Central) on page 336.

Procedure

To create a VM in ESXi cluster, perform the following steps:

1. Log in to Prism Central.
2. Select **Infrastructure** application from Application Switcher Function, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information on the **Navigation Bar**, see Application-specific Navigation Bar. The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment. For information on how to access the list of non-nutanix VMs managed by an external *vCenter*, see VMs Summary View on page 104 and .

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2641

3. Click **Create VM**, and enter the following information in the **Configuration** step:

   a. **Name**: Enter a name for the VM.

   b. **Description** (optional): Enter a description for the VM.

   c. **Cluster**: Select the target ESXi cluster from the drop-down list on which you intend to create the VM.

   d. **Number of VMs**: Enter the number of VMs you intend to create. The created VM names are suffixed sequentially.

   e. **vCPU(s)**: Enter the number of virtual CPUs to allocate to this VM.

   f. **Number of Cores per vCPU**: Enter the number of cores assigned to each virtual CPU.

   g. **Memory**: Enter the amount of memory (in GiBs) to allocate to this VM.

4. In the **Resources** step, perform the following actions to attach a Disk to the VM:

   Disks: Click **Attach Disk** , and enter the following information:

   a. **Type**: Select the type of storage device, **Disk** or **CD-ROM**, from the dropdown list.

   b. **Operation**: Specify the device contents from the drop-down list.

      - Select **Empty CD-ROM** to create a blank CD-ROM device. A CD-ROM device is needed when you intend to provide a system image from CD-ROM. The **Empty CD-ROM** option is available only when *CD-ROM* is selected as the storage device in the **Type** field.
      - Select **Allocate on Storage Container** to allocate space without specifying an image. Selecting this option means you are allocating space only. You have to provide a system image later from a CD-ROM or other source. The **Allocate on Storage Container** option is available only when *Disk* is selected as the storage device in the **Type** field.

   c. If you select **Allocate on Storage Container** in the **Operation** field, the system prompts you to specify the **Storage Container**. Select the appropriate storage container.

   d. **Bus Type**: Select the bus type from the drop-down list.

      The options displayed in the drop-down list varies based on the storage device **Type** selected in the **Type** field.

      If the storage device **Type** is:

      - **Disk** - The available choices are **SCSI**, **SATA**, **PCI**, or **SATA**.
      - **CD-ROM** - The available choices are **IDE**, or **SATA**

   e. **Path**: Enter the path to the desired system image.

   f. **Capacity**: Enter the disk size in GiB.

   g. When all the field entries are correct, click **Save** to attach the disk to the VM and return to the **Create VM** window.

   Repeat this step to attach additional devices to the VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2642

5. In the **Resources** step, perform the following actions to create a network interface for the VM:

   Networks: Click **Attach to Subnet**. The **Attach to Subnet** window appears.

   a. **Subnet**: Select the target subnet from the drop-down list.

      The list includes all the defined networks. For information on how to configure the network, see Creating VLAN Connections on page 347.

   b. **Network Adapter Type**: Select the network adapter type from the drop-down list.

      For information on the list of supported adapter types, see External vCenter Server Integration on page 326.

   c. **Network Connection State**: Select the state for the network after VM creation:

      - *Connected* - If the VM needs to be connected to the network to operate.
      - *Disconnected* - If the VM needs to be in disconnected state after creation.

   d. Click **Save** to create a network interface for the VM,and return to the **Create VM** window.

   Repeat this step to create additional network interfaces for the VM.

6. In the **Management** step, perform the following actions to define categories and timezone:

   a. **Categories**: Search for the category to be assigned to the VM. The policies associated with the category value are assigned to the VM.

   b. **Guest OS**: Type and select the guest operating system.

      The guest operating system that you select affects the supported devices and number of virtual CPUs available for the virtual machine. The Create VM wizard does not install the guest operating system. For information on the list of supported operating systems, see External vCenter Server Integration on page 326.

7. In the **Review** step, when all the field entries are correct, click **Create VM** to create the VM, and close the **Create VM** window.

   The new VM appears in the VMs **Summary** page and **List** page.

Managing a VM through Prism Central (ESXi)

This section describes how to manage VMs in an ESXi cluster through Prism Central in **Nutanix** environment.

About this task

The procedure to manage VMs in an ESXi cluster in Nutanix environment is same as for AHV cluster, however the fields can vary when you create or manage a VM in an ESXi cluster. For information on the fields, see Creating a VM through Prism Central (ESXi) on page 170 and .

About this task

To manage a non-nutanix VM on an external *vCenter*, you can use playbooks. For more information, see VMs Summary View on page 104.

> **Note:** Do not install any external software on the Prism Central VM.

Procedure

To manage a VM of an ESXi cluster in **Nutanix** environment:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2643

- For information on how to manage a VM of an ESXi cluster in **Nutanix** environment, see Managing a VM through Prism Central (AHV) on page 143 and .

  You can perform only those operations for which you have permissions from the admin.

Nutanix Guest Tools

Nutanix Guest Tools (NGT) is a software package that comes bundled with AOS. You can install NGT in a guest virtual machine (VM) to enable advanced VM management functionalities provided by Nutanix.

Nutanix Guest Tools Overview

The NGT software package for Linux and Windows includes the following components:

- **NGT Installer**: Allows you to install NGT in a guest VM.
- **Nutanix Guest Agent (NGA) Service**: Maintains a communication channel between the Controller VM (CVM) and the guest VMs.
- **Nutanix VirtIO Package**: Includes the drivers required to run the VM on the AHV hypervisor. For more information about VirtIO drivers, see Nutanix VirtIO for Windows in *AHV Administration Guide*.
- **Python**: The NGA service is written in Python and is shipped with a dedicated installation of Python so it does not interact with the other components in the system.
- **Nutanix VSS package**: Enables Nutanix native in-guest Volume Snapshot Service (VSS) agent to take application-consistent snapshots for all the VMs that support VSS.

In addition, the NGT software package for Windows also includes the following components:

- A custom module that performs checks and fulfills all the prerequisites.
- Microsoft Visual C++ 2015 x64 redistributable component
- Integration with Windows Performance Monitor for hypervisor statistics.

Installing NGT in a guest VM allows you to use the following advanced VM management features:

- **File Level Restore CLI**

  Performs self-service file-level recovery from the VM snapshots. For more information about self-service restore, see Self-Service Restore in the *Data Protection and Recovery with Prism Element* guide.

- **Nutanix VM Mobility**

  Facilitates VM migration between ESXi and AHV, in-place hypervisor conversion, and cross-hypervisor disaster recovery (CHDR) features. For more information about cross-hypervisor disaster recovery, see Nutanix Cross Hypervisor Disaster Recovery in the *Data Protection and Recovery with Prism Element* guide. For more information about in-place hypervisor conversion, see In-Place Hypervisor Conversion in the *Prism Element Web Console Guide*.

- **Application-consistent snapshots for Windows VMs**

  Enables Nutanix native in-guest Volume Snapshot Service (VSS) agent to take application-consistent snapshots for all the VMs that support VSS. This mechanism takes application-consistent snapshots without any VM stuns (temporary unresponsive VMs) and also enables third-party backup providers like CommVault and Rubrik to take application-consistent snapshots on the Nutanix platform regardless of which hypervisor is used in the cluster. For more information about Nutanix VSS-based snapshots for the Windows VMs, see the *Application-consistent Snapshots with Microsoft Volume Shadow Copy Service (VSS)* section in the Conditions for Application-consistent Snapshots topic of the *Data Protection and Recovery with Prism Element* guide.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2644

- **Application-consistent snapshots for Linux VMs**

  Supports application-consistent snapshots for Linux VMs by running specific scripts on VM quiesce. For more information, see the Conditions for Application-consistent Snapshots information of the *Data Protection and Recovery with Prism Element* guide.

- **Static IP address preservation support after failover for Nutanix Disaster Recovery (DR)**

  This feature allows the preservation of the IP address of a guest VM (with a static IP address) for its failover (DR) to an IPAM network. For more information, see the *Networking Requirements* section in the Nutanix Disaster Recovery Requirements topic of the *Nutanix Disaster Recovery Guide*.

- **In-guest scripts execution support for Nutanix Disaster Recovery (DR)**

  In-guest scripts automate various task executions upon recovery of the VMs. For example, you can automate the task of changing the domain controller or performing the reassigning of the DNS IP address and reconnection to the database server at the recovery AZ. For more information about the tasks that can be automated using In-guest scripts, see Creating a Recovery Plan in the *Nutanix Disaster Recovery Guide*.

Nutanix Guest Tools Requirements

Ensure that the following requirements are met so that you can successfully install NGT, and use all the NGT features.

General Requirements

- NGT can be installed on VMs running Windows or Linux OS only. It cannot be installed on VMs running VMware Photon OS. For information about the supported OS for specific NGT features, see the NGT section in *Compatibility and Interoperability Matrix*.
- A virtual IP address must be configured for the Nutanix cluster. If you change the virtual IP address of the cluster, the reconfiguration impacts all the VMs in your cluster on which NGT is installed. For more information, see Virtual IP Address Impact in the *Prism Element Web Console Guide*.
- Network access from the virtual IP address of the cluster to the guest VMs where Prism Central-based management of NGT is required.
- Network access from the guest VM to the virtual IP address of the cluster where IP-based connectivity is used for NGT.
- VMs must have at least one empty IDE or SATA CD-ROM to attach the ISO required for the configuration and installation of NGT, and for NGT functionalities such as IP-remapping during DR failover, enabling NGT on a remote cluster after DR failover, or CCLM.
- The following ports must be accessible to use the specific NGT functionality:
  - If IP-based communication is enabled, the TCP port 2074 of the cluster virtual IP address must be accessible from the guest VMs so that the guest VMs can communicate with the CVM. For more information, see Nutanix Guest Agent and Controller VM Communication.
  - The TCP port 23578 in the guest VM must be accessible if you want to use the VSS service.

  For the complete list of required ports, see Port Reference.

Windows Requirements

In addition to the General Requirements, ensure that the following requirements are met so that you can successfully install NGT in a Windows VM:

- To install NGT, you need a local user account in the VM with administrative privileges. Domain accounts are currently not supported.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2645

- For Windows Server Edition VMs, ensure that Microsoft Volume Shadow Copy Service (VSS) is enabled before you install NGT with the VSS application enabled. For more information about how to verify if Microsoft VSS is enabled on your server, see Microsoft documentation.

  Note:

  - Before you enable the VSS feature, upgrade the NGT version on the Windows Server Edition VMs to 2.3.2 or later. If not, the VSS snapshots will be marked as crash-consistent.
  - NGT's VSS feature is not supported on Windows Client Edition VMs or Linux VMs.

- During NGT installation a few PowerShell commands are executed. To run these commands, the PowerShell executable must be present in the PATH system variable of the environment. Otherwise, the installation of NGT might fail. For more information, see KB-7284.
- The PowerShell version on the Windows VMs must be 3.0 or later.
- Antivirus scanners might need exclusions added for the C:\Program Files\Nutanix directory for successful NGT installation.
- Windows Remote Manager Service (winrm) must be running and configured to allow SSL-based connections. The following commands are one of the many methods to configure winrm with SSL. These commands must be executed from an administrative Windows PowerShell console.

```
> $certificate = New-SelfSignedCertificate -DnsName $env:computername -
CertStoreLocation cert:\LocalMachine\My
```

```
> winrm create winrm/config/Listener?Address=*+Transport=HTTPS
 "@{Hostname=`"$env:computername`";CertificateThumbprint=`"$($certificate.ThumbPrint)`"}"
```

```
> cmd /c 'winrm set winrm/config/service/auth @{Basic="true"}'
```

```
> netsh advfirewall firewall add rule name=\"WinRM-HTTPS\" dir=in localport=5986
 protocol=TCP action=allow
```

  Note: Windows Remote Manager Service (winrm) is required to install NGT from Prism Central only. It is not required when you upgrade NGT or install NGT manually by logging in to the guest VM.

Linux Requirements

In addition to the General Requirements, ensure that the following requirements are met so that you can successfully install NGT in a Linux VM:

- To install NGT in bulk, ensure that any package manager configuration within the VMs works properly, as old or invalid configurations might prevent NGT package installation.
- Ensure that the VM has Python 2.6 or a later version installed.
- You must have a guest VM user account with password-based SSH, and root or passwordless SUDO access enabled.
- Ensure that the user has write permissions for the /usr/local directory as NGT is installed at this location.
- Ensure that the user has write permissions for the /mnt/nutanix/ngt directory to mount the NGT ISO at this location.
- Ensure that a minimum available disk space of 550 MB is available in the /mnt/nutanix/dir directory for copying the NGT installer when upgrading NGT.
- Ensure that the user has write access to /tmp directory for the duration of the installation.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2646

General Notes

- NGT includes VirtIO drivers when you install it on a Windows VM. If these drivers are already installed in your guest VM, they might be replaced during the installation of NGT, depending on the version that is bundled with NGT. If the drivers were downgraded, you might need to manually reinstall VirtIO and restart the VM if prompted. For more information about VirtIO drivers, see Nutanix VirtIO for Windows in *AHV Administration Guide*. For information about the compatible VirtIO driver versions, see the *AOS - NGT - VM Mobility Matrix* section in the *NGT* tab of the Compatibility and Interoperability Matrix.
- VirtIO driver installation updates the NIC driver in the guest VM. During the update, the guest VM might lose network connectivity. The network connectivity is restored after the update is complete.
- If a VM is connected to a volume group (VG), NGT captures the iSCSI Qualified Name (IQN) of the VM and stores the information. If you change the IQN of the VM and take a snapshot of the VM before the NGT refresh cycle (currently at 5 minutes) occurs, NGT does not provide the auto restore capability because the snapshot operation cannot capture the VM-VG connection.

  Workaround:

  - **Windows VM**: In the command prompt, run the net stop "Nutanix Guest Tools Agent" && net start "Nutanix Guest Tools Agent" command.
  - **Linux VM**: Restart the Nutanix Guest Agent (NGA) service by running one of the following commands:
    - For guest VMs that support the **systemd** OS, run the $ systemctl restart ngt_guest_agent command.
    - For guest VMs that do not support the **systemd** OS, run the $ sudo service ngt_guest_agent restart command.
- By default, NGT client certificates expire every 1,000 days. Regenerate the certificates before they expire. For more information, see Regenerating NGT Certificates for Guest VMs information in the *Prism Element Web Console Guide*.

NGT Management in Prism Central

You can use Prism Central to perform the following operations on a guest VM or multiple guest VMs:

- Enable NGT and mount the NGT installer
- Install NGT
- Upgrade NGT
- Manage NGT applications

In addition, NGT installation through Prism Central provides the following capabilities:

- Enable Nutanix Volume Shadow Copy Service (VSS) and Self Service Restore (SSR) applications as part of the install workflow
- Select multiple VMs in Prism Central from the VM Entity browser and upgrade NGT on these VMs
- Defer restarting of the VMs to a specified later time and date after installing or upgrading NGT
- Define policies that allow you to defer restarting of the VMs to a specified later time and date

Installing NGT

The installation of NGT using Prism Central is fully automated. You do not need to manually log in to the VM to install NGT. For large-scale deployments, Nutanix recommends to use Prism Central to install NGT.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2647

Before you begin

Ensure that all the requirements specified in Nutanix Guest Tools Requirements are met before you install NGT.

About this task

To install NGT, perform the following steps on a guest VM or multiple guest VMs at the same time in Prism Central:

> **Note:**
>
> - The guest VM must be powered on to install NGT in the VM.
> - You cannot install NGT on VMs created on storage containers with replication factor 1.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and go to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default with VMs across all the registered clusters.

   > **Tip:** The **NGT** status column associated with a VM displays whether the NGT is installed in the VM, whether it is the latest version, and whether an upgrade is available or not.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2648

3. Select the target VM checkbox in which you want to install NGT, and choose **Install NGT** from the **Actions** dropdown menu.
   The system displays the **Install NGT** window.

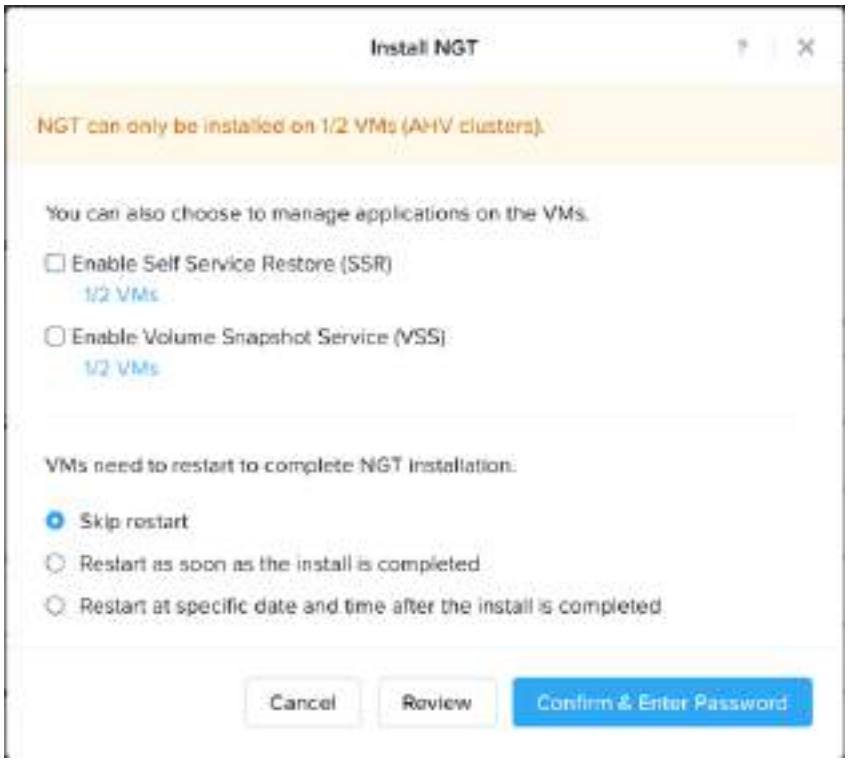


Figure 61: Installing NGT

> **Note:** If you select multiple VMs, this window displays the number of VMs on which you can install NGT. For example, if you select a VM on which NGT is already installed, it is skipped during this operation.

4. (Optional) To enable SSR and VSS applications, select the **Enable Self Service Restore (SSR)** and **Enable Volume Snapshot Service (VSS)** checkboxes.
   If you choose not to enable these features during the installation of NGT, you can do it later by following the instructions in Managing NGT Applications.

5. Select the restart schedule of the VM using either of the following options:

   - **Skip restart**: The VM does not restart after the installation completes.

     > **Note:** If you select **Skip restart**, the system checks if any NGT policy is defined, and applies the restart action; **Restart as soon as the install is completed** or **Restart at specific date and time after the install is completed** based on the NGT policy (if defined). For more information about how to create an NGT policy, see Creating a NGT Policy on page 485.

   - **Restart as soon as the install is completed**: The VM restarts after the installation completes.
   - **Restart at specific date and time after the install is completed**: The VM restarts at the specific date and time that you configure in the **Date** and **Time** fields.

     > **Note:** Nutanix recommends that you restart the VM after the NGT installation completes.

6. (Optional) Click **Review** to view your configurations.

7. Click **Confirm & Enter Password**.

8. In the **Username** and **Password** fields, enter a username and password of an account that meets the requirements specified in Nutanix Guest Tools Requirements, and is accessible to all the VMs on which NGT is being installed.

   > **Note:** If you choose to install NGT on multiple VMs and the VMs do not have the same username and password, you can add them to a JSON file and paste the file in the box provided. Click **Download sample json** to download a sample of the JSON file.

9. Click **Done** to start the installation process.

   When the installation completes successfully on a VM, the **NGT** status column of the VM in the **List** tab displays the status as **Latest**. It takes a few minutes for the status to reflect in Prism Central because this is an asynchronous operation.

   > **Note:** If the Nutanix Guest Tools Requirements are not met or you experience any issue with the installation process, the NGT installation fails and an alert message displays. Ensure that all the requirements are met and perform the installation process again to install NGT in the VMs.

10. (Optional) If you do not want to install NGT automatically or cannot provide the username and password of an account that meets the requirements, click **Skip and Mount** to complete the installation manually.

    Prism Central enables the NGT feature in the VM, mounts the NGT installer, and attaches an ISO to the virtual CD drive with the volume label NUTANIX_TOOLS to the selected VMs. You can then install NGT by logging in to the VM. For more information, see Installing NGT in a Windows VM or Installing NGT in a Linux VM in the *Prism Element Web Console Guide*.

    > **Note:** If NGT is already installed in the VM, it detects the NUTANIX_TOOLS CD and reconfigures itself. Once NGT is installed and the reconfiguration is successful, the system automatically unmounts NUTANIX_TOOLS. For more information, see CD-ROM Eject Functionality of NGT.

Enabling NGT and Mounting the NGT Installer on Cloned VMs

If you have cloned a VM or multiple VMs from a VM that had NGT installed, perform the following steps to re-enable and configure NGT on the cloned VMs.

About this task

Perform the following steps to enable NGT and mount the NGT installer on cloned VMs.

> **Note:** After you perform the following steps, you do not need to separately install NGT on the cloned VMs.

Procedure

1. Navigate to the **Install NGT** window by following the instructions mentioned in Steps 1 through 3 of Installing NGT.

2. Enable NGT and mount the NGT installer on the cloned VMs by following the instructions in Step 10 of Installing NGT (choosing **Skip and Mount**).

   NGT automatically identifies the ISO, updates the configuration, and unmounts the CD.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2650

Managing NGT Applications

Prism Central allows you to enable or disable the Nutanix Volume Shadow Copy Service (VSS) and Self-Service Restore (SSR) applications even after NGT is installed in a guest VM.

About this task

Perform the following steps to enable the SSR and VSS applications if you have not enabled them during the NGT installation workflow. You can also disable these applications (if already enabled) after NGT is installed using this procedure.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default with VMs across all the registered clusters.
3. Select the target VM checkbox in which you want to enable or disable the SSR and VSS applications, and choose **Manage NGT Applications** from the **Actions** dropdown menu.
4. In the **Manage Applications** window, select the corresponding option to enable or disable applications.
5. Click **Confirm** to save the changes.
   When you enable an application, the **Services Enabled** field in the **Properties** widget of the **Summary** tab displays the services enabled for the VM. For example, if you enable the SSR application the **Services Enabled** field displays **SSR**.

Upgrading NGT

Prism Central allows you to upgrade NGT on the guest VMs.

Before you begin

- Ensure that all the requirements specified in Nutanix Guest Tools Requirements are met.
- Unless you upgrade AOS, you cannot upgrade NGT.
- Upgrading NGT using Prism Central is supported on VMs that have NGT version 1.2.3 or later. If the VM has an earlier version of NGT, upgrade NGT using the procedure in the Upgrading NGT topic in the *Prism Element Web Console Guide*.

About this task

Perform the following steps to upgrade NGT on a guest VM.

> **Note:**
>
> - You can upgrade NGT on a maximum of 60 VMs at the same time.
> - For Linux VMs, upgrading a cluster running any NGT version prior to NGT 4.0 to NGT 4.0 or later versions, might fail. For more information, see KB-15396.

Procedure

1. Log in to Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2651

2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default with VMs across all the registered clusters.

3. Select the target VM checkbox in which you want to enable or disable the SSR and VSS applications, and choose **Upgrade NGT** from the **Actions** dropdown menu.
   The system displays the **Upgrade VMs** window.

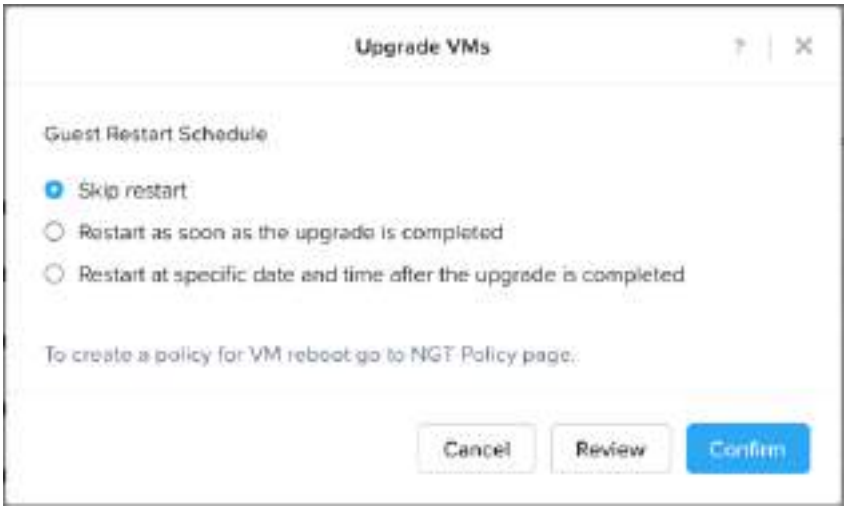


Figure 62: Upgrading NGT

4. In the **Upgrade VMs** window, select the restart schedule of the VMs using either of the following options:

   - **Skip restart**: The VM does not restart after the installation completes.
   - **Restart as soon as the install is completed**: The VM restarts after the installation completes.
   - **Restart at specific date and time after the install is completed**: The VM restarts at the specific date and time that you configure in the **Date** and **Time** fields.

   Note:

   - If you select multiple VMs to upgrade, the Upgrade VMs window displays the number of VMs on which you can upgrade NGT. For example, if you select a VM on which the latest version of NGT is already installed, that VM is skipped during this operation.
   - Nutanix recommends that you restart the VM after upgrading NGT.

5. (Optional) Click **Review** to view your configurations.

6. Click **Confirm** to start the upgrade process.

   When the upgrade is complete, the **NGT** status column associated with the VMs displays the status as **Latest**. It takes a few minutes for the status to reflect in Prism Central because this is an asynchronous operation.

   Note: If the Nutanix Guest Tools Requirements are not met or if you experience any issue with the upgrade process, the NGT upgrade fails and an alert message displays. Ensure that all the prerequisites are met and perform the upgrade process again to upgrade NGT.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2652

Uninstalling NGT

Prism Central does not support automatic uninstallation of NGT.

You must log in to a guest VM to uninstall NGT in that VM. For more information, see Uninstalling and Removing Nutanix Guest Tools in the *Prism Element Web Console Guide*.

> **Note:** If the NGT Status in Prism Central displays **Latest** after uninstalling NGT, follow the instructions mentioned in Step 3 of Uninstalling and Removing Nutanix Guest Tools in the *Prism Element Web Console Guide* to remove the NGT information from Prism Central.

Manage Bulk Operations for NGT

You can install or upgrade NGT in bulk on multiple guest virtual machines (VMs) using third-party endpoint management tools, such as Microsoft Intune or HCL BigFix, or automation tools, such as Ansible. Using these management tools, you can also remove NGT in bulk from guest VMs.

Bulk installation of NGT is supported on guest VMs running AOS 6.7 or later versions only.

The Nutanix Support portal lists the following NGT installer files:

- EXE file for Windows OS
- TGZ file for RPM-based Linux OS
- TGZ file for DEB-based Linux OS
- Nutanix NGT GnuPG public key

Download the latest installer files to install or upgrade NGT in bulk.

> **Note:** Bulk installation of NGT using third-party endpoint management tools does not require Prism Central. However, you must enable and mount NGT in guest VMs using Prism Central after installing NGT in VMs. For more information, see Enable and Configure NGT.

Prepare the NGT installation files for Distribution

You can install NGT using the installer files available in the Nutanix Support portal in a single VM or, in bulk, on multiple VMs. When you prepare to install NGT in bulk on multiple VMs, download the installer files and make them available for use by the third-party endpoint management tool deployed at your site. The instructions in this document assume that the third-party endpoint management tool deployed at your site requires that you host the NGT installer files on a web server.

Hosting the files for Windows VMs

Before you begin

Ensure that the NGT version is compatible with the AOS version installed in your cluster.

Procedure

1. Go to the Nutanix Support portal, select **Downloads** > **NGT**, and download the *nutanix-guest-agent-<version>.exe* installer file for Windows, which matches the AOS version installed in your clusters.
2. Host this installation file directly on the web server.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2653

Hosting the files for Red Hat Package Manager (RPM) based VMs

Before you begin

Ensure that the NGT version is compatible with the AOS version installed in your cluster.

Procedure

1. Go to the Nutanix Support portal, select **Downloads** > **NGT**, and download the *nutanix-guest-agent-rpm-<version>.tar.gz* installer file for RPM-based distributions, which matches the AOS version installed in your clusters.
2. Extract the *nutanix-guest-agent-rpm-<version>.tar.gz* file, and host the *NUTANIX-NGT-GPG-KEY* file and the *ngt_repo* directory on the web server.

Hosting the files for Debian (DEB) based VMs

Before you begin

Ensure that the NGT version is compatible with the AOS version installed in your cluster.

Procedure

1. Go to the Nutanix Support portal, select **Downloads** > **NGT**, and download the *nutanix-guest-agent-deb-<version>.tar.gz* installer file for DEB-based distributions, which matches the AOS version installed in your clusters.
2. Extract the *nutanix-guest-agent-deb-<version>.tar.gz* file, and host the i386 and amd64 directories on the web server.
3. (Optional) Perform the following steps to verify the DEB installer packages against the detached signatures using the *NUTANIX-NGT-GPG-KEY* file:
   a. Run the following command to import the public key:

      ```
      $ gpg --import NUTANIX-NGT-GPG-KEY
      ```

      The following is an example.

      ```
      $ gpg --import NUTANIX-NGT-GPG-KEY
      gpg: key 42DBF8BB: public key "Nutanix, Inc. (NGT Packaging)
       <security@nutanix.com>" imported
      gpg: Total number processed: 1
      gpg:               imported: 1  (RSA: 1)
      ```

   b. Run the following command to verify the DEB installer packages against the detached signatures:

      ```
      $ gpg --verify os-arch/nutanix-guest-agent.deb.asc os-arch/nutanix-guest-
      agent_version-1_os-arch.de
      ```

      Replace *os-arch* with the architecture of the OS of guest VM, and *version* with the NGA version.

      The following is an example.

      ```
      $ gpg --verify i386/nutanix-guest-agent.deb.asc i386/nutanix-guest-
      agent_4.0-1_i386.deb
      gpg: Signature made Wed 24 May 2023 01:46:29 PM UTC using RSA key ID 42DBF8BB
      gpg: Good signature from "Nutanix, Inc. (NGT Packaging) <security@nutanix.com>"
      gpg: WARNING: This key is not certified with a trusted signature!
      gpg:          There is no indication that the signature belongs to the owner.
      Primary key fingerprint: D8B0 18BD CFEB 774C D157  F0A5 11B1 600F 42DB F8BB
      ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2654

Install NGT in Bulk on Multiple VMs

You can install NGT in bulk on multiple Windows and Linux guest VMs using the NGT installer files available in the Nutanix Support portal.

Installing NGT in Bulk on Windows VMs

Before you begin

- Ensure that the cluster meets all NGT requirements. For more information, see Nutanix Guest Tools Requirements on page 174.
- Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.
- Review the end user license agreement (EULA) for Nutanix Guest Tools using a manual installation because the following installation procedure requires you to accept the EULA automatically.

Procedure

1. Configure the third-party endpoint management tool deployed at your site to distribute the *nutanix-guest-agent-<version>.exe* file to the VMs where NGT is installed.

   For more information, see the tool-specific documentation.

2. Configure the third-party endpoint management tool to install NGT by running one of the following commands:

   » `C:\ngtinstaller> nutanix-guest-agent-version.exe /quiet ACCEPTEULA=yes /norestart`

   Replace `version` with the NGA version.

   Use this command to ensure that VMs do not restart after you install NGT.

   > **Note:** This command might update the Nutanix VirtIO drivers if no Nutanix VirtIO drivers are installed or if a newer version is available, but the updated functionality of the VirtIO drivers is available only after a VM restart.

   » `C:\ngtinstaller> nutanix-guest-agent-version.exe /quiet ACCEPTEULA=yes`

   Replace `version` with the NGA version.

   Use this command to automatically restart the VM and to make all the updated VirtIO driver functionalities to be available in the VM.

3. (Optional) To generate the NGT logs in a location other than the %TEMP% directory, install NGT by running the following command.

   `C:\ngtinstaller> nutanix-guest-agent-version.exe /quiet ACCEPTEULA=yes /log log_file`

   Replace `version` with the NGA version, and `log_file` with the filename to write the logs.

   Ensure that the directory containing the filename that you provide has the necessary write permissions. Also, the installation process adds some events to the Windows application event log.

What to do next

After successful installation, enable and configure NGT in guest VMs. For more information, see Enable and Configure NGT.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2655

Installing NGT in Bulk on Linux VMs

About this task

This sample procedure provides steps to install NGT on Red Hat Package Manager (RPM) based operating systems. Use this procedure as a template to install NGT on Debian-based operating systems.

Before you begin

- Ensure that the cluster meets all NGT requirements. For more information, see Nutanix Guest Tools Requirements on page 174.
- Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.

Procedure

1. To verify the package signatures, configure the third-party endpoint management tool deployed at your site to install the NUTANIX-NGT-GPG-KEY file on RPM-based operating systems.

   For more information, see the tool-specific documentation.

2. Configure the third-party endpoint management tool to set up the repositories.

   For more information, see the tool-specific documentation.

   For example, guest VMs running RedHat 8.x distribution might need a repository configuration in /etc/yum.repos.d/nutanix-guest-tools.repo similar to the following configuration:

   ```
   [NutanixGuestTools]
   name=Nutanix Guest Tools
   baseurl=http://local-web-server/ngt_repo
   enabled=1
   gpgcheck=1
   gpgkey=http://local-web-server/RPM-GPG-PUBLIC-KEY
   repo_gpgcheck=0
   ```

   Replace *local-web-server* with the name of the web server used to distribute the NGT installer files as described in Preparing the NGT installation files for the Distribution.

3. Configure the third-party endpoint management tool to install the Nutanix guest agent package by running the package manager-specific install command.

   For example, the yum install -y nutanix-guest-agent command installs Nutanix guest agent package using the yum package manager for RedHat-based distributions.

   ```
   [nutanix@localhost ~]$ yum install -y nutanix-guest-agent
   ```

   For information about the install command specific to the package manager at your site, see the package manager-specific documentation.

What to do next

After successful installation, enable and configure NGT in guest VMs. For more information, see Enable and Configure NGT.

Enable and Configure NGT

Use Prism Central to enable and configure NGT in VMs so that you can use the NGT applications such as self-service restore, volume snapshot service, and application-consistent snapshots. The initial configuration of NGT requires mounting an ISO into the CD-ROM drive of guest VMs. The NGT agent detects the ISO and performs the initial configuration, making connections to the CVM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2656

Enabling and Configuring NGT using Prism Central

Before you begin

- Ensure that the cluster meets all NGT requirements. For more information, see Nutanix Guest Tools Requirements on page 174.
- Ensure that you install NGT in the VMs.

> **Note:** Because NGT is installed, you do not require WinRM or SSH access to the VM or a local user account in the VM with administrative privileges.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and go to **Compute** > **VMs** from the **Navigation Bar**.
   The system displays the **List** tab by default with VMs across all the registered clusters.

   > **Tip:** The **NGT** status column associated with a VM displays whether the NGT is installed in the VM, whether it is the latest version, and whether an upgrade is available or not.

3. To enable and configure NGT in a VM, select the target VM checkbox and choose **Install NGT** from the **Actions** dropdown menu.
   The system displays the **Install NGT** window.

   > **Note:** The Install NGT workflow is the same for installing NGT and enabling and configuring NGT if NGT is already installed.

4. To enable SSR and VSS applications, select the **Enable Self Service Restore (SSR)** and **Enable Volume Snapshot Service (VSS)** checkboxes.
   If you choose not to enable these features during NGT configuration, you can do it later by following the instructions in Managing NGT Applications.
5. Select **Skip restart** as the restart schedule.

   > **Note:** Because NGT is already installed in the VM, a restart is not required during NGT configuration.

6. Click **Confirm and Enter Password**.
7. Click **Skip and Mount**.
   Prism Central enables the NGT feature in the VM, mounts the NGT installer, and attaches an ISO to the virtual CD drive with the volume label NUTANIX_TOOLS to the selected VMs.

   > **Note:** Because NGT is already installed in the VM, it detects the NUTANIX_TOOLS CD and reconfigures itself. After NGT is installed and the reconfiguration is successful, the system automatically unmounts NUTANIX_TOOLS. For more information, see Automatic CD-ROM Ejection on page 193.

What to do next

The Nutanix Guest Agent (NGA) service in the VMs starts periodic communication with the CVM. To verify whether the NGA service is communicating with the CVM, log in to the CVM and run the following command:

```
nutanix@cvm$ nutanix_guest_tools_cli list_vm_tools_entities include_vm_info=true
 vm_name=vm-name
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2657

Replace *vm-name* with the name of one of the VMs.

Upgrade NGT in Bulk on Multiple VMs

You can upgrade NGT in bulk on multiple Windows and Linux guest VMs using the NGT installer file available in the Nutanix Support portal.

Upgrading NGT in Bulk on Windows VMs

Before you begin

- Ensure that the NGT version is compatible with the AOS version installed in your cluster. For more information, see the NGT section in the *Compatibility and Interoperability Matrix*.
- Ensure that the cluster meets all NGT requirements. For more information, see Nutanix Guest Tools Requirements on page 174.
- Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.

Procedure

- Perform Step 1 to Step 3 in Installing NGT in Bulk on Windows VMs.
  The installer detects that an existing NGT version is already present on the VM and performs an upgrade.

Upgrading NGT in Bulk on Linux VMs

About this task

This sample procedure provides steps to upgrade NGT on Red Hat Package Manager (RPM) based operating systems. Use this procedure as a template to upgrade NGT on Debian-based operating systems.

Before you begin

- Ensure that the NGT version is compatible with the AOS version installed in your cluster. For more information, see the NGT section in the *Compatibility and Interoperability Matrix*.
- Ensure that the cluster meets all NGT requirements. For more information, see Nutanix Guest Tools Requirements on page 174.
- Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.

Procedure

1. To verify the package signatures, configure the third-party endpoint management tool deployed at your site to install the NUTANIX-NGT-GPG-KEY file on RPM-based operating systems.
   For more information, see the tool-specific documentation.
2. Configure the third-party endpoint management tool to set up the repositories.
   For more information, see the tool-specific documentation.
   For example, guest VMs running RedHat 8.x distribution might need a repository configuration in /etc/yum.repos.d/nutanix-guest-tools.repo similar to the following configuration:

```
[NutanixGuestTools]
name=Nutanix Guest Tools
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2658

```
baseurl=http://local-web-server/ngt_repo
enabled=1
gpgcheck=1
gpgkey=http://local-web-server/RPM-GPG-PUBLIC-KEY
repo_gpgcheck=0
```

Replace *local-web-server* with the name of the web server used to distribute the NGT installer files as described in Preparing the NGT installation files for the Distribution.

3. Configure the third-party endpoint management tool to upgrade the Nutanix guest agent package by running the package manager-specific upgrade command.

   For example, the yum update -y nutanix-guest-agent command upgrades Nutanix guest agent package using the yum package manager for RedHat-based distributions.

   ```
   [nutanix@localhost ~]$ yum update -y nutanix-guest-agent
   ```

   For information about the upgrade command specific to the package manager at your site, see the package manager-specific documentation.

Uninstall NGT in Bulk from Multiple VMs

You can uninstall NGT in bulk from guest VMs using the third-party management tool deployed at your site.

> **Note:** Before uninstalling NGT from a guest VM, ensure the communication link between guest VM and CVM remains active. The CVM displays that NGT is uninstalled only if the communication between CVM and guest VM is active during the uninstallation. If the communication link is down, CVM continues to display that NGT is installed on the guest VM even after the successful uninstallation of NGT. For information about how to verify that the communication link is active, see Step 4 in Enabling NGT and Mounting the NGT Installer on Cloned VMs of the *Prism Element Web Console Guide*.

Uninstalling NGT from Windows VMs

About this task

When you install NGT in a Windows VM, NGT registers an uninstaller in the VM that can be accessed manually using Add/Remove Programs in the Windows Control Panel. This uninstaller can also be used by a third-party endpoint management tool to remove NGT from the VM.

Before you begin

Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.

Procedure

- Configure the third-party endpoint management tool to uninstall the Nutanix Guest Agent package using the uninstaller registered with Add/Remove Programs in the Windows Control Panel.

  For more information, see the tool-specific documentation or Microsoft Windows documentation.

Uninstalling NGT from Linux VMs

About this task

This sample procedure provides steps to remove NGT on Red Hat Package Manager (RPM) based operating systems. Use this procedure as a template to remove NGT on Debian-based operating systems.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2659

Before you begin

Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.

Procedure

- Configure the third-party endpoint management tool to uninstall the Nutanix guest agent package in bulk by running the package manager-specific removal command.

  For example, the yum remove -y nutanix-guest-agent command uninstalls Nutanix guest agent package using the yum package manager for RedHat-based distributions.

  ```
  [nutanix@localhost ~]$ yum remove -y nutanix-guest-agent
  ```

  For information about the removal command specific to the package manager at your site, see the package manager-specific documentation.

Nutanix Guest Agent and Controller VM Communication

You can set up connectivity between the controller virtual machine (CVM) and the guest VMs using the Nutanix Guest Tools (NGT) service that runs on the CVM and the Nutanix Guest Agent (NGA) service that runs on the guest VMs in the Nutanix cluster. After you install NGT in a guest VM, the NGA service in the guest VM starts periodic communication with the CVM based on the type of communication in a VM:

- **IP-less**: Communication between NGA and CVM happens only over a serial port connected to the guest VM.
- **IP-based**: NGA communicates with the CVM over SSL by connecting to the virtual IP of the CVM on port 2074.

By default on AHV clusters, the NGA service communicates with the CVM over IP-less connections using the serial port with index 1 on the guest VM. If the CVM does not respond, NGA reverts to IP-based communication.

For more information about how to check the communication type in a guest VM, to verify whether the NGA is communicating with the CVM, or to verify whether NGA is communicating with the CVM using IP or without an IP, see Communication Type Verification.

The communication type used between NGA and the CVM is determined when the guest VM starts. NGA might select an alternative communication type following a failover event or an event that requires a VM restart, such as disaster recovery or high availability.

IP-less Communication

In IP-less communication, the NGA service in the guest VM starts periodic communication with the CVM over the serial port with index 1 on the guest VM. The NGA service communicates with the CVM by sending remote procedure calls (RPCs) over the serial port to the CVM. The communication link over the serial port becomes active when NGA receives a response from the CVM. If the CVM does not respond, NGA reverts to IP-based communication.

> **Note:**
>
> - The serial port with index 1 on the guest VM is reserved for IP-less communication using NGT.
> - Only AHV clusters support IP-less communication.
> - Nutanix recommends that the virtual IP port 2074 on the CVM is accessible so that NGA can revert to IP-based communication in case of any failures.

IP-less communication enhances the security of the communication link because it does not require the CVM to be accessible by the VM over the network, and identification of the VM is guaranteed by the hypervisor without in-guest certificates.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2660

Prerequisites and Requirements

IP-less communication between the CVM and the guest VMs is established automatically when the following prerequisites and requirements are met:

- The guest VM must be running on AOS 6.6 or later, and NGT 3.0 or later versions.
- NGT is installed. For information about how to install NGT, see:
  - NGT Installation to install using Prism Element web console.
  - Installing NGT on page 176 to install using Prism Central.
- If an older version of NGT is already installed on the guest VM, you must upgrade it to the latest version. For information about how to upgrade NGT, see:
  - Upgrading NGT to upgrade using Prism Element web console.
  - Upgrading NGT on page 180 to upgrade using Prism Central.
- To switch an existing guest VM from IP-based communication to IP-less communication, Nutanix recommends that you upgrade AHV and AOS to the latest version, then restart the VM when installing or upgrading NGT on the VM. If you do not restart the VM, the serial port remains deactivated and the NGA service continues to communicate with the CVM using the virtual IP port 2074 on the CVM. After NGT is installed or upgraded, you must power cycle the VM to activate the serial port that is attached to it before IP-less communication can be used. An in-guest reboot might not be sufficient.

IP-based Communication

With IP-based communication, after you install NGT in a guest VM, the NGA service in the guest VM starts periodic communication with the CVM over SSL connections.

> **Note:** AHV, ESXi, and mixed clusters support IP-based communication.

Each Nutanix cluster is configured as a certificate authority (CA). When NGT is enabled in a VM, a certificate pair is generated specifically for that VM and it is embedded in an ISO that is configured for that VM. The security certificates are installed inside the VM as part of the installation process.

The NGA service inside the guest VM initiates an SSL connection to port 2074 of the cluster virtual IP address to communicate with the CVM. Any firewall must be configured to allow the guest VM to reach port 2074 on the cluster virtual IP address. For the complete list of required ports, see Port Reference.

NGT provides three levels of security for VM communication:

- SSL certificates that ensure a secure TCP connection between the CVM and the guest VM
- Capability-based authorization that ensures only NGT features that are supported by the cluster are enabled on the guest VM.
- NGT ensures that the communication is established only if the system or BIOS UUID of the guest VM and the UUID of the guest VM (provided by the hypervisor) stored in the CVM are the same.

Communication is successful only if all the three conditions are met. For example, if a VM that has NGT installed is cloned, the new VM cannot communicate with the CVM. You must separately enable NGT, and mount the NGT installer on the cloned VM. The NGT installer includes configuration specific to the VM, and when the VM is re-configured and is able to communicate with the CVM, it automatically unmounts the installation media. You do not need to separately install NGT again on the cloned VMs.

NGA also publishes information about the VM to the CVM, for example, guest OS type, status of VM mobility, and VSS services.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2661

Communication Type Verification

You can verify the type of communication established between the controller VM (CVM) and the guest VMs using Prism Central or the CVM SSH (CLI) console.

Verifying Communication Type Using Prism Central

You can verify the type of communication established between the CVM and the guest VM using Prism Central.

About this task

To verify the communication type using Prism Central, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default with VMs across all the registered clusters.
3. Click **Modify Filters** option to access the list of available filters.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2662

4. In the **NGT COMMUNICATION TYPE** filter, select the **IP-based** or **IP-less** checkbox to filter the VMs based on the NGT communication type.

   Note:

   - The **NGT COMMUNICATION TYPE** filter on a Prism Central hosted on an AOS 6.5.x cluster might in-correctly display the **IP-less** checkbox even though IP-less communication is not supported on AOS 6.5.x.
   - To check the VMs on which NGT is installed, select the **Installed** checkbox in the **NUTANIX GUEST TOOLS** filter. The system displays the list of VMs on which NGT is installed.

   The system displays the list of VMs based on the selected options.

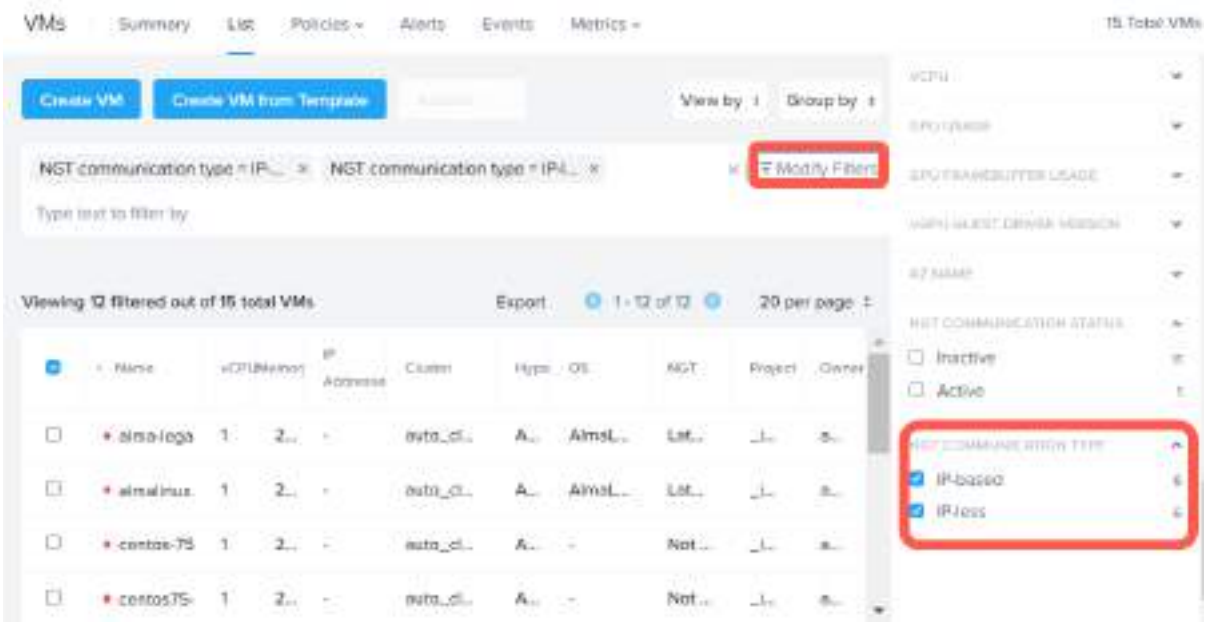


Figure 63: IP-Based and IP-Less Filter

Verifying Communication Type Using CLI

You can verify the type of communication established between CVM and guest VM using CVM SSH (CLI) console.

About this task

To verify the communication type using the CVM SSH console, perform the following steps:

Procedure

1. Log in to any CVM in the cluster as a Nutanix user with SSH.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2663

2. Run the following command:

```
nutanix@cvm $ nutanix_guest_tools_cli list_vm_tools_entities include_vm_info=true
 vm_name=vm-name
```

Replace *vm-name* with the name of the guest VM.

Observe the following attributes in the command output:

- communication_link_active = true - Indicates that the NGA is communicating with the CVM.
- communication_link_over_serial_port_active = true - Indicates that the communication between NGA and the CVM is IP-less.
- communication_link_over_serial_port_active = false - Indicates that the communication between NGA and the CVM is over IP.

Automatic CD-ROM Ejection

After NGT is installed or re-configured in a guest VM, the CD-ROM is auto-ejected from the VM in the following stages.

1. CD-ROM is automatically ejected from the VM immediately after the installation of NGT is successfully completed.
2. NGA indicates to the controller VM (CVM) that the installation is complete and the CD-ROM is detached from the VM through the hypervisor. This operation depends on the communication between the guest VM and the CVM and may take up to 10 minutes.

Note:

- These operations can occur at different times. It is possible that the CD-ROM shows up as empty inside a VM, but the status in the NGT-Controller VM service Tools Mounted might display as true. If this situation occurs, unmount the CD-ROM using the Prism Element web console.
- If the NGT software version in the ISO is more recent than the installed version in the guest VM, the CD-ROM does not eject automatically. This functionality enables the upgrade of the NGT software inside the VM.

NGT Usage in Disaster Recovery

If NGT is enabled on a guest VM that is protected by Nutanix Disaster Recovery, the snapshots of the VM include NGT relevant information along with its capabilities.

The NGT information is preserved for a restored guest VM in the following scenarios:

- Migrating the VM to the remote cluster (Planned Failover)
- Performing an in-place restore of the VM on the source cluster
- Creating a clone of the VM on the source cluster

In these scenarios, a new NGT ISO image containing only the relevant configuration information (SSL certificates, Controller VM IP address, ans so on) is created for the recovered guest VM and the image is automatically attached to the VM. When the VM is powered on, the NGA service running on the VM copies the relevant configuration information and detaches the NGT ISO CD-ROM automatically.

The NGT information is not preserved for a restored guest VM in the following scenarios:

- Performing an out-of-place restore of the VM on the remote cluster.
- Retrieving and restoring the snapshot from the remote cluster to the source cluster.

In these scenarios, you must enable NGT again in the restored VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2664

Storage Quality of Service (QoS)

Storage QoS provides administrators granular control to manage the performance of virtual machines and ensure that the system delivers consistent performance for all workloads. You can use a controllable knob to limit the IOPS that the storage layer would serve for individual virtual machines. IOPS is the number of requests the storage layer can serve in a second. You can set throttle limits on a VM to prevent noisy VMs from over-utilizing the system resources.

Note:

- Storage QoS is applicable only if you have an AOS Pro or above license. See the License Manager Guide for more information on AOS licenses.
- Setting storage QoS is not allowed when the AOS upgrade is in progress.

Terminology

Throttled IOPS

The maximum IOPS that the storage layer tries to admit over a sustained period. Applications that are running on the VM are not permitted to exceed this level. This prevents VMs from affecting a system beyond the set limits. However, if the system is in a state of flux, your application might not be throttled. To prevent application crashing due to misconfiguration, the throttled IOPS setting must not be less than one hundred. Otherwise, an error is raised.

Setting maximum IOPS on a VM may affect the cluster latency for that VM and may result in higher latency being displayed in the cluster latency charts. Performance of any other VM is not affected by this setting. You can view individual VM latency graph to ensure that the other VMs are not affected. You can also create a custom focus view to display the throttled IOPS for all the VMs.

Throughput

Throughput is the amount of data that an application sees from the storage layer underneath per second. The maximum throughput is calculated by multiplying the number of IOPS with the block size.

Calculation of the IOPS and Throughput

The default block size used for IOPS calculation is 32 KiB. If the block size is less than or equal to 32 KiB, then the system is rate limited by the number of IOPS and the bandwidth is calculated by multiplying the number of IOPS with the block size of the application. Otherwise, if the block size is greater than 32 KiB, the system is rate limited by the throughput and the number of IOPS is calculated by dividing the throughput by block size of the application.

For example, if you have set a throttle limit of 800 IOPS on a VM and the application is admitting IOPS with 8 KiB block size, then the application would see 800 IOPS and throughput of 6.25 MBps. However, if application is admitting IOPS with 64 KiB block size, then the application would see 400 IOPS and a throughput of 25 MBps.

The following table provides the information about the block size, IOPS, and throughput relationship when throttle limit is set to 800, 400, or 200 IOPS:

Table 33: Relationship between Block Size, IOPS, and Throughput

Block size	IOPS	Throughput
8 KiB	800	6.25 MBps
16 KiB	800	12.50 MBps
32 KiB	800	25 MBps
64 KiB	400	25 MBps

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2665

Block size	IOPS	Throughput
128 KiB	200	25 MBps

Limitations

Storage QoS has the following limitations:

- Storage QoS is not supported for an in-place restore, out-of-place restore, and snapshot operation on VM.
- While creating a clone of a VM, any QoS attributes throttle limit set on the original VM might not be applied to the new cloned VM. QoS throttle limit needs to be set on the new cloned VM separately.
- For linked clones, when you are sharing the vDisks across multiple VMs, shared disks are not a part of QoS policy and shared disks would not be throttled. Each VM might exceed the maximum limit depending on the shared vDisk usage. For example, during bootstorm in a VDI setup.
- If a VM has volume groups attached, then QoS is not applicable.
- Storage QoS is not supported for Metro Availability, synchronous replication, and Nutanix Files virtual machines.

Setting QoS for an Individual VM

About this task

Storage QoS allows you to set throttle limits on a VM to prevent noisy VMs from over-utilizing the system resources. Perform the following procedure to set the QoS for an individual VM.

To set QOS for an individual VM, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default with VMs across all the registered clusters.
3. Perform either of the following actions:
   - » Select the target VM checkbox, and choose **Set QoS Attributes**from the **Actions** dropdown menu.

     Note: This action is not permitted (greyed out) for the VM on which Prism Central is hosted.
   - » Click the target VM to access the VM Details View on page 117, and choose **Set QoS Attributes** from the **More** dropdown menu.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2666

4. In **Input Type** field, select either of the following options:

   » IOPS - For more information about IOPS, see *Throttled IOPS* information in Storage Quality of Service (QoS) on page 194.

   » Throughput - For more information about throughput, see *Throughput* information in Storage Quality of Service (QoS) on page 194.

   If you select:

   - **IOPS**- Enter a value for the throttled IOPS in the **Throttled IOPS** field.
   - **Throughput** - Enter a value for the throttled throughput in the **Throttled Throughput** field.

5. (Optional) Click **Show Details** to populate a table that describes the relationship between block size, IOPS, and throughput.

6. Click **Confirm** to set the defined QOS values for the target VM.

   Click **Clear Attributes** to delete all the values.

   The system stores the number of IOPS or throughput to be served by the storage layer.

   > **Note:** To edit the storage QoS setting, follow the same steps as described in this section, and enter a new value for **IOPS** or **Throughput**.

Memory Overcommit Management

The Memory Overcommit feature enables you to optimize the physical memory utilization of a VM. It allows the host to automatically detect whether the memory is under-utilized or over-utilized for a VM. Using Prism Central, you can enable the Memory Overcommit feature.

For more information about Memory Overcommit feature, and how to enable or disable it using Prism Central, see Memory Overcommit information in *AHV Administration Guide*.

Policies for VM Management

You can define VM-Host Affinity, VM-VM Anti-Affinity, and NGT policies for managing a VM. For information about Affinity and NGT policies, see VM Policy Management on page 463.

VM Template Management

In Prism Central, you can create VM templates to manage the golden image of a VM. A VM template can be considered as a master copy of a virtual machine. It captures the virtual machine configuration and the contents of the VM including the guest operating system, and the applications installed on the VM. You can use this template to deploy multiple VMs across clusters.

> **Note:** You can create or manage a VM template only as an admin user or a user with admin privileges.

VM Template Summary View

The **Templates** page displays the information about all the VM templates across registered clusters.

To access the summary view of all VM templates, perform the following steps:

1. Log in to Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2667

2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Templates** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The following is an example showing the **Templates** page with all the VM templates:

Figure 64: Summary View - All VM Templates

Table 34: Templates Page - Field Description

Field	Description	Values
Name	Displays the template name. Click the template name to view the detailed information about that template. For more information, see VM Template Details View on page 198.	*<Template name>*
Compute	Displays the virtual CPU count of the VM that is deployed using this template.	(vCPU count) x vCPU, where x is numeric digit.
Memory	Displays the total amount of memory available to the VM that is deployed using this template.	(Memory) x [MB|GiB], where x is numeric digit.
Storage	Displays total amount of storage available to the VM that is deployed using this template.	x [MB|GiB], where x is numeric digit.
Network	Displays the NIC count of the VM that is deployed using this template.	x NIC, where x is numeric digit.
Updated On	Displays the last date and time when the template has been updated.	(date and time), Timestamp in MM DD, YYYY, hh:mm AM/PM format. For example, Dec 27, 2022, 06:51 AM
Updated By	Displays the user who most recently updated the template.	<user>. For example admin
Active Version	Displays the name of the active version of the template. An active version is the version of the template that gets deployed by default when you click **Deploy VMs**.	(version). For example, Initial Version

You can perform the following actions for the VM templates in the **Templates** page:

- Access the detailed information about an individual VM template. For more information, see VM Template Details View on page 198.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2668

- Deploy a VM. For information about how to deploy a VM using VM template, see Deploying VM from a Template on page 204.
- Filter the VM templates list based on the template name using **Filters** pane. For more information about **Filters** pane, see Filters Pane on page 55.
- Sort the list of templates from the **Name** and **Updated On** columns. For information about sorts function, see Sort Function on page 55.
- Use the **Actions** dropdown menu to perform the available operations as described in Managing a VM Template on page 207.

VM Template Details View

The VM template details view includes two pages: **Summary** page and **Versions** page.

Summary Page

The **Summary** page of an individual VM template consists of a dashboard that provides the detailed information about the VM.

To access the **Summary** page of an individual VM template:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Templates** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
3. Click the <*VM_Template_Name*> to view the **Summary** page of an individual VM template.

> **Note:** Replace <*VM_Template_Name*> with the actual VM name at your site.

The following is an example showing the **Summary** page of an individual VM template:

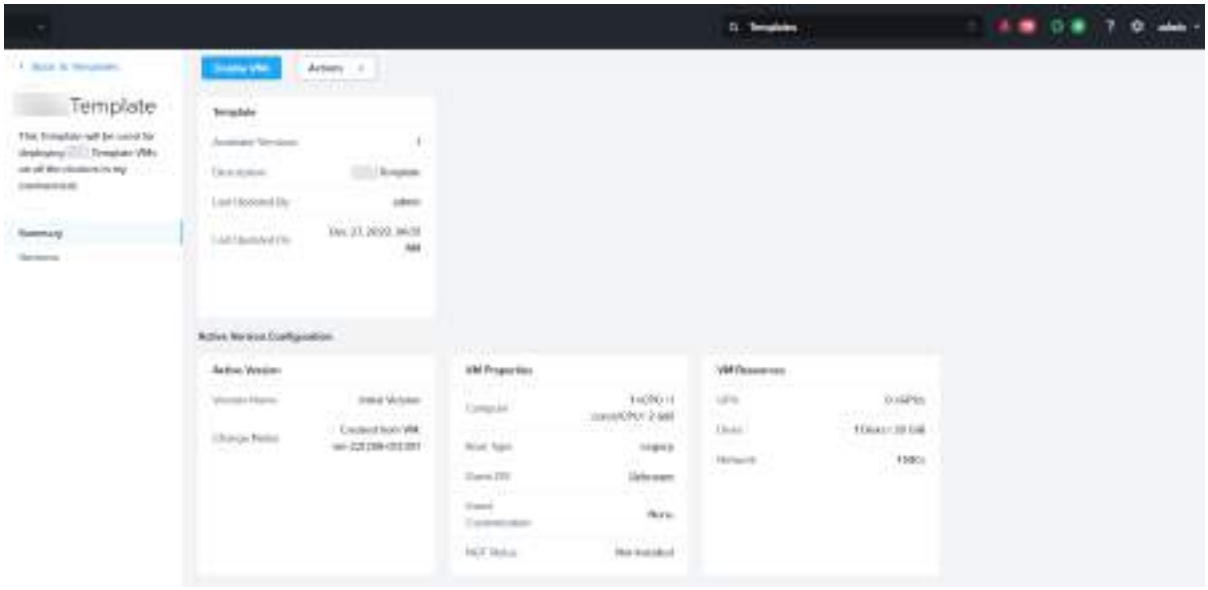


Figure 65: Summary Page - Individual VM Template

The **Summary** page provides you the options to deploy a VM using the selected VM template, and an **Actions** dropdown menu.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2669

- For information about how to deploy a VM using the VM template, see Deploying VM from a Template on page 204.
- For information about the list of actions available under **Actions** dropdown menu, see Managing a VM Template on page 207.

The **Summary** page of an individual VM template provides the following widgets:

- **Template**: This widget displays the following parameters:
  - **Available Versions**: Number of versions available
  - **Description**: User-provided description of the template
  - **Last Updated by**: User who has last updated the template
  - **Last Updated on**: Date and time of last update to the template
- **Active Version Configuration**: This widget displays the following parameters:
  - **Version Name**: Name of the currently active version of the template
  - **Change Notes**: User-provided change notes for the active version
- **VM Properties**: This widget displays the following parameters:
  - **Compute**: Compute resources of the VM such as CPU, core per CPU, and memory
  - **Boot Type**: Boot type of the VM such as legacy or UEFI
  - **Guest OS**: Guest OS of the VM. If the source VM of the template does not have NGT installed on it, then this field is displayed as unknown.
  - **Guest Customization**: Status of the guest customization application (applied/not applied)
  - **NGT Status**: Status of the NGT installation
- **VM resources**: This widget displays the following parameters:
  - **GPU**: Number of GPU assigned to the VM
  - **Disks**: Number of disks and total disk capacity assigned to the VM
  - **Network**: Number of NICs assigned to the VM

Versions Page

To view the **Versions** page of an individual VM template, click **Versions**.

The following is an example showing the **Versions** page of an individual VM template:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2670

Figure 66: Versions Page - VM Template

You can perform the following actions for the VM template version in the **Versions** page:

- Deploy a VM using the selected VM template version. For information about how to deploy a VM using the selected VM template version, see Deploying VM from a Template on page 204.

  Note: By default the active version of the template always gets deployed. In the **Versions** page, you can select the specific VM template version, and make it Active for VM deployment.

- Select a version and set it as active, or delete a selected version from the **Actions** dropdown menu. For more information, see Managing a VM Template on page 207.
- Filter the VM templates list based on the template name using **Filters** pane. For more information about **Filters** pane, see Filters Pane on page 55.
- Sort the list of templates from the **Name** and **Updated On** columns. For information on sorts function, see Sort Function on page 55.

Table 35: Versions Fields

Parameter	Description	Values
Name	Displays the VM Template version name. This column also indicates if the version is an active version.	*<Template _Version_name>*
Compute	Displays the virtual CPU count of the VM that gets deployed using this version.	(vCPU count) x vCPU, where x is numeric digit.
Memory	Displays the total amount of memory available to the VM that gets deployed using this version.	(Memory) x [MB|GiB], where x is numeric digit.
Storage	Displays total amount of storage available to the VM that gets deployed using this version.	x [MB|GiB], where x is numeric digit.
Network	Displays the NIC count of the VM that gets deployed using this version.	x NIC, where x is numeric digit.
Added On	Displays the last date and time when the version was added.	(date and time), Timestamp in MM DD, YYYY, hh:mm AM/PM format. For example, Dec 27, 2022, 06:51 AM

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2671

Parameter	Description	Values
Added By	Displays the user who added the version.	<user>. For example admin
Notes	Displays the user-specified change note for the version.	<Version-specific-text> that you specify in **Change Notes** field when you update a VM template version.

You can sort the list of versions by clicking on **Name** and **Added On** columns.

Limitations of VM Template Feature

The current implementation of the VM template feature has the following limitations:

- You cannot create a VM template if any of the following conditions is applicable at your site:
  - VM is not on AHV.
  - VM is an agent or a PC VM.
  - Any volume group is attached to the VM.
  - VM is undergoing vDisk migration.
  - VM has disks located on containers with replication factor 1.
  - VM is protected by PD-based DR.
- VM templates do not copy the following attributes from the source VMs:
  - Host affinity attributes
  - HA priority attributes
  - Nutanix Guest Tools (NGT) installation
  - Quality of service (QoS) configuration

  You must reconfigure the above-listed attributes at the deployed VMs.
- VM Template does not protect the underlying VM recovery point from deletion by a user having delete permission. VM Template deployment fails if you delete the associated VM recovery point.

Creating a VM Template

This section describes how to create a VM template in Prism Central.

About this task

To create a VM template, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab as default

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2672

3. In **List** tab, select the VM to create a VM template.

> **Note:** Before you select a VM to create a VM template, ensure that the VM is powered off.

4. In the **Actions** dropdown menu, select **Create VM Template**.

   You can also click **Create VM Template** in the **Summary** page of an individual VM. For information about how to access the **Summary** page of an individual VM, see VM Details View on page 117.

   The system displays the **Create template from VM** window.

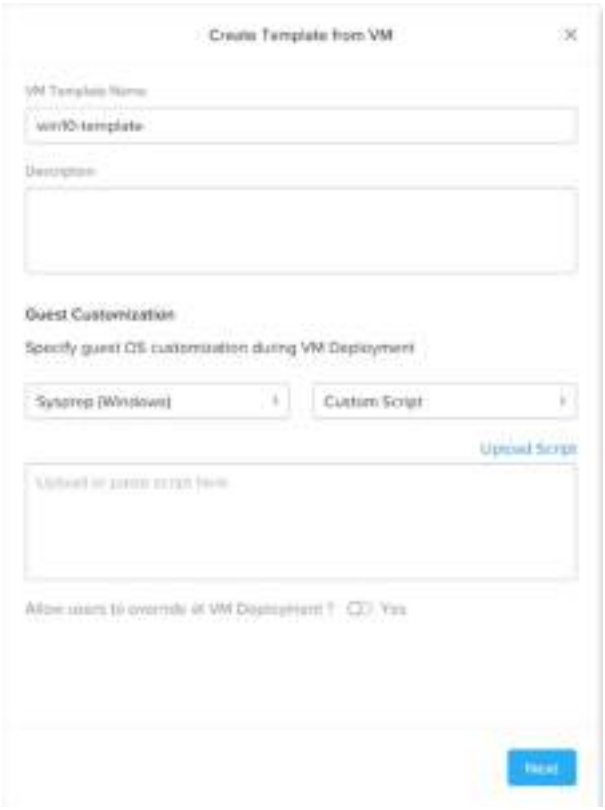


Figure 67: Create Template from VM window

5. In the **Create Template from VM** window, enter the following information:

   a. **Name** - Name of the VM Template.

   b. **Description** - Description for the VM template. Description is an optional field.

   c. For the **Guest Customization** fields, select the following options for guest operating system (OS) for the VMs that you deploy using this VM template:

      - In the **Script Type** field, select **Sysprep (Windows)** to customize the Windows OS, and **Cloud-init (Linux)** to customize the Linux OS.

> **Note:** If you select **No Customization** at the time of creating the template and allow the users to override the guest customization settings using **Allow users to override at VM Deployment?** toggle field, it

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2673

gives the maximum customization control to the users. In this case, the users can customize the script type and the configuration method.

- In the **Configuration Method** field, for each of these script types selected in **Script Type** field, select either upload a custom script or opt for a guided setup in the field.

  Note:

  - If you select **Custom Script**, you can either upload a script to customize the guest OS of the VMs, or you can copy-paste the script in the text box.
  - If you select **Guided Script** , enter the following information:
    - **Authentication Type**: Select one of the radio button to set the authentication type:
      - **Password**: Set a username and password for the user who uses this template to deploy the VM.
      - **SSH Key** [Cloudinit (Linux) only]: Set the SSH key for the user who use this template to deploy the VM.
    - **Locale**: Select the locale (language) from the dropdown list.
    - **Hostname**: Enter the hostname for the user who uses this template to deploy a VM
    - **License Key**: Enter the license key.

      Important: The information that you enter is used to customize the OS of the VMs that are deployed using this template.

Note: If you opt for **Guest Customization** setup with script (custom or guided script), ensure that the script is in a valid format. The system does not validate the guest customization scripts. In the script is not in valid format, the VM deployment might succeed but the guest customization script may not work as expected. You can observe the discrepancies (if any) only after the VM gets deployed.

d. Set the **Allow users to override at VM Deployment?** toggle field as per your requirement. This toggle field is used to enable or disable the override permission for guest customization settings.

- If this toggle field is:
  - *Enabled*: The system allows the users (who use this VM template to deploy VM) to modify the guest OS customization settings in VM template. The users can modify the settings only for the **Configuration Method** field. For example, the users can change the authentication information at the time of deploying a VM from VM template, or they can change from a guided setup to a custom script.
  - *Disabled*: The settings that are already provided in the VM template, can be used for VM deployment.

6. Click **Next**.

On the next page, you can review the template details.

The system prompts you to review the configuration details, resource details, network details, and management details.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2674

7. Click **Save** to save the inputs and create a VM template.

   The new template appears in the **Templates** page list.

   > **Note:** Once you create a VM template, the template metadata is available in Prism Central. The template data is stored as a VM recovery point and is co-located with the source VM. If you use the VM template to deploy a VM to another cluster, the recovery point is copied to the destination cluster before deployment.

Deploying VM from a Template

Before you begin

Ensure that the VM template is available. For information on how to create a VM template, see Creating a VM Template on page 201.

About this task

After you create a VM template, you can use the VM template to deploy any number of VMs across clusters.

To deploy a VM using a VM template, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Templates** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66 .
3. Select the target VM template to deploy VMs using either of the following methods:

   - In the **Templates** page, select the target template checkbox, and click **Deploy VMs**. For more information about **Templates** page, see VM Template Summary View on page 196.
   - In the **Summary** page of an individual VM template, click **Deploy VMs**. For more information about **Summary** page of an individual VM template, see VM Template Details View on page 198.
   - In the **Versions** page of an individual VM template, select the target VM template version, and click **Deploy VMs**. For more information on **Versions** page of an individual VM template, see VM Template Details View on page 198.

     > **Note:** In the **Versions** page, you can select any active or non-active VM template version for VM deployment.

   > **Note:** By default, the active version of the VM template is used for VM deployment.

   The **Deploy VM from Template** window appears. By default, you see a **Quick Deploy** method. You can click**Advanced Deploy** to access the **Advanced Deploy** method in **Deploy VM from Template** window . In **Advanced Deploy** method, you can view and modify some VM properties and network settings.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2675

4. Deploy VM using either of the following deployment methods:

   - **Quick Deploy** method:

     The is an example showing the **Quick Deploy** method:

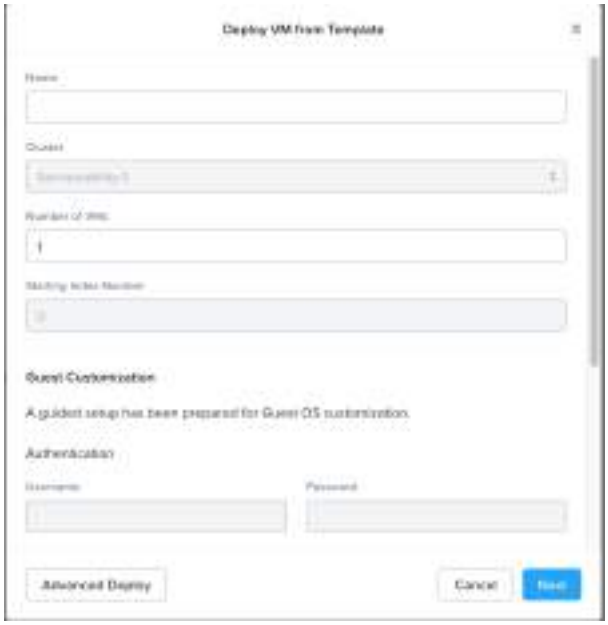


Figure 68: Deploy VM from VM Template using the Quick Deploy Method

1. Enter the following information:

   - **Name**: Enter a name for the VM.
   - **Cluster**: Select the cluster where you want to deploy the VM.
   - **Number of VMs**: Enter the number of VMs that you want to deploy.
   - **Starting Index Number**: Enter the starting index number for the VMs when you are deploying multiple VMs simultaneously. These index numbers are used in the VM names. For example, if you are deploying two VMs and specify the starting index number as 5, the VMs are named as *vm_name*-5 and *vm_name*-6.
   - **Guest Customization**: The template can have any one of the following options for guest OS customization:

     - **No Customization**
     - **Sysprep (Windows)**, or **Cloud-init (Linux)**. For **Sysprep (Windows)**, or **Cloud-init (Linux)**, you can choose to either upload a custom script or opt for a guided setup.

       Note: These fields are enabled for modification only if the VM template allows you to override its guest customization settings while deploying the VM. The **Allow users to override at VM Deployment?** toggle field is used to enable or disable the override for guest customization settings. For information on how to set this toggle field during VM template creation, see Creating

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2676

a VM Template on page 201. If the override permission for the guest OS customization is disabled, the settings that are already provided in the template can be used for VM deployment.

2. Click **Next** to verify the configuration details of the VMs to be deployed.
3. Click **Deploy** to deploy the VMs.

- **Advanced Deploy** method:

  The following is an example showing the **Advanced Deploy** method:

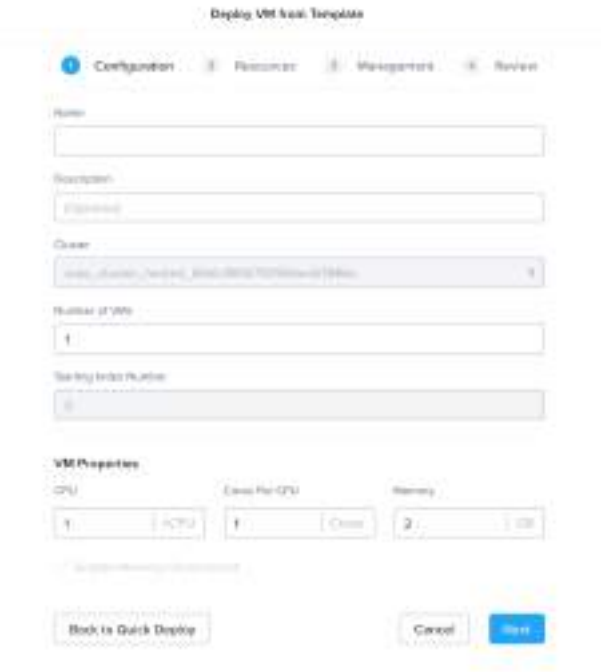


Figure 69: Deploy VM from VM Template using the Advanced Deploy Method

1. Enter the following information:

   - **Configuration**: Provide inputs for name and description (optional) of the VM, cluster where you want to deploy the VM, Number of VMs to be deployed, and starting index number (only if deploying multiple VMs). In this tab, you can also view and modify the VM properties such as CPU, core per CPU, and memory.
   - **Resources**: Review the configuration settings for the VM resources such as disks, networks, and boot configuration. Here, you can modify the network settings but cannot modify any other settings.
   - **Management**: The fields in this tab are enabled for modification only if the VM template allows you to override its guest customization settings while deploying the VM. The **Allow users to override at VM Deployment?** toggle field is used to enable or disable the override for guest customization settings. For information on how to set this toggle field during VM template creation, see Creating a

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2677

VM Template on page 201. If the override permission for the guest OS customization is disabled, the settings that are already provided in the template can be used for VM deployment.

If guest customization has been enabled, provide inputs for authentication type, username, password, locale, and Hostname.

> **Note:** Hostname of the VM is automatically generated based on the VM names that you provide. If you are deploying a single VM, you can override the automatic generation of the hostname by specifying a hostname. If you are deploying multiple VMs, you cannot override the automatic hostname generation.

- **Review**: Review the information displayed in this tab.

2. Click **Deploy** to deploy the VMs.

Managing a VM Template

About this task

After you create a VM template, you can perform the following actions to manage the VM Template:

- Update the guest OS of the source VM specified in the VM template
- Complete guest OS update
- Cancel guest OS update
- Update the configuration of the template to create a new VM template version
- Delete the VM template.

For information on how to create a VM template, see Creating a VM Template on page 201.

To manage a VM template, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Templates** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66 .

Select the target VM template using either of the following methods:

- Select the target VM template checkbox in the **Templates** page. For more information on **Templates** page, see VM Template Summary View on page 196.
- Click the target template to view the **Summary** page of an individual VM template. For more information about **Summary** page of an individual VM template, see VM Template Details View on page 198.

3. Select the required action from the **Actions** dropdown menu:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2678

Note: The available actions appear in bold and the unavailable actions are greyed out. The available actions depend on the current state of the template and user permissions.

The following actions are available in **Actions** drop down menu:

- **Update Guest OS**

  To update the guest OS in a VM Template, perform the following steps:

  1. Select the target VM template version on which the guest OS is to be updated in **Select a version to Update** window, and click **Proceed**.

     Note: By default the active version of the VM Template is selected for VM Template update, however the system provides you an option to select the VM Template version on which the guest OS is to be updated.

  2. Review the information displayed in the **Update Guest OS** window, and click **Proceed**.

     At this stage, the system deploys a temporary VM from the selected VM template version, and provides you an option to access the VM. You can also access the new VM from VMs **List** tab. For information on VMs **List** tab, see VMs Summary View on page 104.

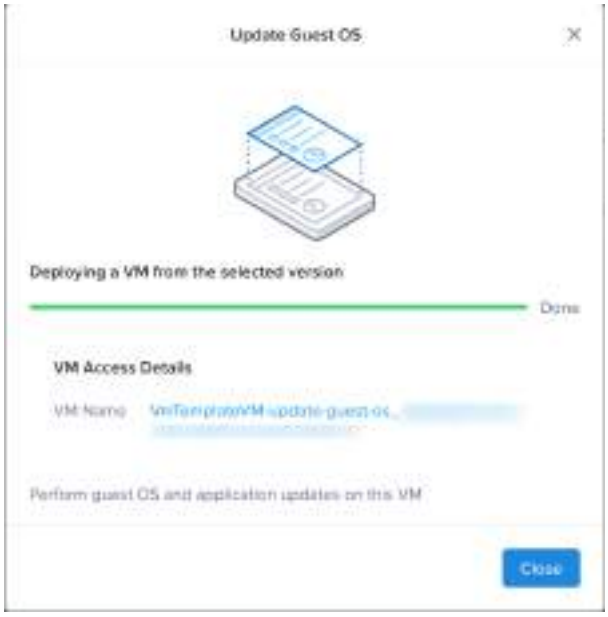


Figure 70: Update Guest OS

  3. Start the temporary VM, log on to the VM, and update the guest OS of the temporary VM. For information on how to update a VM, see Managing a VM through Prism Central (AHV) on page 143.
  4. Complete the guest OS update using the **Complete Guest OS Update** option from the **Actions** dropdown menu.

- **Complete Guest OS Update** to complete the process initiated for guest OS update. You must select this option only after successful update of the guest OS of the temporary VM. If you have opted for guest customization for

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2679

the deployed VMs, ensure to run Sysprep (for Windows) or Cloud-init (for Linux) before completing the guest OS update.

> **Note:** At this stage, the system prompts you to create a new version of the VM Template with updated guest OS. Specify the details for the new version, and click **Complete Update**.

The temporary VM automatically gets deleted after completion of the guest OS upgrade process.

- **Cancel Guest OS Update** to cancel the process initiated for guest OS update.

  The temporary VM automatically gets deleted after cancellation of the guest OS upgrade process.

- **Update Configuration** to modify the VM template configuration. In **Select a version to Update** window, select the VM template version that you want to modify, and create a version on top of it.

  Perform the following steps to update the VM template configuration in **Update Template Configuration** window:

Figure 71: Update Template Configuration

1. In the **Configuration** step, view the name of the base version that you want to update, change notes for that version, cluster name, VM properties (CPU, cores per CPU), and memory). In this section, you can modify only VM properties.
2. In the **Resources** step, view the information about disks, networks, and boot configuration. In this section, you can modify only network resources.
3. In the **Management** step, modify the guest customization settings.
4. In the **Review** step, review and modify the configuration settings that you are allowed to modify. You must provide a name and change notes for the new version. You can also choose to set this new version as active version.

   > **Note:** An active version is the version of the template gets deployed by default when you click **Deploy VMs** after VM template configuration update.

5. Click **Save** to save the settings and create a new VM template version.

- **Delete Template** to delete a template. The system prompts you to confirm the delete action. Click **OK** to delete the VM template.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2680

4. To only manage a VM template version:

   a. Select the VM template version from the **Versions** page. For information on how to access the **Versions** page of an individual VM template, see VM Template Details View on page 198.

   b. Select either of the following options from the **Actions** dropdown menu:

- **Set as Active** to make the selected VM template version as the active version.
- **Delete** to delete the selected VM template version.

> **Note:** You cannot delete the active version of a VM template.

Kubernetes Clusters Management

The **Kubernetes Clusters** entity in the **Infrastructure** application allows you to see the Kubernetes clusters that you deploy on the Nutanix clusters.

To see the Kubernetes clusters in the **Kubernetes Clusters** entity in the **Infrastructure** application, you must onboard the Kubernetes clusters to Prism Central. See Onboarding the Kubernetes Cluster to Prism Central on page 211 for more information.

Before you onboard any Kubernetes clusters to Prism Central, the **Kubernetes Clusters** entity page is displayed as follows:

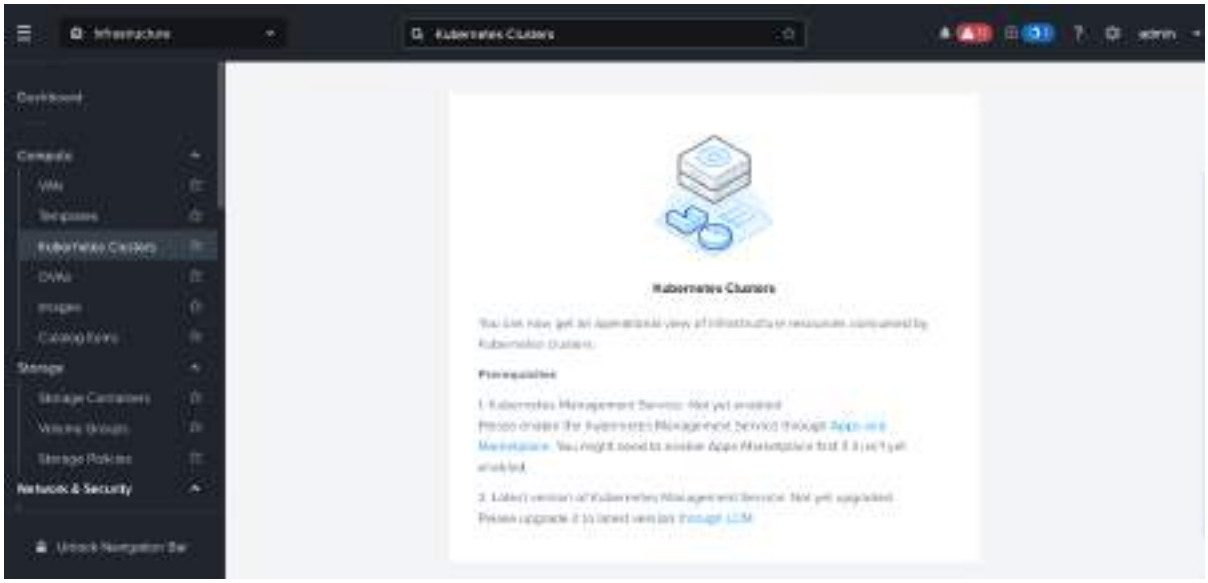


Figure 72: Kubernetes Clusters entity page before onboarding Kubernetes clusters

If you do not want to manage the Kubernetes clusters in Prism Central **Infrastructure** application, off-board the Kubernetes clusters. To off-board the cluster, use the `helm uninstall <helm-chart-name>` command. See the *What to do next* section in Onboarding the Kubernetes Cluster to Prism Central.

Kubernetes Cluster Entity Views

Prism Central provides the following views for the **Kubernetes Clusters**.

- Kubernetes Clusters Summary View on page 211
- Kubernetes Cluster Details View on page 212

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2681

Onboarding the Kubernetes Cluster to Prism Central

After creating the Kubernetes clusters with NKE Next Generation Workload Clusters (In Technical Preview) or Red Hat OpenShift, you need to onboard the clusters to Prism Central. After onboarding, you can view the Kubernetes clusters on Prism Central.

For information on NKE Next Generation Kubernetes cluster (In Technical Preview), see Next Generation Workload Cluster (Technical Preview) in the *Nutanix Kubernetes Engine Guide*.

For information on onboarding the Kubernetes cluster to Prism Central, see Onboarding Kubernetes Cluster to Prism Central in the *Nutanix Data Services for Kubernetes*.

Kubernetes Clusters Summary View

The **List** tab in the **Kubernetes Clusters** summary view provides a list of the Kubernetes clusters that you onboard to the Prism Central instance. To access the **Kubernetes Clusters** summary view, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Kubernetes Clusters** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   After you onboard the Kubernetes clusters, the **List** tab displays the onboarded Kubernetes clusters as follows.

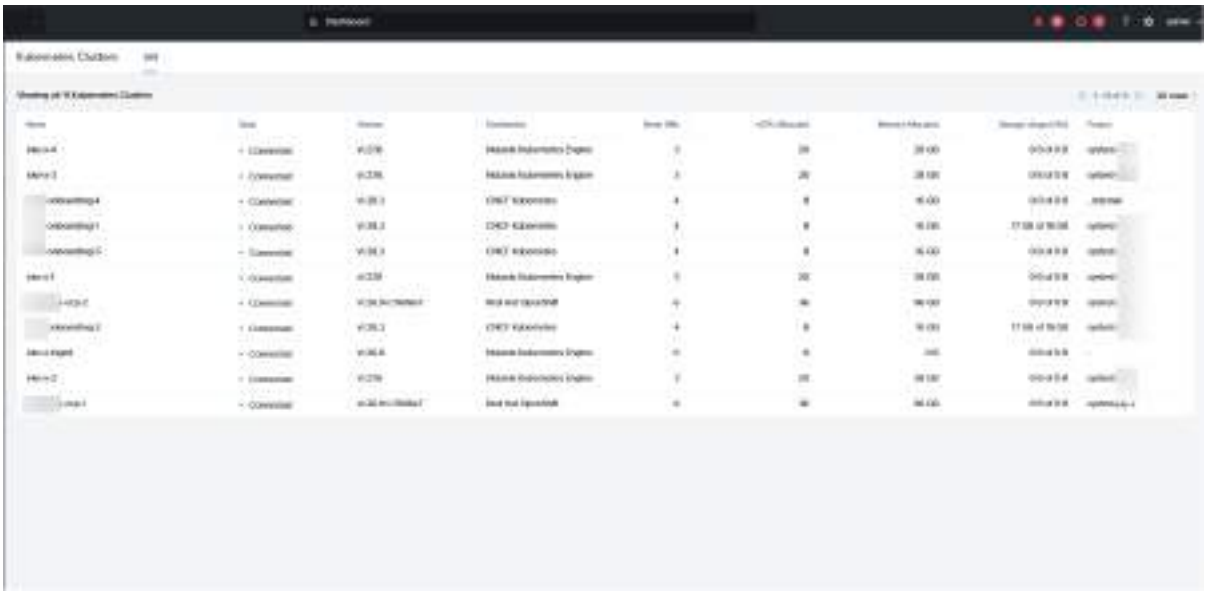


Figure 73: Kubernetes Clusters entity page after onboarding Kubernetes clusters

The following table describes the fields that appear in the **List** tab of the **Kubernetes Clusters** page. A dash (-) is displayed in a field when a value is not available or applicable.

Table 36: Kubernetes Clusters - List Tab Field Description

Field	Description	Values
Name	Displays the name of the Kubernetes cluster.	String
State	Displays the state of the connection to the Kubernetes cluster onboarding agent.	**Connected** or **Disconnected**

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2682

Field	Description	Values
Version	Displays the version of Kubernetes bundle used to deploy the Kubernetes cluster.	<version>. For example, **1.27.6**
Distribution	Displays the name of the tool used to create the Kubernetes.	**CNCF Kubernetes** **Red Hat OpenShift** **Nutanix Kubernetes Engine**
Node VMs	Displays the number of Node VMs in the Kubernetes cluster.	Integer
vCPU Allocated	Displays the number of vCPUs allocated to the Kubernetes cluster.	Integer
Memory Allocated	Displays the amount of memory in GB allocated to the Kubernetes cluster.	(Decimal number) GB
Storage Usage (VGs)	Displays the amount of Volume Group storage in bytes used by the Kubernetes cluster.	(Decimal number) B of (Decimal number) B
Project	Displays the name of the Project that manages the Kubernetes cluster. Displays `_Internal` if the Kubernetes cluster infrastructure resources are assigned to the default project VM.	String

Kubernetes Cluster Details View

The Kubernetes cluster details view displays the properties of individual Kubernetes cluster listed on the **List** tab of the **Kubernetes Clusters** summary view.

The Kubernetes cluster details view page provides information about the Kubernetes cluster on the following tabs:

- **Summary** tab—This tab is the default landing tab of the details view page.
- **Nodes** tab—This tab provides details of all the Kubernetes nodes in the Kubernetes cluster.
- **Storage** tab—This tab provides the details of the storage (Volume Groups or VGs) associated with the Kubernetes cluster.
- **Alerts** tab—This tab provides the details of the infrastructure alerts raised for the Kubernetes cluster.

To access the details view of an Kubernetes cluster, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Kubernetes Clusters** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
3. Click the **Name** of the Kubernetes cluster to view the **Summary** tab of the details view.

Summary Tab

The following is an example showing the **Summary** tab of an individual Kubernetes cluster.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2683

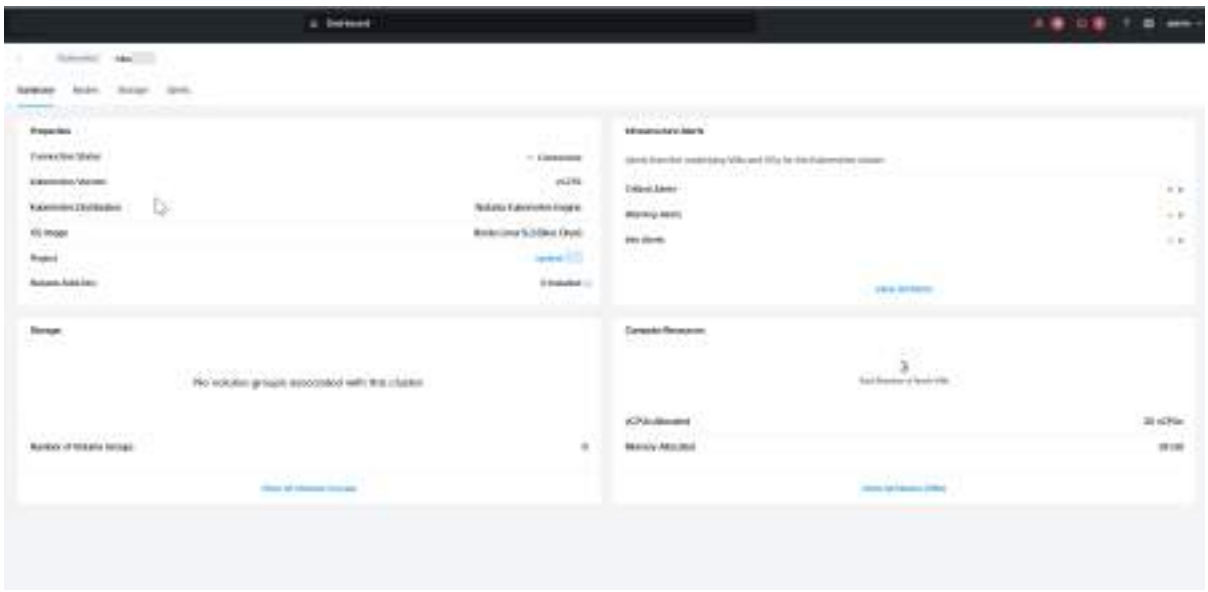


Figure 74: Kubernetes Cluster - Summary Tab

The **Summary** tab of an individual Kubernetes cluster provides the following widgets:

- **Properties**: This widget provides the following parameters.
  - **Connection Status**: The state of the connection to the Kubernetes cluster onboarding agent.
  - **Kubernetes Version**: The version of Kubernetes bundle used to deploy the Kubernetes cluster.
  - **Kubernetes Distribution**: The name of the Kubernetes distribution used to create the Kubernetes cluster.
  - **OS Image**: The distribution and version of the operating system underlying the Kubernetes cluster. For example, Ubuntu 22.04.3 LTS.
  - **Project**: The name of the project that is configured in the **Prism Central Admin Center** application, to manage the infrastructure resources utilized by the Kubernetes cluster.
  - **Nutanix Add-Ons**: The number of the Nutanix add-on packages such as Nutanix CSI or any Container Network Interface (CNI) packages.
- **Infrastructure Alerts**: This widget displays the purpose of this widget in a banner. This widget provides the following parameters for the alerts from the underlying VMs and VGs for this Kubernetes cluster.
  - **Critical Alerts**: The number of critical alerts generated in the AHV host for the VMs and VGs associated with the Kubernetes cluster.
  - **Warning Alerts**: The number of warning alerts generated in the AHV host for the VMs and VGs associated with the Kubernetes cluster.
  - **Info Alerts**: The number of informational alerts generated in the AHV host for the VMs and VGs associated with the Kubernetes cluster.

  For more information about alerts, see the Prism Central Alerts and Events Reference Guide.
- **Storage**: This widget provides the **Number of Volume Groups** associated with the Kubernetes cluster.

  It also provides a clickable link that opens the **Storage** tab in the Kubernetes cluster details view.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2684

- **Compute Resources**: This widget provides the following parameters about the VMs associated with the Kubernetes cluster.
  - **Total Number of Node VMs**: The total number of VMs on the AHV host associated with the Kubernetes cluster.
  - **vCPUs Allocated**: The number of vCPUs allocated to the Kubernetes cluster.
  - **Memory Allocated**: The amount of memory allocated (in GB) to the Kubernetes cluster.

  The widget also provides a clickable link that opens the **Storage** tab in the Kubernetes cluster details view.

Nodes Tab

The **Nodes** tab provides information about the AHV hosts associated with the individual Kubernetes cluster. The following is an example showing the **Nodes** tab of the Kubernetes cluster.

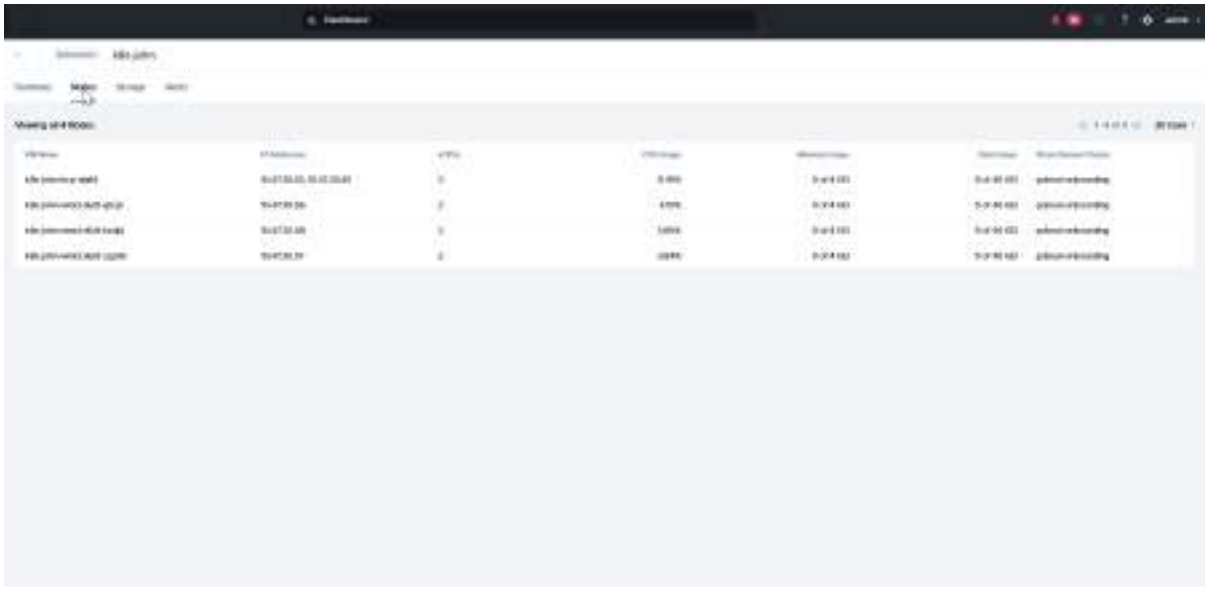


Figure 75: Kubernetes Cluster - Nodes Tab

Table 37: Nodes Tab Field Descriptions

Parameter	Description	Values
VM Name	Displays the name of the VM in the AHV host, that is associated with the individual Kubernetes cluster.	(String)
IP Addresses	Displays the IP addresses of the VM.	Comma-separated list of IP addresses in XXX.XXX.XXX.XXX without CIDR prefix.
vCPUs	Displays the number of vCPUs associated with the AHV host.	Integer
CPU Usage	Displays the CPU usage in percentage.	Decimal number with two decimal places suffixed with %.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2685

Parameter	Description	Values
Memory Usage	Displays the usage of the allocated memory.	<Usage> of <Allocated> memory suffixed with GB.
Disk Usage	Displays the usage of the allocated disk space.	<Usage> of <Allocated> disk space suffixed with GB.
Prism Element Cluster	Displays the name of the Prism Element cluster.	(String)

Storage Tab

The **Storage** tab provides the storage allocation and usage information associated with the individual Kubernetes cluster. The following is an example showing the **Storage** tab for the Kubernetes cluster.

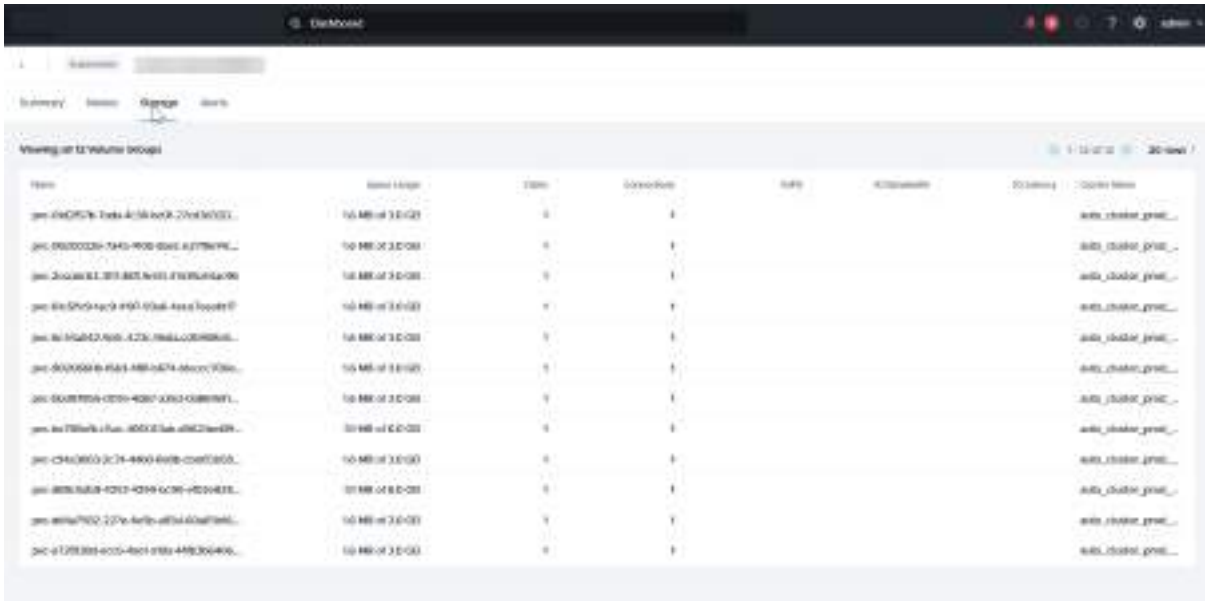


Figure 76: Kubernetes Cluster - Storage Tab

Table 38: Storage tab Field Descriptions

Parameter	Description	Values
Name	Displays the name of the Volume Group (VG).	Volume Group name
Storage usage	Displays the usage of the VG storage.	XX GB of <total> capacity GB
Disks	Displays the number of disks associated with the VG.	(Integer number)
Connections	Displays the number of connections to the VG.	(Integer number)
IOPS	Displays the IOPS of the VG.	(Integer number)
IO Bandwidth	Displays the Input Output (I/O) Bandwidth in MBps.	(Integer number)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2686

Parameter	Description	Values
IO Latency	Displays the I/O latency.	Time in ms
Cluster Name	Displays the name of the cluster on which the VG is located.	(Cluster name)

Alerts Tab

The **Alerts** tab provides the alerts information associated with the individual Kubernetes cluster. The following is an example showing the **Alerts** tab for the Kubernetes cluster.

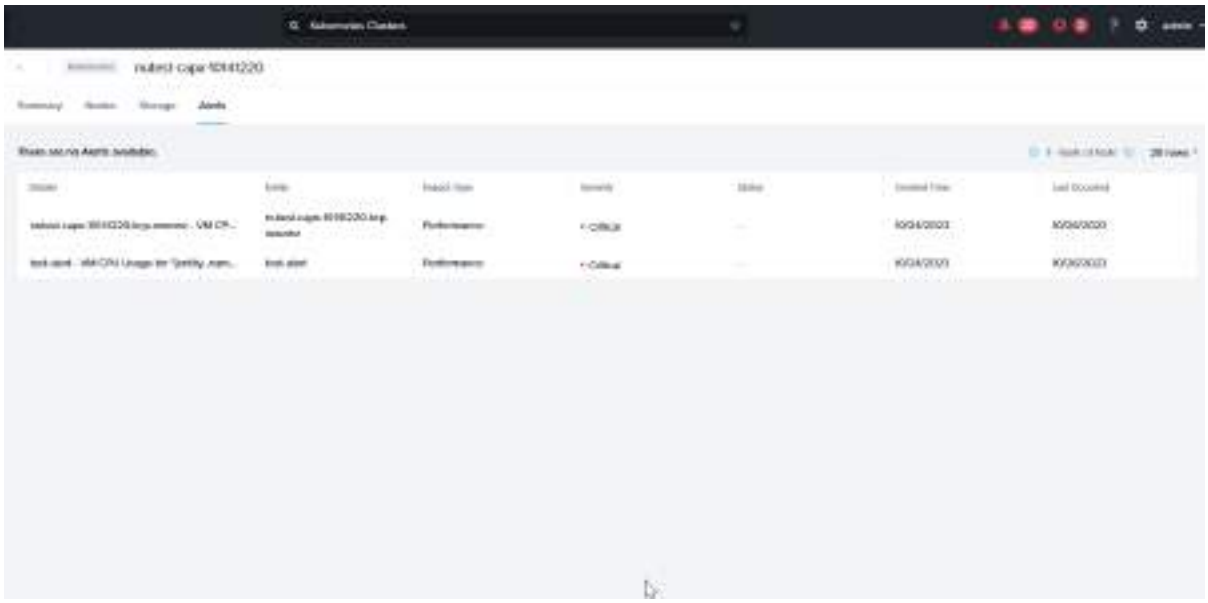


Figure 77: Kubernetes Cluster - Alerts Tab

The Alerts tab shows an extract of the entity's alert tab. For example, the alert page shows the alerts for the VM that the workload nodes are created on. This tab provides the same features and options as the Alerts dashboard, however it is filtered to display the alerts only for the selected Kubernetes cluster. For more information about alerts, see Prism Central Alerts and Events Reference Guide.

Table 39:

Parameter	Description	Values
Details	Displays the name of the entity and type of alert.	Concatenated value of entity name (for example, VM name) and the alert name.
Entity	Displays the name of the entity (VM or VG) that the alert applies to.	<entity-name>
Impact Type	Displays the category in which the alert is classified.	Availability, Capacity, Configuration, Performance, System Indicator

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2687

Parameter	Description	Values
Severity	Displays the severity level of this condition. There are three levels: Critical An actionable critical situation has been detected, and action is required immediately. The cluster can have the potential issues and can stop running, or run into irreparable issues. Warning An actionable issue has been detected, and user intervention is required. A more serious issue can occur if the alert is not resolved soon. Info (Informational) An actionable minor problem has been detected. It should be resolved relatively soon and not ignored.	Critical, Warning, Informational

Parameter	Description	Values
Status	Indicates whether the alert is resolved. Resolving an error means you set that error as fixed. The alert can return if the condition is scanned again at a future point. If you do not want to be notified about the condition again, turn off the alert for this condition. For more information about how to turn off the alert using alert policies, see Alert Policies (Prism Central). • A blank value means the alert is not resolved. • An **Acknowledged By** value means this alert is acknowledged manually by the specified user at the specified date and time. To manually acknowledge an alert, select the target alert check box and click **Acknowledge**. • An Auto Resolved (date_time) value means this alert was resolved automatically at the specified date and time. This functionality requires the auto resolve setting to be enabled for this alert type. For more information about how to set the auto resolve using alert policies, see Alert Policies (Prism Central). • A **Resolved By** user (date_time)" value means this alert is resolved manually by the specified user at the specified date and time. To manually resolve an alert, check the box for that alert and click **Resolve**.	(blank), Acknowledged By user (date_time), Auto Resolved (date_time), Resolved By user (date_time)
Created Time	Displays the date and time when the alert occurred.	(date and time)
Last Occurred	Displays the date and time when the alert is last generated (before this occurrence). If this is the first occurrence, both **Created Time** and **Last Occurred** display the same date and time.	(date and time)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2689

OVA Management

An Open Virtual Appliance (OVA) file is a tar archive file created by converting a virtual machine (VM) into an Open Virtualization Format (OVF) package for easy distribution and deployment. OVA helps you to quickly create, move or deploy VMs on different hypervisors.

The minimum supported versions to perform OVA operations are AOS 5.18, Prism Central 2020.8, and AHV-20190916.253.

You can perform the following OVA operations in Prism Central:

> **Note:** All the following operations are supported from the **OVAs** page except exporting a VM as an OVA. You can export a VM as an OVA from the **List** tab in VMs Summary View on page 104 or from the **Summary** page in VM Details View on page 117.

- Export a VM as an OVA. For more information, see Exporting a VM as an OVA on page 222.
- Upload an OVA. For more information, see Uploading an OVA on page 223.
- Deploy an OVA file as a VM. For more information, see Deploying an OVA as VM on page 233.
- Download an OVA file to your local machine. For more information, see Downloading an OVA on page 240.
- Rename an OVA file. For more information, see Renaming an OVA on page 240.
- Delete an OVA file. For more information, see Deleting an OVA on page 241.
- Resume upload when an upload is interrupted and shows an error.

> **Note:** The resume upload action is not available in case the concatenate process of the upload is interrupted. In such a case, you need to run the Concatenate API from the **REST API Explorer** to resume the upload.

To perform any action on an OVA, select the target OVA in the **OVAs** page, and choose the required action from the **Actions** dropdown menu.

> **Note:**
>
> The **Actions** dropdown menu appears only if you select an OVA in the **OVAs** page. If the **OVAs** page is empty, then the **Actions** dropdown menu is available only after you create an OVA using **Upload OVA** or export an existing VM as an OVA.
>
> The following is an example showing the **Actions** dropdown menu in **OVAs** page.

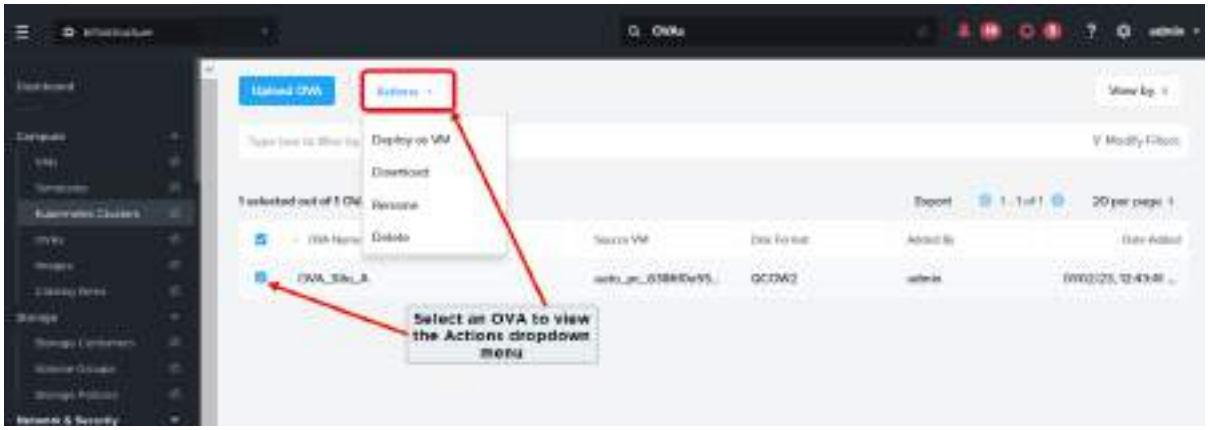


Figure 78: Actions Dropdown Menu - OVAs Page

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2690

You can check the task progress for these actions in **Tasks** page or from the Tasks icon. For information about **Tasks** page, see Tasks View on page 452.

OVAs Summary View

This section provides the information about the OVAs summary view, OVA-specific alerts, and the fields that appear in the **OVAs** page.

> **Note:** Only the **super admin** role has the permission to view OVAs.

To access the summary view of all OVAs across registered clusters, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **OVAs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   Prism Central displays **OVAs** page that enables you to view the information about OVAs available in the cluster.

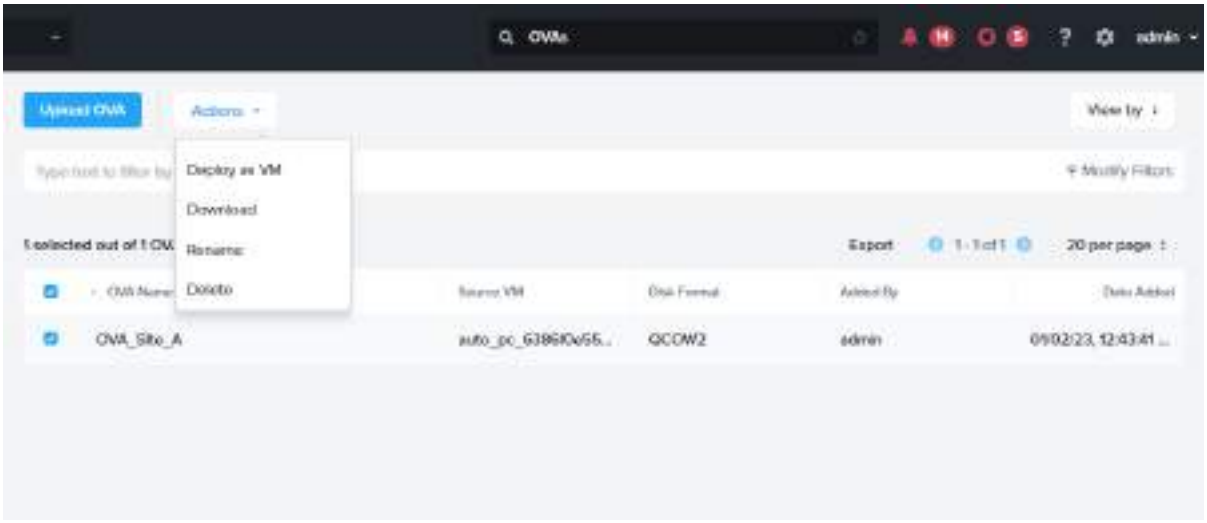


Figure 79: OVAs Page

The following table describes the fields that appear in the **OVAs** page. A dash (-) is displayed in a field when a value is not available or applicable.

Table 40: OVAs Page - Field Description

Field	Description	Values
OVA Name	Displays the name of the OVA file.	*<OVA_File Name>*
Source VM	Displays the name of source VM that was exported as an OVA. The alert indicators for the task status are displayed beside the source VM for which the task is run. See the Alert indicator table for more information.	*<Source_VM_File Name>*
Disk Format	Displays the format of the disks in the OVA.	[QCOW2|VMDK]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2691

Field	Description	Values
Added by	Indicates the user who added this OVA.	*<User_Name>*. For example, admin
Date added	Displays the date and time when the OVA was added.	(Timestamp in mm/dd/yyyy format, time in hr:min:sec [AM|PM] format) Example: 01/07/23, 3:00:20 PM

OVA Alerts

This section provides the information about the OVA specific alerts generated in Prism Central.

Table 41: OVA Alerts

OVA Alerts	Status Message sample	Description
 Figure 80: Failure Alert	`Incorrect file uploaded. Multiple OVA files present in OVA.`	Indicates the upload process failed during validation. You must fix the issue in the OVA file or upload the correct, compatible OVA file.
 Figure 81: Error Alert	`Upload for OVA file has not started. Please start OVA file upload using Resume Upload option.` `Uploaded OVA file has not been verified. Please start verification using Resume Upload option.`	Indicates there is an interruption in one of the three sub-tasks in the upload process. You can resume the upload. See the *Resume Upload* action procedure.
 Figure 82: Progress Alert	`OVA file upload is in progress.`	Indicates the OVA upload is in progress without any error or interrupts. Check the **Tasks** page after some time to verify the successful upload. For information on how to access **Tasks** page, see Icons in Prism Central UI on page 42 (using the Tasks icon) or Tasks View on page 452.

A sample of the error hover message is as follows:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2692

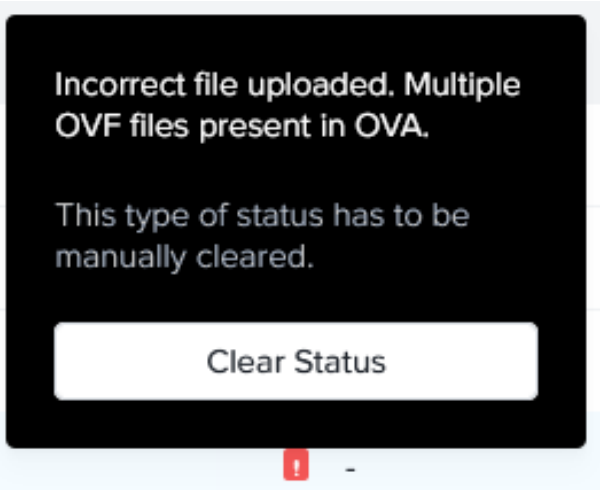


Figure 83: Sample error hover message

Filters Pane - OVAs page

You can filter the information in the **OVAs** page based on the following fields that are available in the **Filter** pane. For information about how to use **Filters** option in Prism Central, see Prism Central GUI Organization on page 54.

Table 42: Filter Pane Field Description - OVAs page

Field	Description	Values
OVA Name	Filters based on the OVA file name. It returns a list of OVAs that matches the name condition/string.	*<OVA file name >*
Source VM	Filters based on the Source VM name. It returns a list of OVAs for which the Source VM field matches the condition/string.	*<Source VM name>*
Disk Format	Filters based on the disk format. Select one or more checkbox for the OVAs of the required disk format.	VMDK, QCOW2

Exporting a VM as an OVA

Before you begin

If you intend to run the OVA in a non-Nutanix environment, ensure that you install the necessary drivers as per the requirements of the destination hypervisor.

About this task

This section describes how to export a VM an OVA.

As a Super Admin, you can select the **Export as OVA** from the **Actions** dropdown menu in the VMs **List** tab or click **Export as OVA** action in the **Summary** page of an individual VM. For information about how to access the **List** tab or **Summary** page of an individual VM, see VMs Summary View on page 104 and VM Details View on page 117.

Note:

- You can export a VM as an OVA with a specified disk format for the disks configured on the VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2693

- The Super Admin role was formerly called as User Admin.

To export a VM as an OVA, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment. For information about how to access the list of VMs managed by external *vCenter*, see VMs Summary View on page 104.
3. Select the target VM checkbox, and choose **Export as OVA** from the **Actions** dropdown menu.

   You can also click the target VM to access VM Details View on page 117, and select **Export as OVA** from the **More** dropdown menu.

   The system displays the **Export as OVA** window:

Figure 84: Export as OVA window

4. Specify the following information:
   a. Enter the name for the OVA file in the **Name** field.
   b. Select the disk format in which you want to export the OVA file in the **Export Disk Format** field.

      The default format is QCOW2. If you want to use the OVA to deploy a VM with disks formatted as VMDK, then select VMDK as the disk format.
5. Click **Export**.

   You can check the progress of the *Export as OVA* task in the **Tasks** page or from the Tasks icon. For information about **Tasks** page, see Tasks View on page 452.

   The exported OVA is available on the OVA dashboard.

Uploading an OVA

About this task

This section describes how to upload an OVA in Prism Central.

You can upload an OVA from the following sources:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2694

- *From a local folder*: When you upload an OVA from a local source, you can upload it to only one target cluster.
- *From a URL*: When you upload an OVA from a URL, you can upload it to multiple clusters. The upload operation runs concurrently on all the selected clusters.

Select the appropriate upload source based on your requirement; a single cluster upload or multiple-cluster upload option.

Note:

- Prism Central supports the upload of up to three OVA files concurrently from local folders. Prism Central queues other OVA files that you upload until one or more of the concurrent uploads are completed.
- There is no restriction on the number of concurrent uploads for OVA uploads from URL.
- You need admin privileges for uploading an OVA.
- For OVA upload from local folders, the upload process can be interrupted due to the following reasons:
  - Network issues when the upload is running.
  - You close the browser window or tab in which the upload is running.
- The concatenate and validate operations of the OVA upload operation fail when an error occurs in the upload services because the checksum provided for the OVA file when it was created is incorrect.

  If the upload process is interrupted due to any reason, you can resume the process. If the validation operation is interrupted due to a concatenation error, you must run the concatenate API to resume concatenation and validation. See Concatenating Upload using APIs on page 230.

Prism Central uses indicators to display the status of OVAs that you may have tried to upload. The status message is displayed when you hover the mouse or pointing device cursor on the indicator. See *OVA Alerts* section in OVAs Summary View on page 220.

To upload an OVA, perform the following steps:

Procedure

1. Log in to Prism Central as a user with admin privileges.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **OVAs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **OVAs** page

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2695

3. Click **Upload OVA**.
   The system displays the **Upload OVA** window.

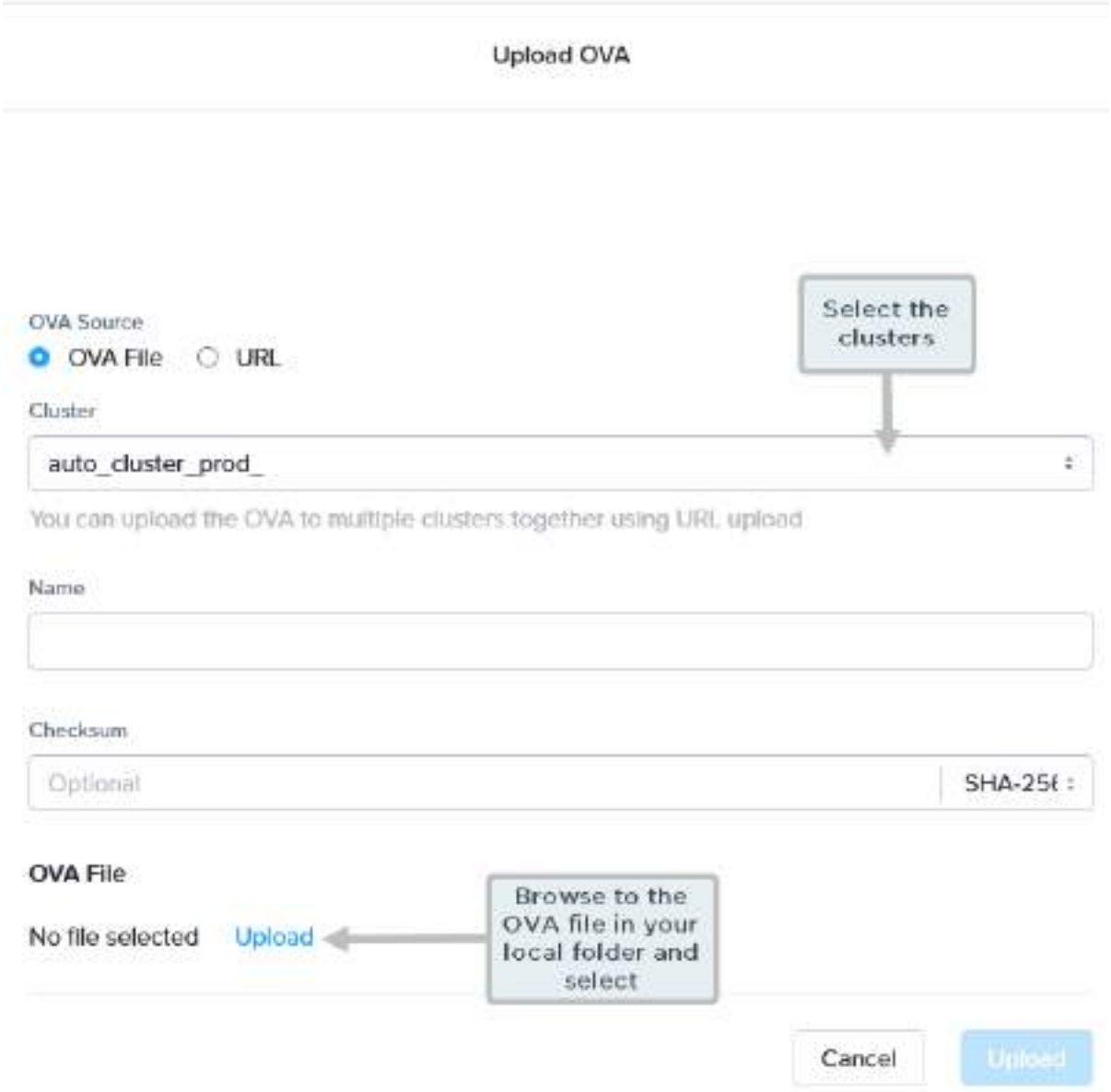


Figure 85: Upload OVA window

4. Specify the following field information in the **Upload OVA** window:

   a. **OVA Source**: Select the OVA source. For example, **OVA File** to upload from a local folder or **URL** to upload from a URL.

      If you choose **URL** in the **OVA Source** field, you can select multiple clusters in the **Select AHV Cluster** field. One cluster gets selected by default in the **Select AHV Cluster** field.

   b. **Name**: Enter the name for the OVA file.

      By default, Prism Central uses the file name of the OVA file that you upload, if you do not specify OVA file name in the **Name** field.

   c. (Optional) **Checksum**: Enter the checksum value of the OVA file based on the selected encryption as SHA-1 or SHA-256 hash algorithm.

   d. Based on your selection in the **OVA Source** field, perform the following relevant action:

      - **OVA File**: Click **Select File** to navigate to the location of the OVA file in your local folder and open it.
      - **OVA URL**: Enter the source URL from where you want to upload the OVA file.

        Note: Only NFS and HTTP protocols are supported.

        To specify one or more URLs, enter the appropriate URL address in the field using the following syntax for either NFS or HTTP:

        ```
        nfs://[hostname|IP_addr]/path
        http://[hostname|IP_addr]/path
        ```

        Enter either the name of the host (*hostname*) or the host IP address (*IP_addr)* and the path to the file. If you use a *hostname*, the cluster must be configured to point at a DNS server that can resolve that

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2697

name (see Configuring Name Servers for Prism Central in *Prism Central Admin Center Guide*). A file uploaded through NFS must have 644 permissions.

The following is an example showing the OVA URL field:

Figure 86: OVA URL field

> **Note:**
>
> Ensure that the URL that you provide is not redirected to another URL. The upload fails for redirected URLs.

Prism Central adds the URL to a list on the page and clears the **OVA URL** text box for another URL.

e. Click **Upload**.

The OVA upload starts. Wait until the **Continue in Background** option is displayed.

> **Note:** The **Continue in Background** option is not displayed for uploads from URL.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2698

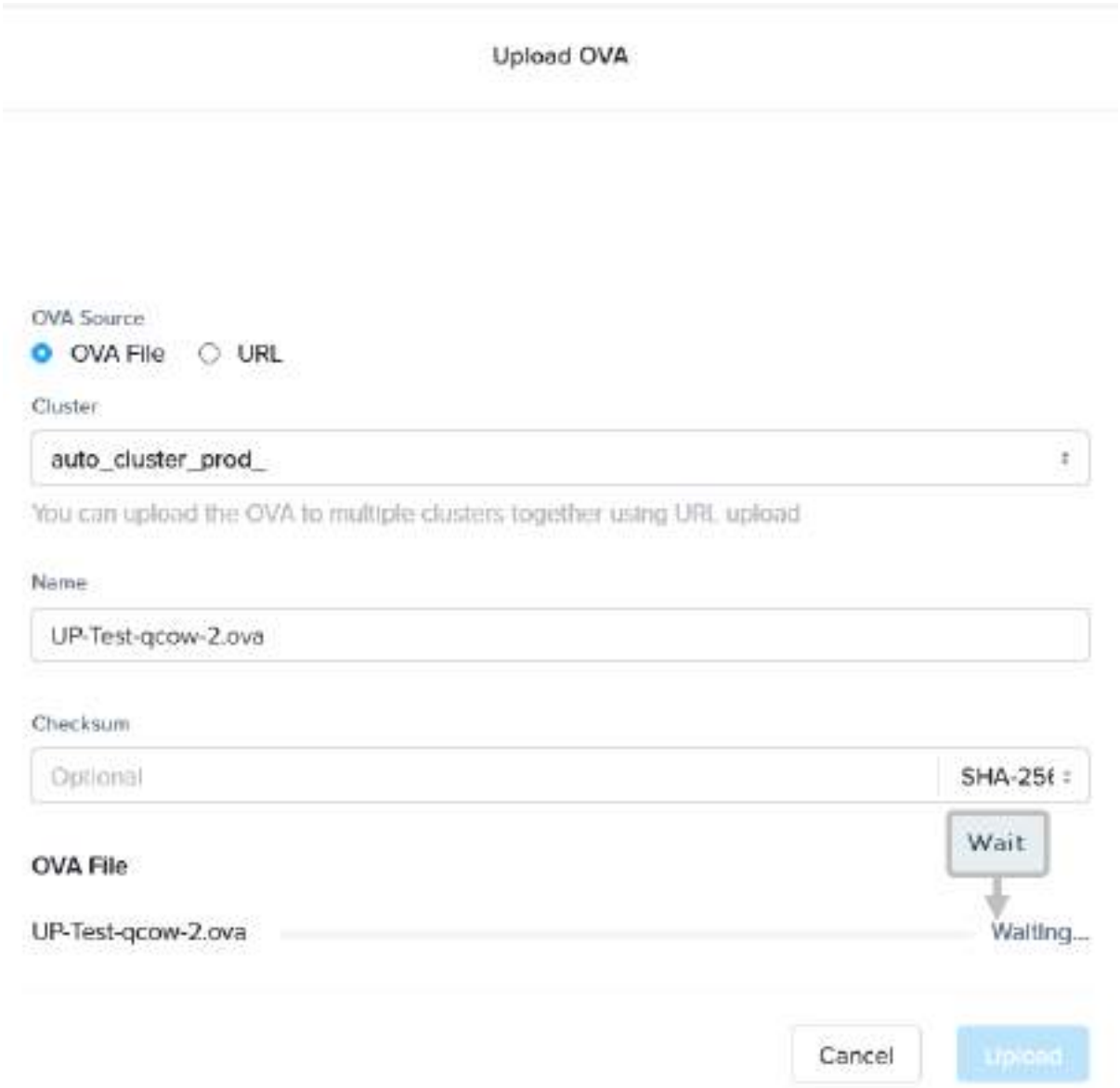


Figure 87: Upload OVA - Waiting

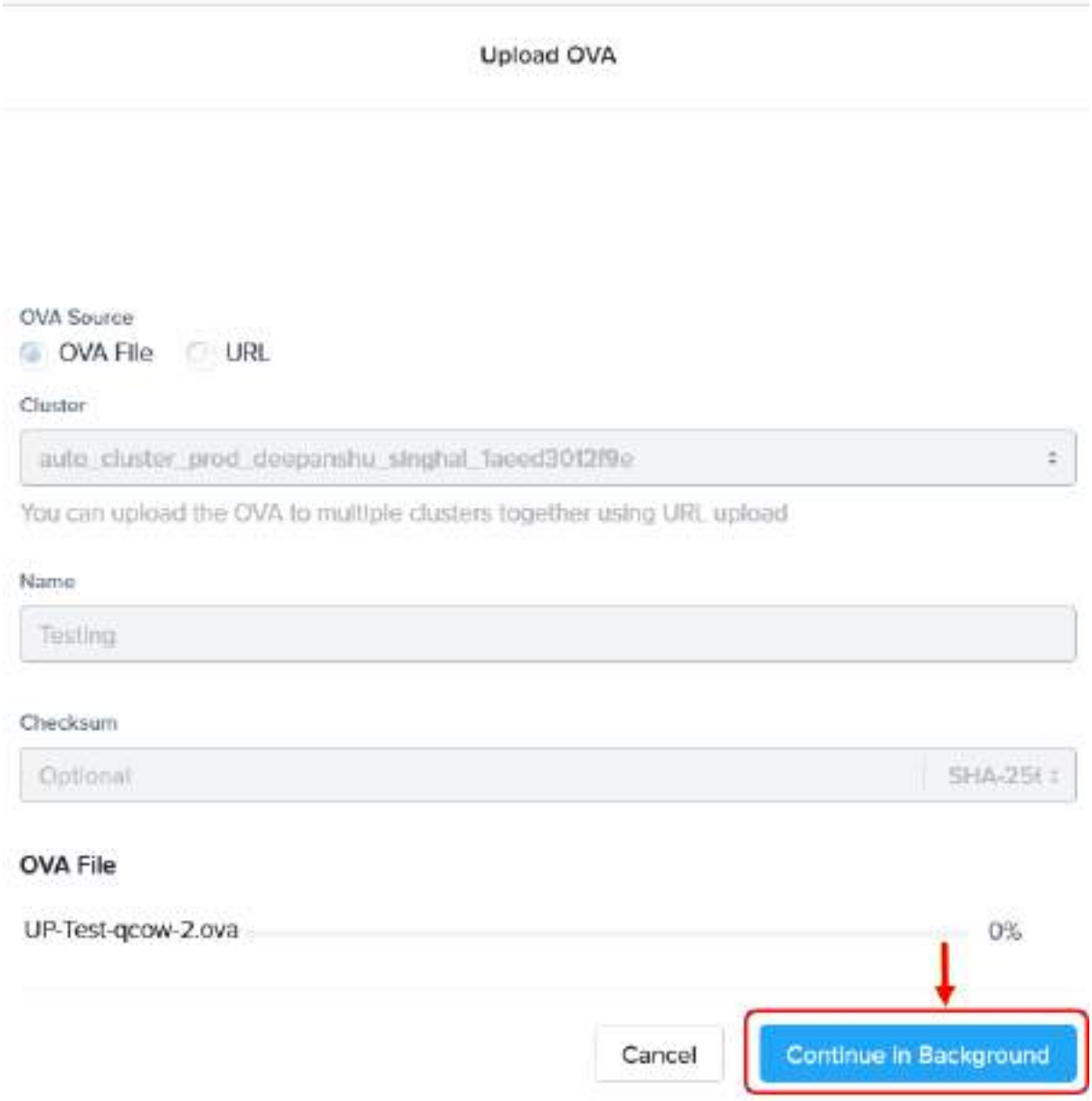


Figure 88: Continue in Background button

When the upload task is successfully completed, the system displays the following message:

```
Upload of the file is successfully completed. Verification of file is progressing in
 background. Please track it from Tasks page.
```

5. To resume an upload process that was interrupted, select the target OVA in the **OVAs** page, and choose **Resume Upload** from the **Actions** dropdown menu.

   The status message appears when you hover the mouse over the status icons for each OVA. The status message provides the indication about whether you can use the **Resume Upload** option to resume the upload.

   Note:

   Check the reason for failure of **OVA Validate** task in the **Tasks** page. If the upload process is interrupted due to concatenation and validation failure resulted from an incorrect checksum, the **Resume Upload** option is not available.

   Upload the OVA again in case the upload process was interrupted due to a checksum error.

Concatenating Upload using APIs

About this task

This section describes how to run the concatenation API using the **REST API Explorer** in Prism Central.

During an OVA upload, the OVA file is chunked and the chunks are uploaded. After upload, during the validation phase, the chunks are concatenated and validated.

When the OVA upload process is interrupted due to the concatenation error, you need to run the concatenation API to resume the upload process.

To run the concatenation API successfully, you need to perform the following actions:

- Derive the UUID of the OVA for which the upload is interrupted. The UUID is derived using the name of the OVA. For more information, see *Step 1* to *Step 4* in the following procedure.
- Run the concatenation API. For more information, see *Step 5* to *Step 6* in the following procedure.

Procedure

To run the concatenation API, perform the following steps:

1. Log in to Prism Central.
2. Select **REST API Explorer** from the `<user>` dropdown menu in the upper-right corner.

   The **REST API Explorer** opens in a new browser tab and displays a list of the objects that can be managed by the API.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2701

3. In the **REST API Explorer** browser tab, navigate to **ovas** > **Post /ovas/list**, and click **Try it Out**.The **Post /ovas/list** helps you filter the OVAs and get the details of the details of the interrupted OVA.

Figure 89: REST API Explorer

Figure 90: REST API Explorer -Try it Out

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2702

4. Enter the name of the OVA in the **"filter"** field of **get_entities_request** API in the following format, and click **Execute**.

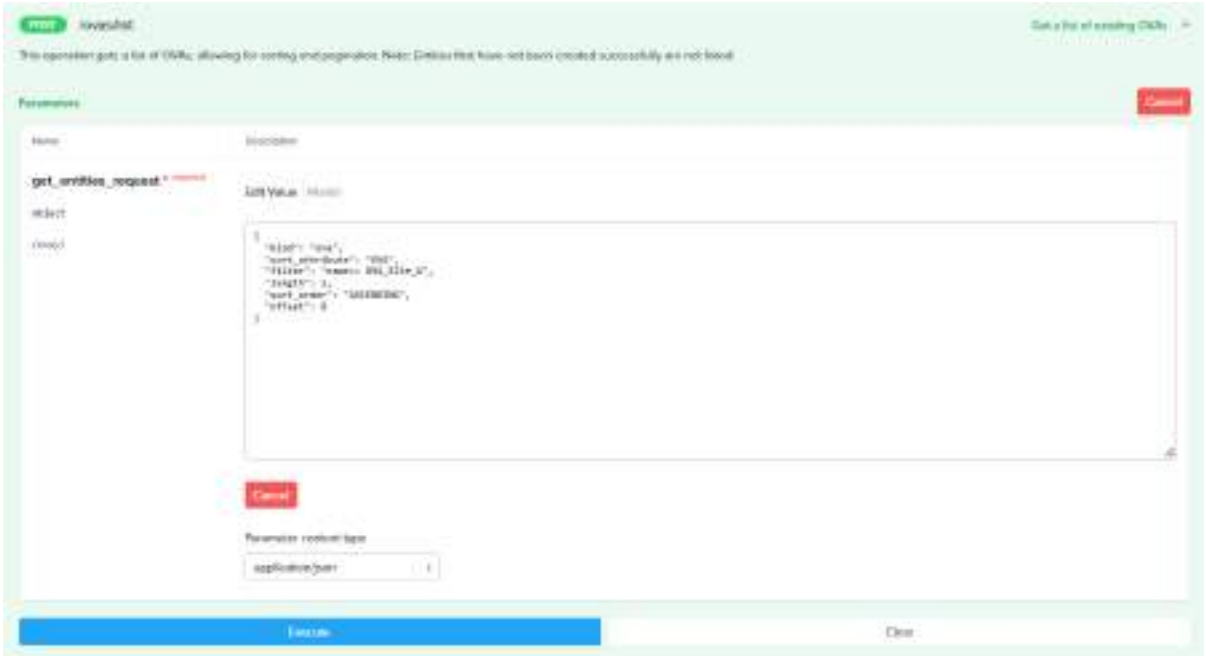


Figure 91: Parameter Filter

In the **Response Body** box, the UUID of the queried OVA is listed. Note or copy the UUID.

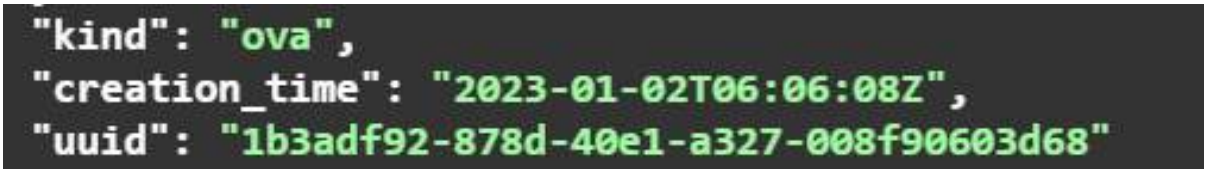


Figure 92: OVA Upload UUID

5. In the **REST API Explorer** browser tab, navigate to **ovas** > **Post /ovas/{uuid}/chunks/concatenate**, and click **Try it Out**.

6. Enter the UUID of the OVA in the **uuid** field, and click **Execute**.

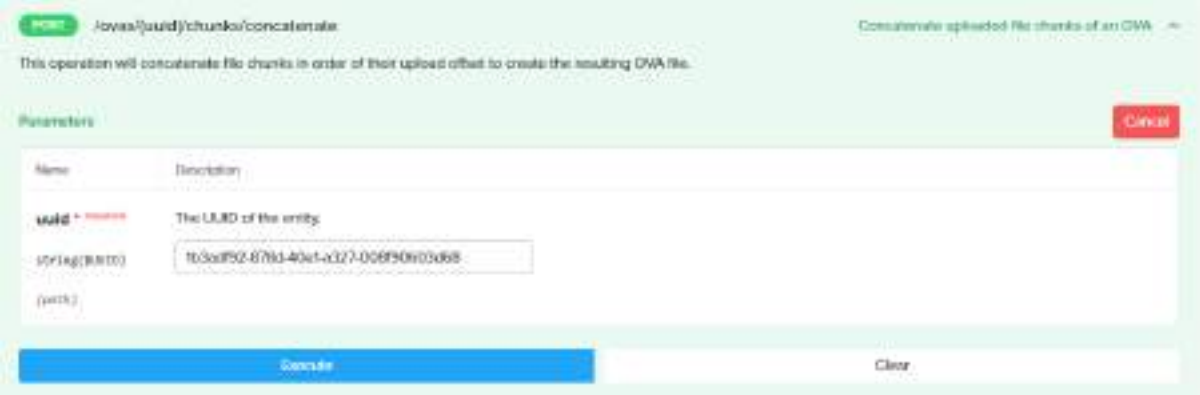


Figure 93: OVA Upload UUID

The **Response Code** field displays 202 indicating that the concatenation and validation request has been accepted.

Deploying an OVA as VM

About this task

This section describes how to deploy an OVA as VM.

> **Note:**
>
> For the OVAs that are not created from AHV, ensure that the pre-installed VirtIO drivers are available for them. For more information about VirtIO drivers, see Nutanix VirtIO for Windows in *AHV Administration Guide*.

To deploy an OVA as a VM, perform the following steps:

> **Note:** You can navigate back and forth between the steps using **Back** and **Next**.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **OVAs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **OVAs** page

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2704

3. Select the target OVA, and choose **Deploy as VM** from the **Actions** dropdown menu.
   The system displays the **Deploy as VM** window.

   You need to use the steps in the **Deploy as VM** window to configure the deployment.

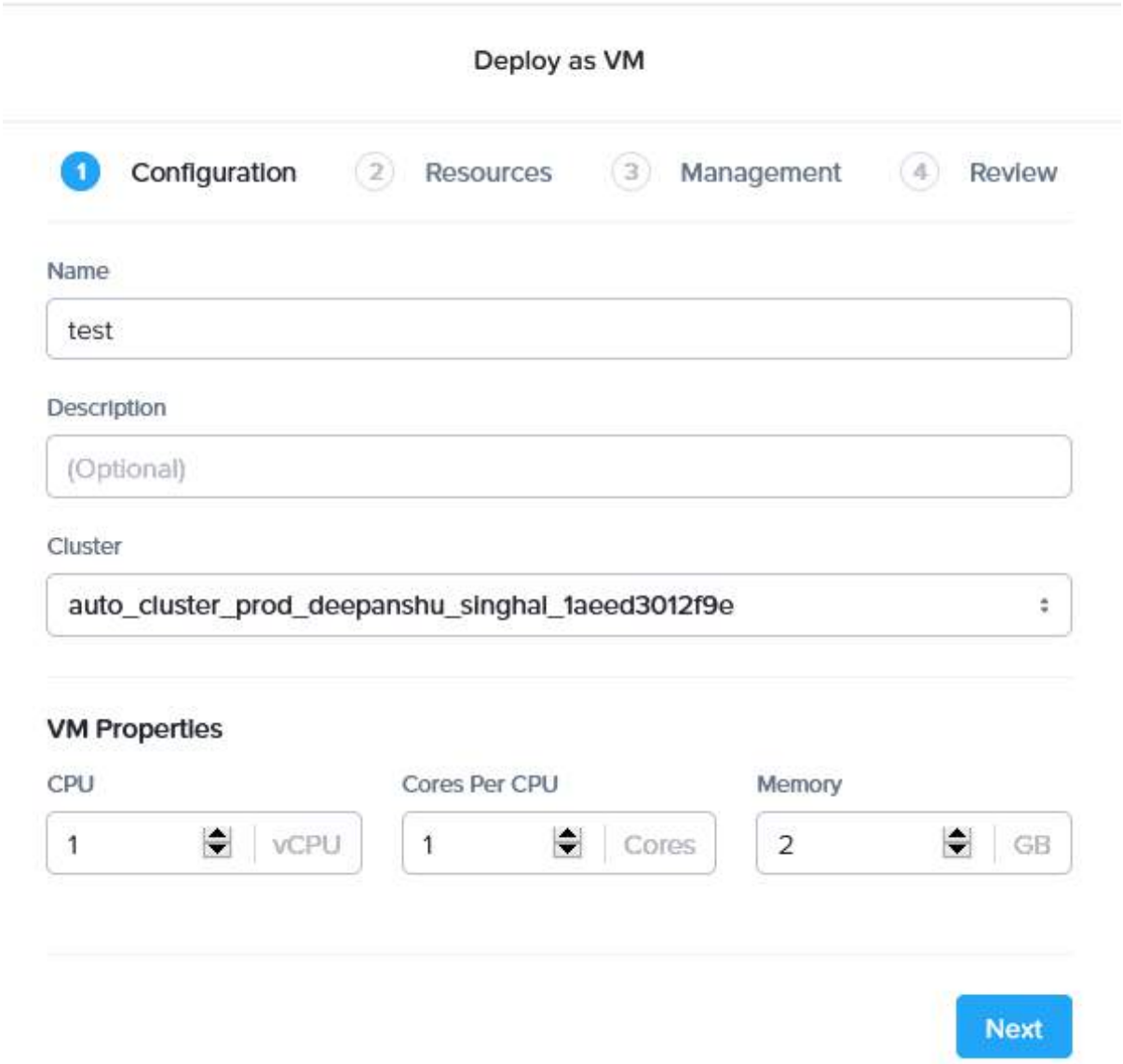


Figure 94: Deploy as VM - Configuration Step

4. In the **Deploy as VM** window, specify the following information in the **Configuration** step:

   a. **Name**: Enter the name of the VM that needs to be deployed.

   b. **Description**: Enter that description such as Backup VM for Prism.

   c. **Cluster**: Select one of the following options from the dropdown menu:

      - Target cluster on which you intend to place the guest VM.

        Only the clusters for which you have access and where OVAs are available, are displayed in the **Cluster** dropdown menu. By default, Prism Central selects a cluster in the dropdown menu for deployment.

      - **Automatic cluster selection**, if you intend to place the guest VM on a system-selected cluster. For more information, see Automatic Cluster Selection for VM Placement section in the *AHV Administration Guide*.

        > **Note:** Automatic cluster selection configuration for VMs with GPU specifications is not supported.

   d. **CPU**, **Cores Per CPU** and **Memory** in **VM Properties**: Specify the CPU and memory requirements as required.

   e. Click **Next**.
   The system displays the **Resources** step.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2706

5. Specify the following information in the **Resources** step:

> **Note:**
>
> You can add new disks, NICs and GPUs.

a. **Boot Configuration**: Select **UEFI Mode** only if your hardware supports UEFI boot mode, else select **Legacy BIOS Mode**.

b. **Set Boot Priority**: The default priority is already set.

c. **Attach Disk**: Used to attach additional disks in addition to the disks already available in the OVA.

In the **Attach Disk** window, specify the required information, and click **Save**.

For more information about how to attach a disk, see Creating a VM through Prism Central (AHV) on page 130.

d. **Attach to Network**: Used to attach the network.

In the **Attach to Network** window, select **Subnet** and **Network Connection State** from the dropdown menus.

For more information about how to configure network, see Creating a VM through Prism Central (AHV) on page 130.

e. Click **Add GPU** to add GPU resources.

> **Note:**
>
> - Automatic cluster selection configuration for VMs with GPU specifications is not supported. If you have selected the **Automatic cluster selection** option in step 4.c on page 235, the system does not provide you the option to add GPU.
> - If the selected cluster has GPU resources, then you can add multiple vGPUs to the same VM. Addition of multiple vGPUs is based on the installed GPU resources.

- For information about how to add multiple GPUs, see Adding Multiple vGPUs to the Same VM on page 156.
- For information about multiple vGPU support, see Multiple Virtual GPU Support information in *AHV Admin Guide*.

f. Click **Next**.
The system displays the **Management** step.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2707

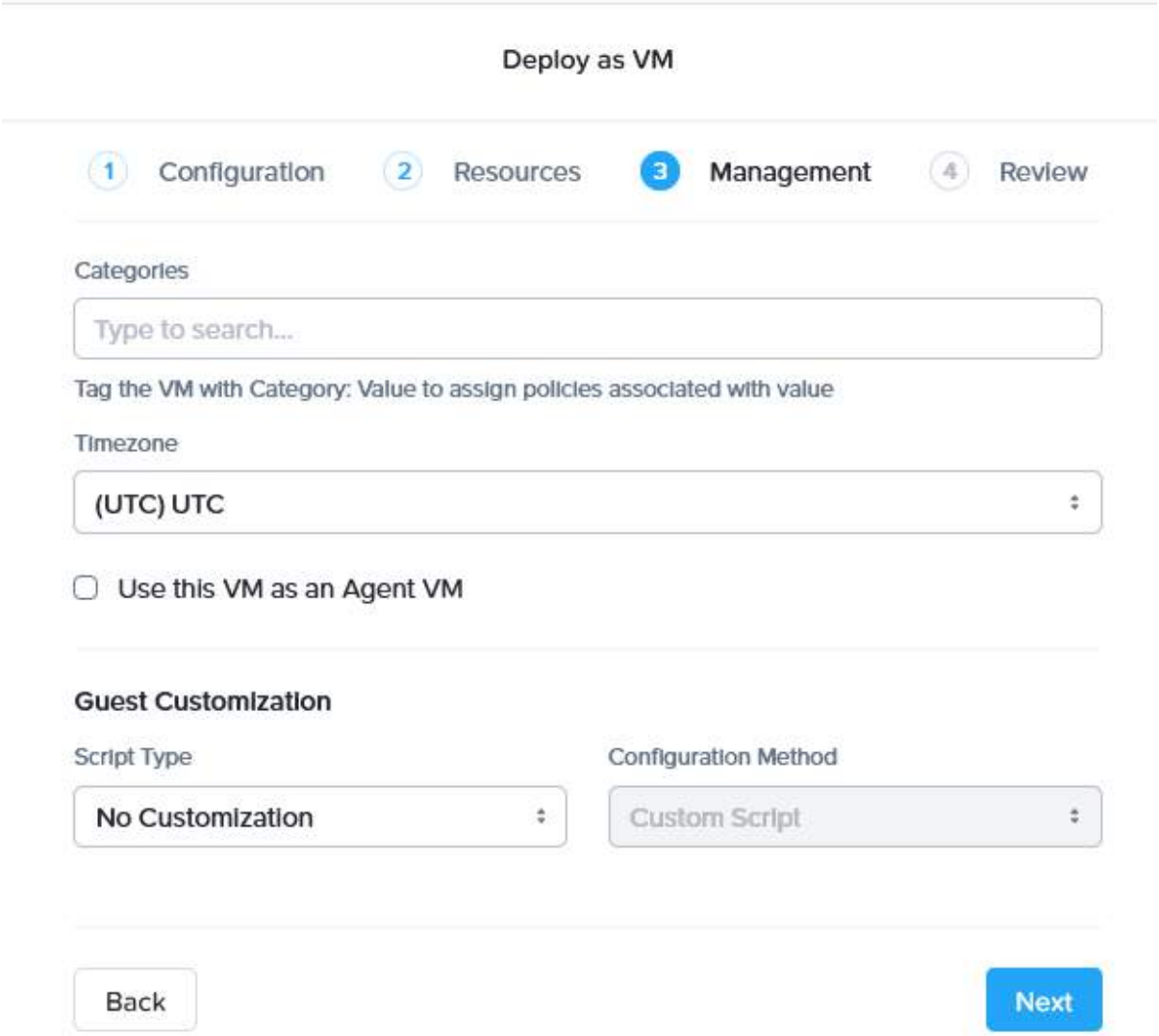


Figure 95: Deploy as VM - Management Step

g. **Categories**: Select the category to be mapped to the VM. Type in this field to display a list of available categories. For more information about categories, see Category Management on page 456.

h. **Timezone**: Select the appropriate timezone as per your requirement.

i. **Use this VM as an Agent VM**- Select this checkbox if you want to use the deployed VM as an agent VM.

j. **Guest Customizations**: Used to customize the VM. Select Cloud-init (for Linux VMs) or Sysprep (for Windows VMs).

Script Type: Select the VM script customization type from the dropdown menu. The options are `No Customization`, `Sysprep(Windows)`, or `Cloud-init (Linux)`.

Configuration Method: Select the VM script customization method from the dropdown menu. This field is activated when the **Script Type** is either `Sysprep(Windows)` or `Cloud-init (Linux)`. The options are `Custom Script` or `Guided Script`.

The system displays the options required to configure Cloud-init and Sysprep, such as options to specify a configuration script and option to upload script.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2708

k. To specify a user data file (Linux VMs) or answer file (Windows VMs) script for unattended provisioning, perform either of the following actions:

» If the file is available on your local computer, click **Upload Script**, choose and upload the file.

» Create or paste the contents of the file in the text box below the **Upload Script**.

> **Note:** The script type supports the following file formats.
>
> - Sysprep: XML
> - Cloud-init (Linux): YAML, JSON, or Shell.

l. Click **Next**.
The system displays the **Review** step.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2709

Deploy as VM

1 Configuration 2 Resources 3 Management 4 Review

Configuration

Name	test
CPU	1 vCPU
Cores Per CPU	1 Cores
Memory	2 GB

Resources

Disks

#	Type	Image	Size	Bus Type
1	Disk	-	0.94 GiB	SCSI
2	Disk	-	0.94 GiB	SCSI

Boot Configuration: Default Boot Order (CD-ROM, Disk, Network)

Networks

Subnet	Private IP
pc_network	Auto-Assign

Management

Categories	None
Timezone	UTC
Guest Customization	No Customization

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2710

6. Review the deployment configuration in the **Review** step, and Click **Launch** .
   You can check the progress of the deployment task in the **Tasks** page or from the Tasks icon. For information about **Tasks** page, see Tasks View on page 452.

Downloading an OVA

This section describes how to download an OVA on your local machine from Prism Central.

About this task

To download an OVA, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **OVAs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **OVAs** page.
3. Select the OVA to be downloaded, and choose **Download** from the **Actions** dropdown menu.
   The system displays the **Download** window.

   The following is an example showing the **Download** window:

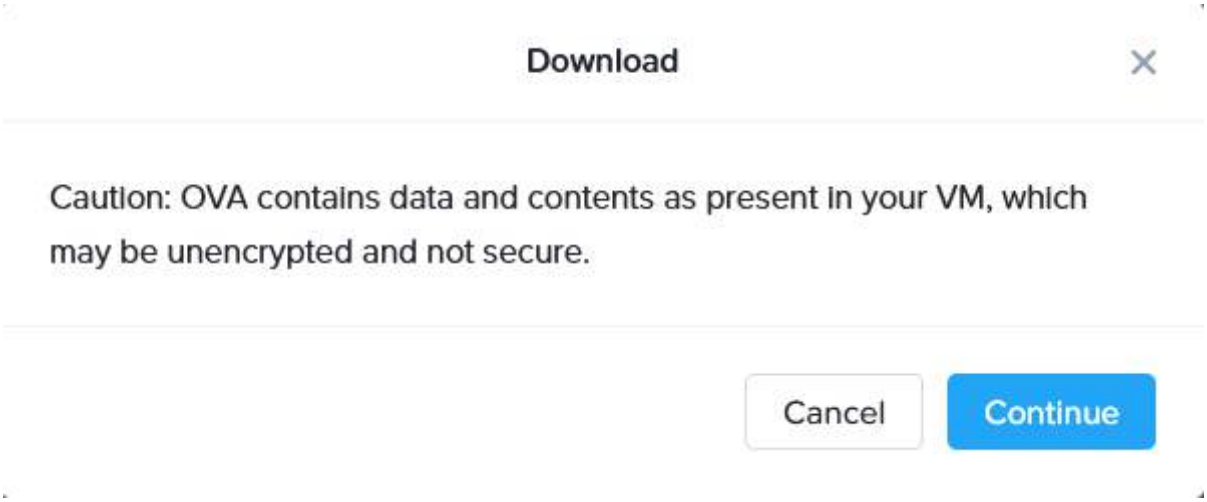


Figure 97: Download window

> **Note:** You can download up to five OVAs in parallel.

4. To confirm the download action, click **Continue**. To cancel the download action, click **Cancel**.

   The downloaded file is saved in a local folder based on your browser's download settings.

   Once the download starts, it continues even after you sign out from the console, as the TCP connection does not break. However, if you close the browser or the internet connection is interrupted, the download fails as the TCP connection breaks.

Renaming an OVA

This section describes how to rename an OVA in Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2711

About this task

To rename an OVA, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **OVAs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **OVAs** page
3. Select the OVA to be renamed, and choose **Rename** from the **Actions** dropdown menu.
   The system prompts you to update the new name for the OVA file.

   The following is an example showing the **Rename** window:

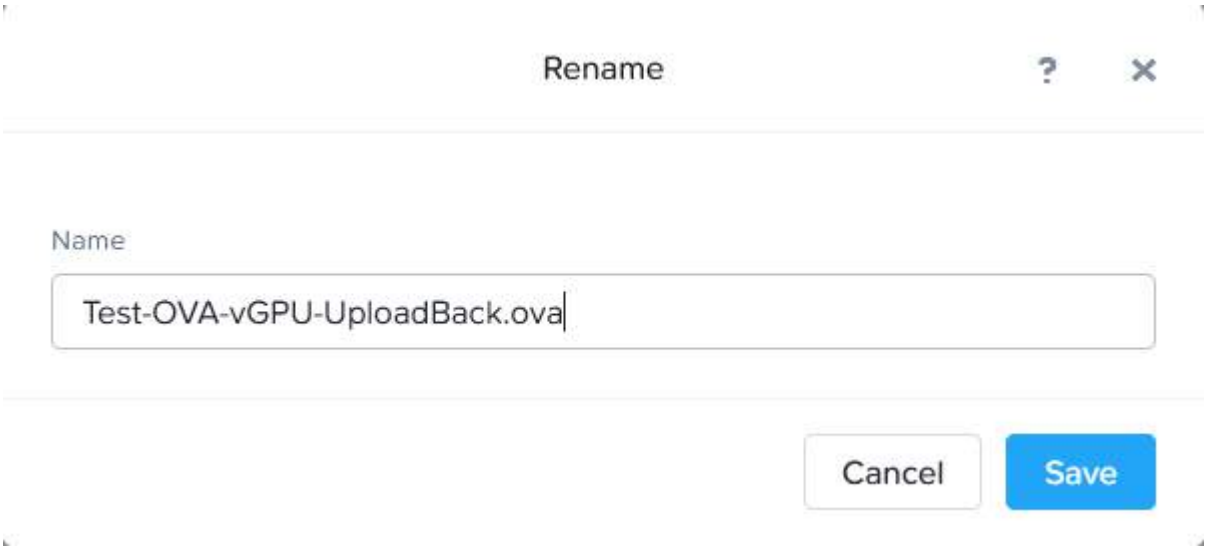


Figure 98: Rename window

4. Delete the old name and enter the new name in the **Name** field.
5. To confirm the rename action, select **Save**.
   To cancel the rename action, select **Cancel**.

Deleting an OVA

This section describes how to delete an OVA in Prism Central.

About this task

To delete an OVA, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **OVAs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **OVAs** page.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2712

3. Select the OVA to be renamed, and choose **Delete** from the **Actions** dropdown menu.
   The system prompts you to confirm the delete action.

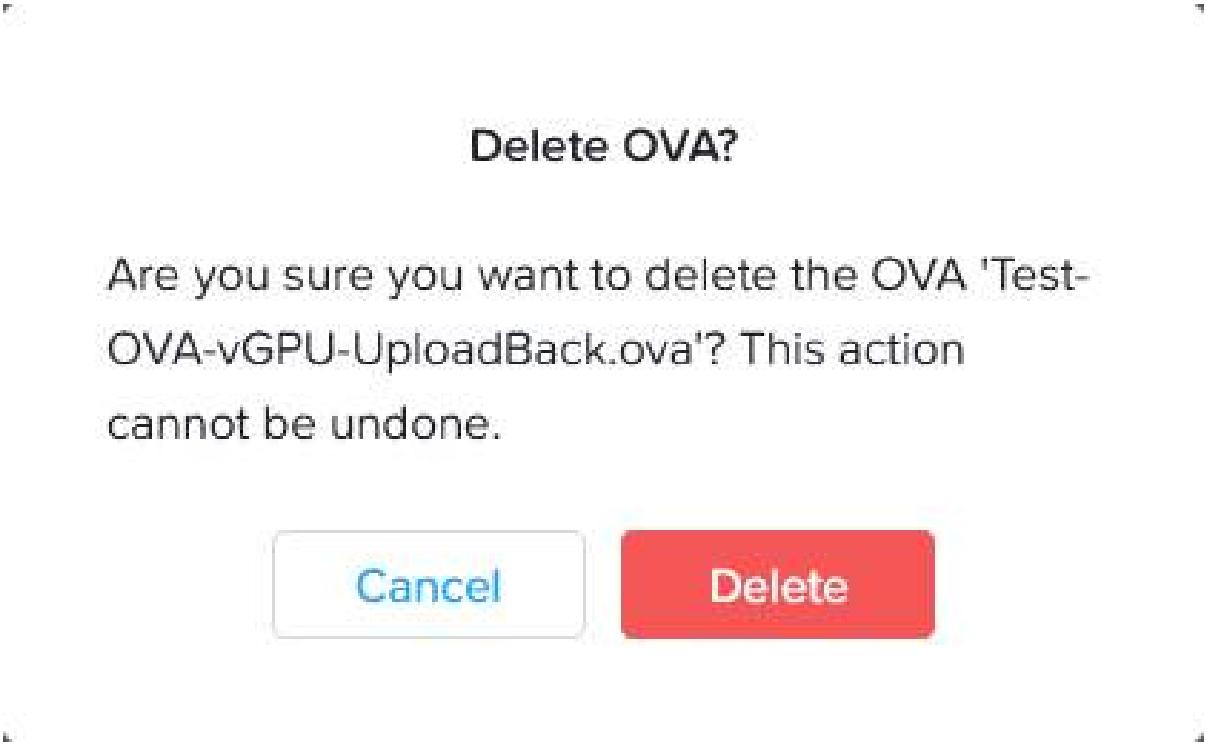


Figure 99: Delete OVA window

4. To confirm the delete action, select **Delete**.
   To cancel the delete action, select **Cancel**.

> **Note:** The **Delete** action deletes the OVA permanently. You cannot recover a deleted OVA.

Image Management

Prism Central provides a centralized location to manage the images you require on registered AHV clusters. You can upload images to the clusters and maintains an inventory of the images on it.

> **Note:**
>
> - You can configure policies that govern the image placement process. These policies allow you to specify the clusters on which the images need to be uploaded. For more information about the image placement policies, see Image Placement Policies on page 488.
> - You can also update the uploaded images. For more information, see Modifying an Image on page 264

Image Source

In Prism Central, you can add images from the following sources:

- Workstation. For more information, see Adding Images from a Workstation on page 248.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2713

- URLs to images on a remote server. For more information, see Adding Images from a Remote Server on page 253.
- VM disk. For more information, see Adding Images from a VM Disk on page 257.

For information about these sources, see Adding an Image on page 248.

Image Placement Methods

When you add images, the system provides you the following image placement methods:

- Select target clusters during images upload, and place image directly on the target clusters.
- Specify target clusters using image placement policies, and place images on the target clusters based on image placement policies.

  In this case, you can select the image categories, and the system uploads images to all the registered clusters mapped to the image categories in image placement policy. For information about image placement policies, see Image Placement Policies on page 488.

  > **Note:** You can also suspend or resume the image placement policies based on your requirement. For more information, see Suspending or Resuming Enforcement of an Image Placement Policy on page 262

For information about how to add images, see Adding Images from a Workstation on page 248 and Adding Images from a Remote Server on page 253.

Images Import from Registered Clusters to Prism Central

In addition to the sources defined in Image Source on page 242, you can also import images from registered AHV clusters. You can import images only from registered clusters that are running AOS 5.8 or later. For more information, see Importing Images to Prism Central on page 265.

Images Summary View

The **List** tab in **Images** page displays the information about all the images across registered clusters.

> **Note:** This section describes the information and options that appear in the **Images** page.
>
> - See Prism Central GUI Organization on page 54 for instructions on how to view and organize that information in various ways.
> - See Image Management on page 242 for information about how to add and manage images through Prism Central.
> - See Image Placement Policies on page 488 for information about image placement policies.
> - See Bandwidth Throttling Policies on page 496 for information about bandwidth throttling policies.

To access the summary view of all images, perform the following steps:

1. Log in to Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2714

2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The system displays the **List** tab by default.

   The following is an example showing the **List** tab in **Images** page:

Figure 100: List tab - Images

The following table describes the fields that appear in the **List** tab in **Images** page:

> **Note:** A dash (-) is displayed in a field when a value is not available or not applicable.

Table 43: Images Page - Field Description

Parameter	Description	Values
Name	Displays the image name. Click the image name to view the detailed information about that image. For more information, see, Image Details View on page 246	<Image name>
Description	Indicates which user uploaded this image.	(text string)
Type	Displays the image type.	ISO, Disk
Size	Displays the image size.	x [MB|GB], where x is numeric digit.
Creator	Displays who created the image.	<user>. For example admin

You can perform the following actions for the images in the **List** tab:

- Access the detailed information about an individual image. For more information, see Image Details View on page 246.
- Filter the images list based on available parameter values using **Filters** pane. For more information about **Filters** pane, see Filters Pane - Images on page 245.
- Export the table that contains the list of images and their information to a file in a CSV format. For more information about **Export** option, see Export on page 59.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2715

- Group the images based on pre-defined criteria. For information about how to group the images, see Group by on page 56.
- View images based on pre-defined criteria or create a custom view. For information about available views and how to create a custom view, see View by on page 56.
- Perform the following image-specific actions on a single or multiple images using the **Actions** dropdown menu:
  - **Update** - Used to update the image file attributes. For details, see Modifying an Image on page 264.
  - **Delete** - Used to delete the image. Select the image(s), and choose **Delete** from the **Actions** dropdown menu.
  - **Add Image to Catalog** - Used to add an image to the catalog. For more information, see Modifying an Image on page 264.

    For information on how to manage the catalogs, see Catalog Management on page 266.
  - **Manage Categories** - Used to assign a category to the images. For information about how to manage image categories , see Modifying an Image on page 264.
  - **Download Image** - Used to download the image. Select the image, and choose **Download Image** from the **Actions** dropdown menu.

    The downloaded image does not have any file extension. If you download an .ISO image, you must rename the file to append .ISO extension before using the image. A downloaded disk image is in raw format and you must manually convert it using *qemu-img* or similar tool before using the disk image.

    The Image download speed is dependent on the following factors:

    - Bandwidth between Prism Element where image is stored and Prism Central
    - Bandwidth between Prism Central and client system

    Note: You can also perform these actions from the **Summary** page of an individual image. For more information, see Image Details View on page 246.

Filters Pane - Images

You can filter the information in the **Images** page based on the following fields that are available in the **Filters** pane. For information about how to use **Filters** option in Prism Central, see Prism Central GUI Organization on page 54.

Table 44: Filter Pane Field Description - Images page

Field	Description	Values
Name	Filters based on the image name. It returns a list of storage containers that satisfy the name condition/ string.	*<Image name >*
Description	Filters based on the image description.	(description string)
Type	Filters based on the image type. Check the box(es) for the desired image types.	Disk, ISO

Policies Tab

The **Policies** tab displays **Placement Policies** and **Bandwidth Throttling Policies**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2716

- For information about how to configure **Placement Policies**, see Image Placement Policies on page 488.
- For information about how to configure **Bandwidth Throttling Policies**, see Bandwidth Throttling Policies on page 496.

Image Details View

To access the details view of an individual image, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The system displays the **List** tab by default.
3. Click the <*Image_Name*> to view the **Summary** tab of an individual image.

> **Note:** Replace <*Image_Name*> with the actual image name at your site.

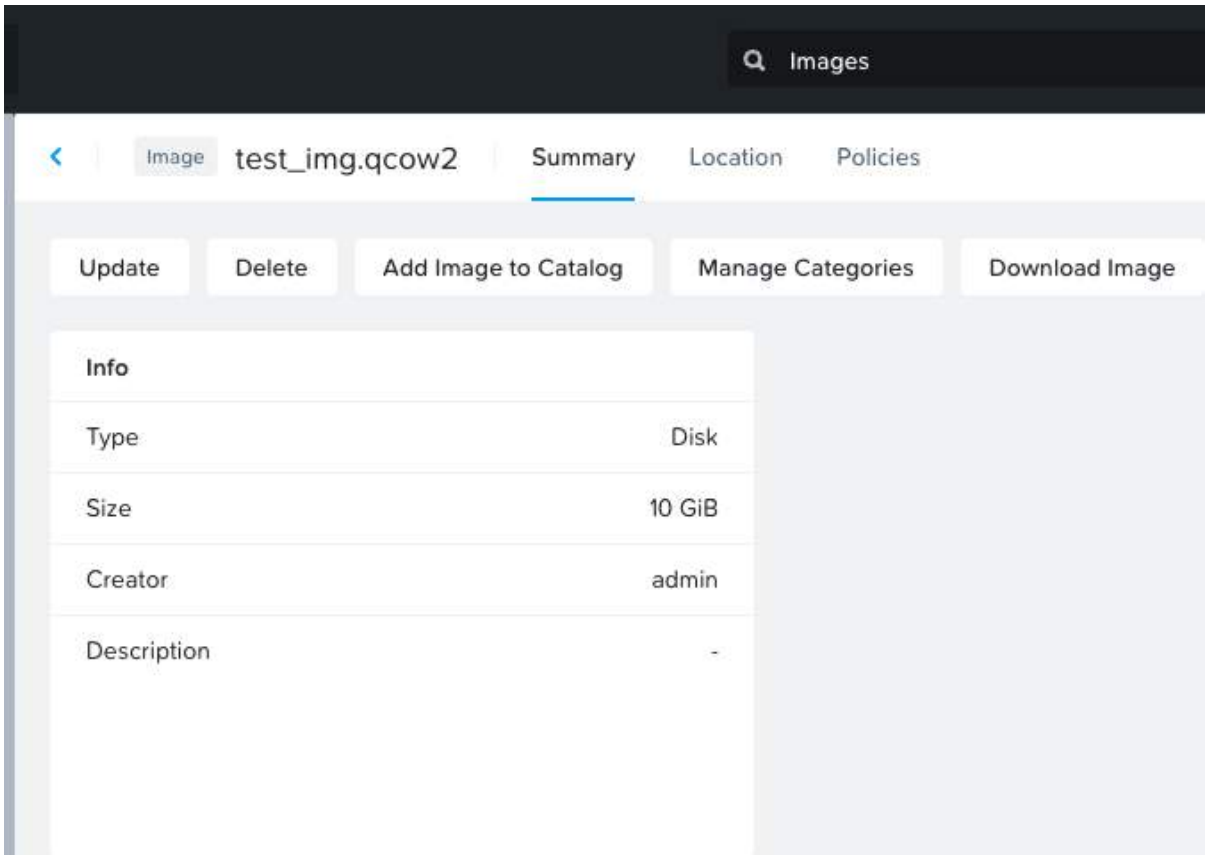


Figure 101: Image Details View (Summary Tab)

For information about the fields available in **Info** widget, see Images Summary View on page 243.

Location Tab

The following table describes the information displayed in the **Location** tab

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2717

Table 45: Location Tab -Field Description

Field	Description	Values
Name	Displays the name of the cluster in which the image is stored. Each row represents another cluster that contains the image.	*<Cluster name>*
AOS Version	Displays the AOS version running in the cluster.	*AOS version number*
Hypervisor	Displays the name of the hypervisor running in the cluster.	AHV, ESXi, Hyper-V
Host Count	Displays the number of hosts in the cluster.	(integer)
VM Count	Displays the number of VMs in the cluster	(integer)

Policies Tab

The **Policies** tab lists the policies that apply to the selected image. For information about the image-related policies, see Image Policy Management on page 487.

- For information about how to configure **Placement Policies** for images, see Image Placement Policies on page 488.
- For information about how to configure **Bandwidth Throttling Policies** for images, see Bandwidth Throttling Policies on page 496.

Requirements

You must meet the following requirements to access the image management feature in Prism Central:

- The version of both Prism Central and AOS on registered clusters is 5.8 or later.
- Clusters is registered with Prism Central with AHV installed in it.
- The port 2007 must be open for the image service.

Limitations

The following limitations apply to the image management feature in Prism Central:

- You cannot update images that another Prism Central instance managed earlier. However, the images are displayed in Prism Central, and you can use the images to create VMs or delete the images you no longer need.
- You cannot choose a container when uploading images from Prism Central. Prism Central uploads images to the container named `SelfServiceContainer`.
- When you upload images from a workstation and place the images on multiple clusters during the initial image upload, the uploaded image becomes active (in Prism Element) on only one of the selected clusters and remains inactive on the other clusters registered to Prism Central.
- If you add a new cluster that contains images to an existing Prism Central, you must first import the images to Prism Central and then use the image placement policies to push the images to any other cluster already registered with Prism Central.
- If an image is not active on a cluster, as an admin user it is possible that you are unable to use Prism Central to create that VM on that cluster. The cluster on which you want to create the VM cannot check out the image from

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2718

a remote cluster. In this scenario, you must upload the image manually to the cluster on which you want to create the VM.

When you create a VM, Prism Central uses API v2 workflows. API v2 does not have the checkout workflow. The image checkout workflow is used to copy an image on demand from cluster B to cluster A if the image does not exist or is inactive on cluster A.

> **Note:**
>
> You can remove this limitation using an image placement policy. Assign a category to the image that is available on multiple remote clusters, and apply the image placement policy to the image category. When you apply the image placement policy to a image, Prism Central propagates the image to all the clusters that are included in the image placement policy. Prism Central can then checkout the image from the remote cluster where the image is active and create the VM.
>
> The system can take up to 15 minutes to switch the image propagation from an alternative cluster. For example, if an image is located on clusters A and B. As a result of an image placement policy you applied to that image, cluster A starts copying the image to cluster C. During the copy operation, if cluster A becomes unavailable, the system takes up to 15 minutes to switch to cluster B, and starts copying the image from cluster B to cluster C.

Adding an Image

This section describes how to add an image in Prism Central.

About this task

You can add the images in Prism Central from any of the following sources:

Procedure

- Workstation, see Adding Images from a Workstation on page 248.
- Remote Server, see Adding Images from a Remote Server on page 253.
- VM disk, see Adding Images from a VM Disk on page 257.

Adding Images from a Workstation

This section describes how to add (or upload) the images in Prism Central from the workstation that you use to access Prism Central.

About this task

> **Note:**
>
> - By default, the system selects all the clusters. The system also provides you the option to clear the cluster as per your requirement.
> - The image becomes active (in Prism Element) on the selected cluster and inactive on other clusters registered to Prism Central.
> - Image placement policies, if applied, take effect after a short duration.
> - Most modern browsers impose file size limitations that affect this upload method. If you intend to upload images larger than 2 GB, Nutanix recommends you to upload the images from a remote server.
> - The browser type, and CPU and RAM utilization on the workstation limit the number of concurrent uploads. Concurrent uploads that exceeds the default limit of the browser are queued or throttled by the browser and can consume more time.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2719

- Large file uploads, and high CPU and memory utilization can slow down the browser.

To upload an image from a workstation, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2720

3. Click **Add Image**.
   The system displays the **Add Images** window.

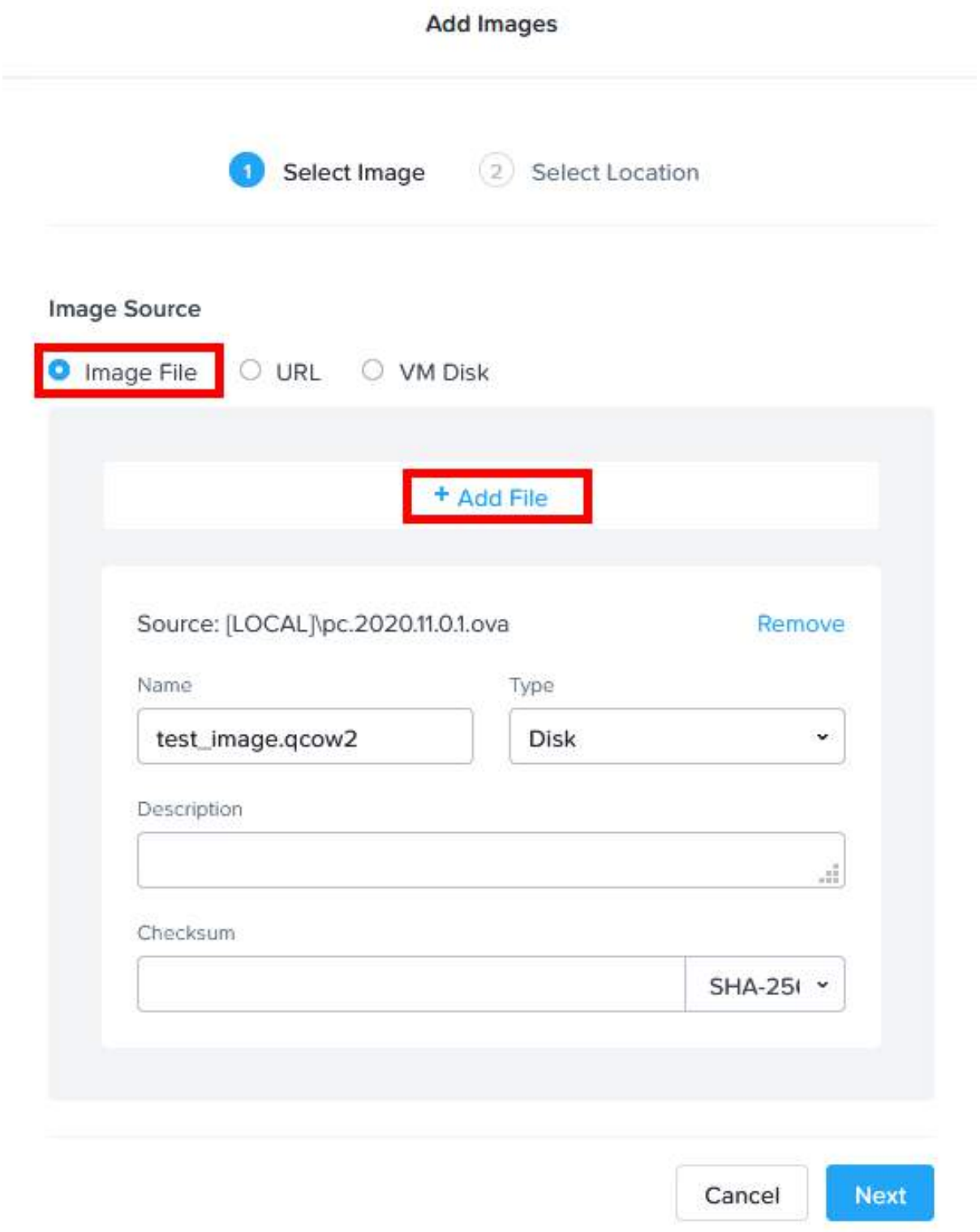


Figure 102: Add Images: File

4. Specify the following information in the **Select Image** step:

   a. **Image Source** - Select **Image File** radio button.

   b. Click **Add File**. The system displays the file attributes.

   c. Browse to the location of the image file, and then click **Open**.

   d. Specify the following attributes for the image file:

      - **Image Name** - Enter the image name. By default, the system pre-fills the name of the file you selected, however you can change the image name as per your requirement.

        Note: Ensure that the name of the image is unique across all the images in Prism Central.

      - **Image Type** - Select the type of image.
      - **Image Description** - Enter the description for the image file.
      - **Checksum** - Select the hashing algorithm.

   e. Repeat step b to step d if you want to add multiple image files.

      To remove an image file entry, locate the entry and click **Remove**.

   f. Click **Next** after you add all the image files.
      The system displays the **Select Location** step.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2722

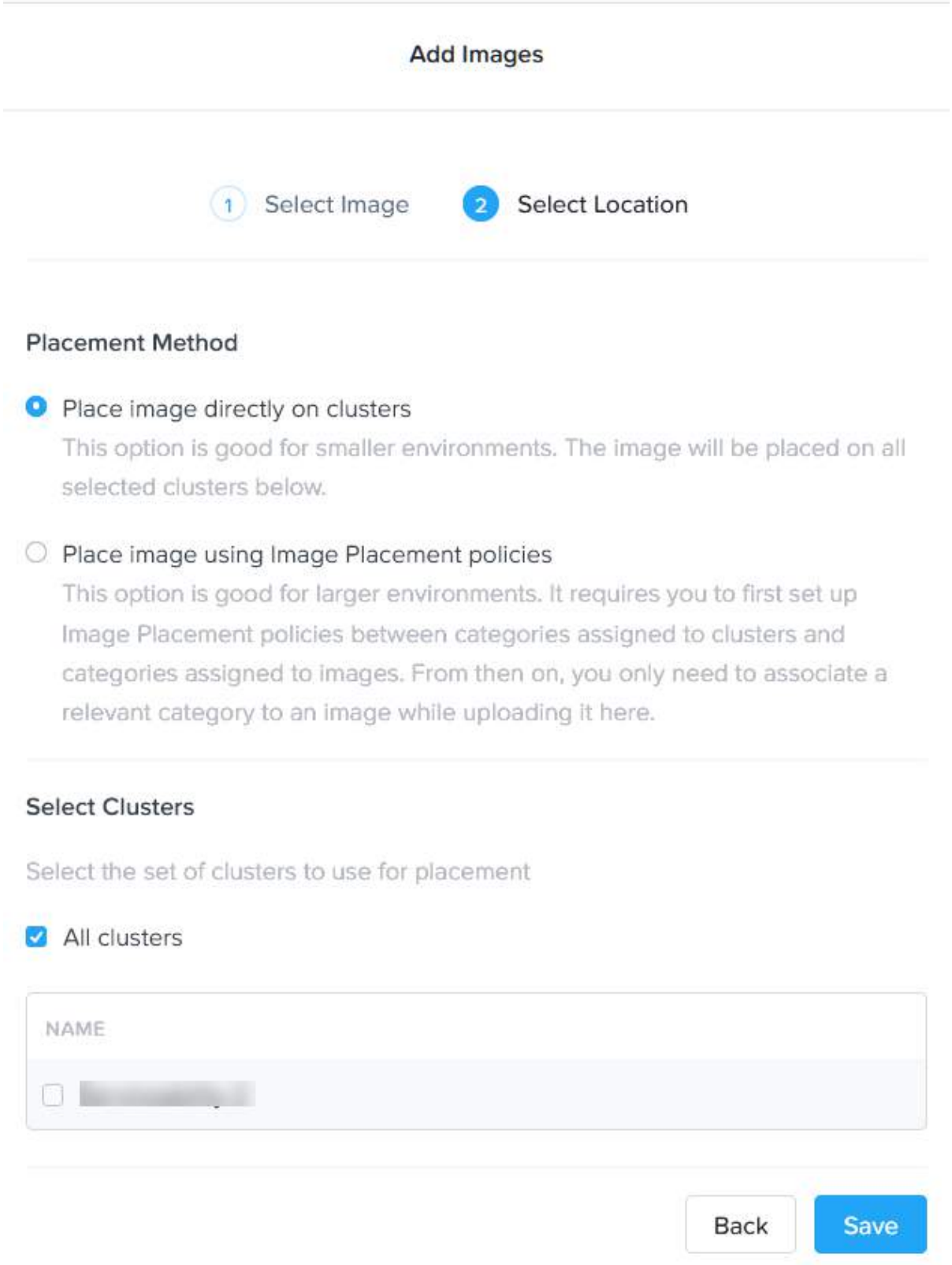


Figure 103: Add Images: Select Location

5. Specify the following information in the **Select Location** step:

   a. **Placement Method** - Select one of the following placement methods:.

   - **Place image directly on clusters**- Used to place the images directly o the selected clusters.
   - **Place image using Image Placement policies** - Used to delegate image placement decisions to configured policies and assign categories to the images

   b. If you select:

   - **Place image directly on clusters** - Specify the following information:

     Select Clusters - Select the clusters in which you want to add the image file in the **Name** column.

     Note:

     - By default, the system selects all the registered clusters.
     - If you want to add the images to all registered clusters, ensure that you select all the clusters in the **Name** column.
     - If you want to upload to only a subset of the registered clusters, clear all clusters in the **Name** column, and only select the clusters you want from the list.

   - **Place image using Image Placement policies** - Specify the following information:

     Select Image Categories - Click inside the search box and select the category you want from the list. You can also type the name of the category to reduce the list to matching names.

     Note:

     - To select multiple categories, click Add icon beside each category name that you want to include in the categories.
     - To remove a category, click Remove icon beside each category name that you want to remove from the selected categories.
     - For information about how to create a category and assign a category value to an image, see Creating a Category on page 459 and Associating Images with Categories on page 491.

6. Click **Save**.
   The system adds the image files in batches and takes some time to enforce the image placement policies (if selected).

   Note: You can also suspend or resume the image placement policies based on your requirement. For details, see Suspending or Resuming Enforcement of an Image Placement Policy on page 262.

Adding Images from a Remote Server

You can add an image from a remote server to registered Nutanix clusters. To add an image from a remote server, you need the URL of the image. You can also specify URLs to multiple images as part of a single operation. When you specify image URLs, Prism Central adds the images to all registered clusters. Adding the image from a remote server also allows you to overcome file size limitations imposed by modern browsers. The file size limitation is usually 2 GB.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2724

About this task

To add an image from a remote server, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default.
3. Click **Add Image**.
   The system displays the **Add Images** window.

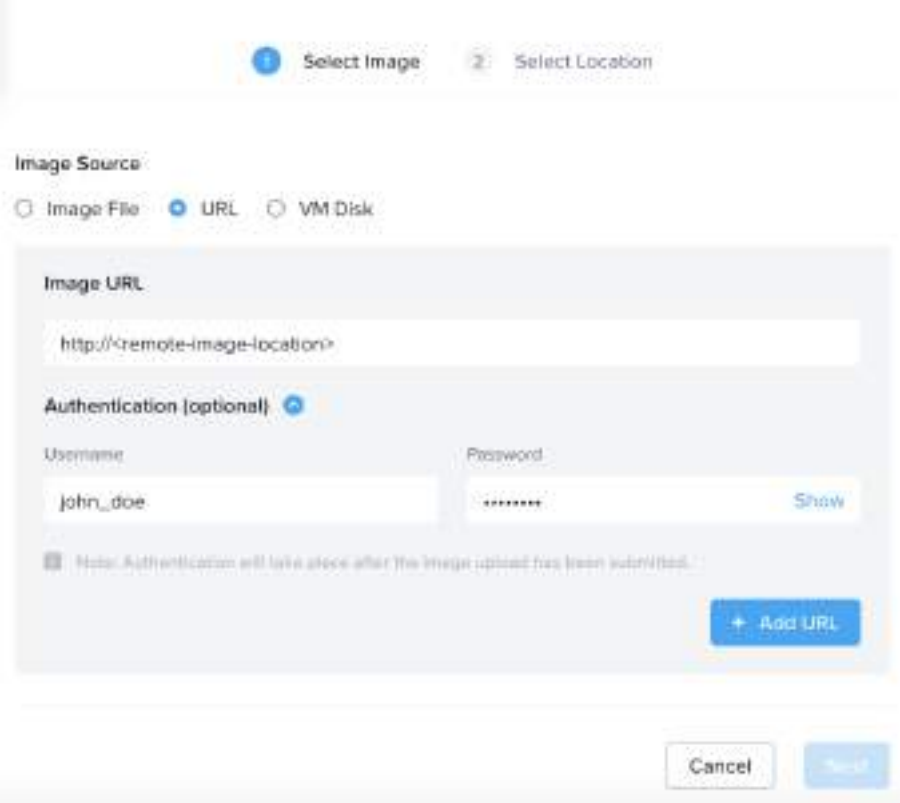


Figure 104: Add Images: URL

4. Specify the following information in the **Select Image** step:
   a. **Image Source** - Select **URL** radio button.
   b. **Enter Image URL** - Enter the appropriate URL address in the field using the following syntax for either NFS or HTTP, and then click **Upload File**.

      Note: The system supports only NFS and HTTP protocols.

      ```
      nfs://[hostname|IP_addr]/path
      ```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2725

`http://[hostname|IP_addr]/path`

Enter either the name of the host (*hostname*) or the host IP address (*IP_addr*) and the path to the file. If you use a *hostname*, the cluster must be configured to point at a DNS server that can resolve that name. For more information, see Configuring Name Servers for Prism Central in *Prism Central Admin Center Guide*.

> **Note:** A file uploaded through NFS must have 644 permissions.

c. Optionally, if the remote image location requires authentication credentials, enter the **Username** and **Password**, then click **Next**.

> **Note:** The authentication is validated after the image upload request is submitted.

d. Specify the following attributes for the image file:

- **Image Name** - Enter the image name. By default, the system pre-fills the name of the file you selected, however you can change the image name as per your requirement.

  > **Note:** Ensure that the name of the image is unique across all the images in Prism Central.

- **Image Type** - Select the type of image.
- **Image Description** - Enter the description for the image file.

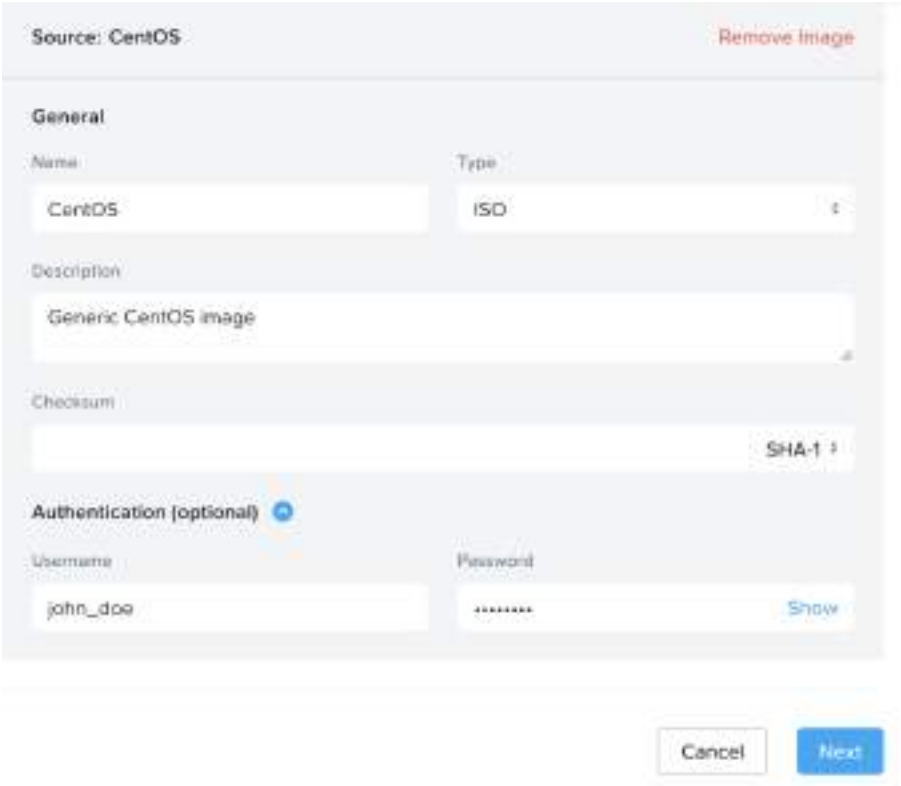


Figure 105: Add Image Attributes: URL

e. Repeat step b to step c if you want to add multiple image files.

To remove an image file entry, locate the entry and click **Remove**.

f. Click **Next** after you add all the image files.

The system displays the **Select Location** step.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2726

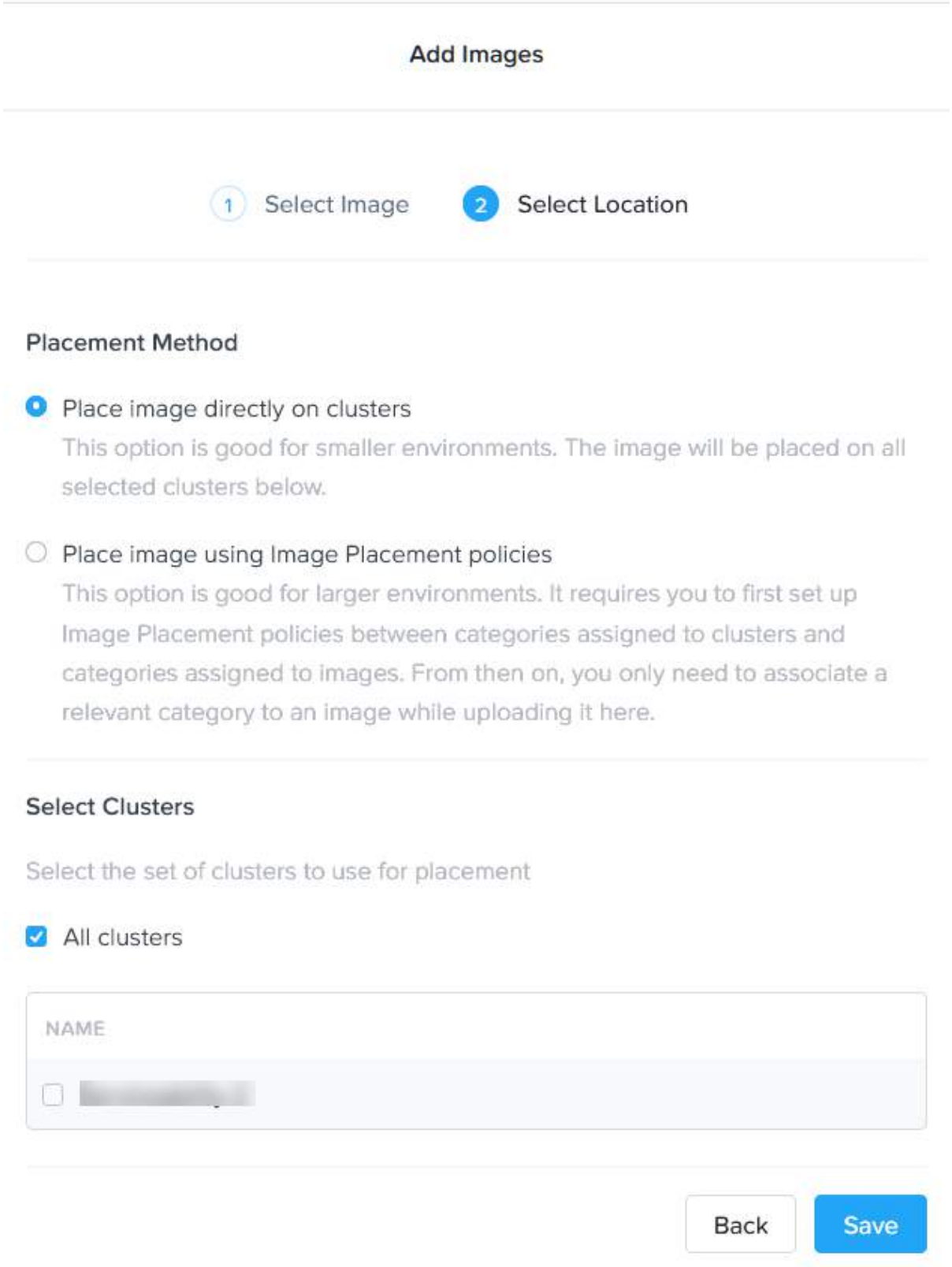


Figure 106: Add Images: Select Location

5. Specify the following information in the **Select Location** step:

   a. **Placement Method** - Select one of the following placement methods:.

   - **Place image directly on clusters**- Used to place the images directly o the selected clusters.
   - **Place image using Image Placement policies** - Used to delegate image placement decisions to configured policies and assign categories to the images

   b. If you select:

   - **Place image directly on clusters** - Specify the following information:

     Select Clusters - Select the clusters in which you want to add the image file in the **Name** column.

     Note:

     - By default, the system selects all the registered clusters.
     - If you want to add the images to all registered clusters, ensure that you select all the clusters in the **Name** column.
     - If you want to upload to only a subset of the registered clusters, clear all clusters in the **Name** column, and only select the clusters you want from the list.

   - **Place image using Image Placement policies** - Specify the following information:

     Select Image Categories - Click inside the search box and select the category you want from the list. You can also type the name of the category to reduce the list to matching names.

     Note:

     - To select multiple categories, click Add icon beside each category name that you want to include in the categories.
     - To remove a category, click Remove icon beside each category name that you want to remove from the selected categories.
     - For information about how to create a category and assign a category value to an image, see Creating a Category on page 459 and Associating Images with Categories on page 491.

6. Click **Save**.
   The system adds the image files in batches and takes some time to enforce the image placement policies.

   Note: You can also suspend or resume the image placement policies based on your requirement. For more information, see Suspending or Resuming Enforcement of an Image Placement Policy on page 262.

Adding Images from a VM Disk

This section describes how to add an image from a VM disk on the registered cluster.

Before you begin

Ensure that the following prerequisites are met before you add an image from a VM disk.

- The source VM belongs to an AHV cluster.
- The source VM on which the disk resides is in the powered-off state.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2728

- To place the image on clusters associated with relevant categories, you must first set up the image placement policies between categories assigned to clusters and categories assigned to images.

  For information about how to create a category and assign a category value to an image, see Creating a Category on page 459 and Associating Images with Categories on page 491.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2729

3. Click **Add Image**.
   The system displays the **Add Images** window.

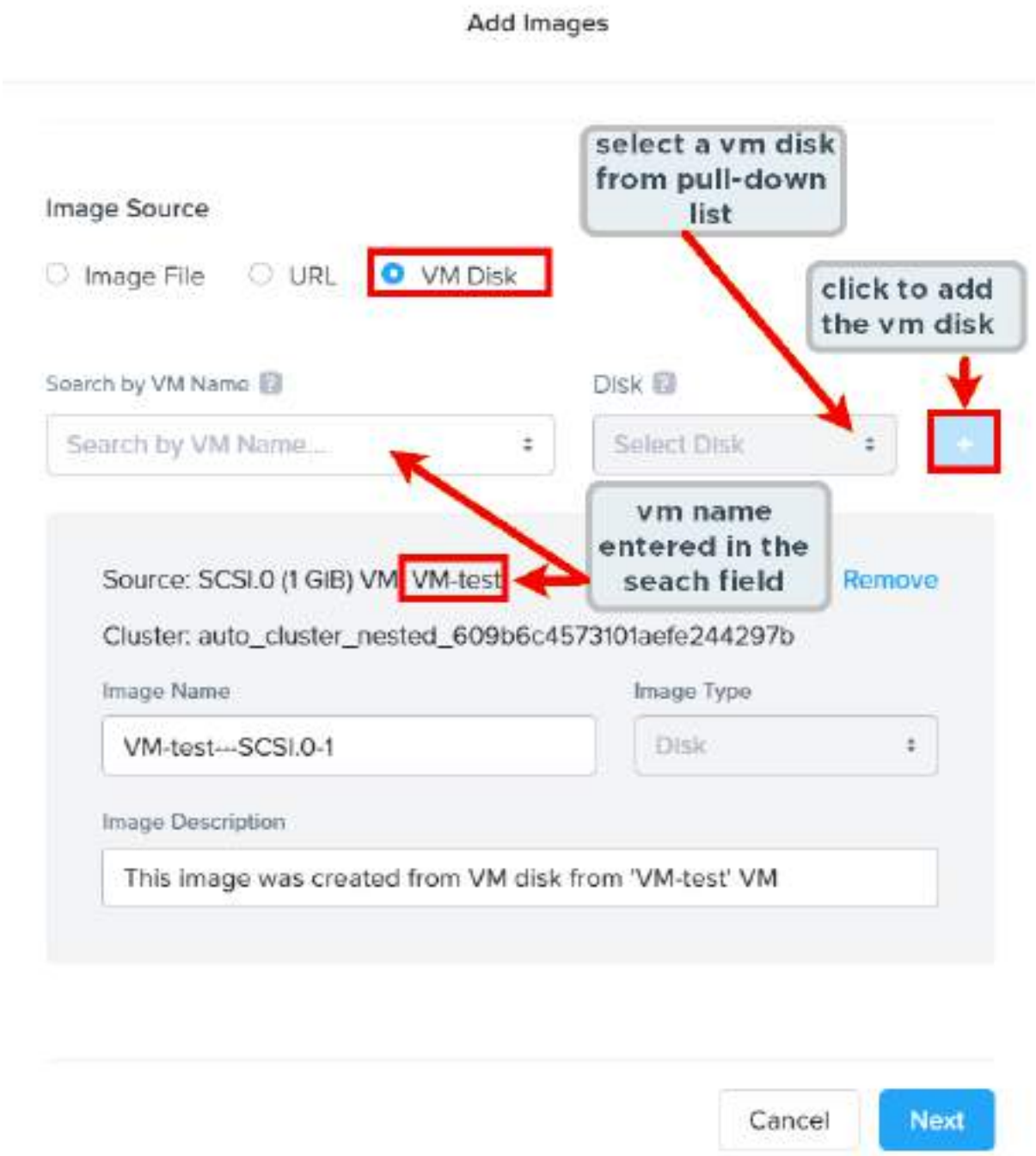


Figure 107: Add Images: VM Disk

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2730

4. Specify the following information in the **Select Image** step:

   a. **Image Source** - Select **VM Disk** radio button.

   b. **Search by VM Name** - Click inside this field text box, and select the target VM from the displayed list. The list displayed consists of all the powered-off VMs in the cluster.
   The system adds the VM to a list and populates the list of disks attached to this VM in the **Disks** dropdown list.

   c. Select the target disk from the **Disks** dropdown list, and click the Add icon,
   The system displays the disk, and cluster information of the VM source.

   d. Specify the following attributes for the image file:

      - **Image Name** - Enter the image name. By default, the system pre-fills the name of the file you selected, however you can change the image name as per your requirement.

        Note: Ensure that the name of the image is unique across all the images in Prism Central.

      - **Image Type** - Select the type of image.
      - **Image Description** - Enter the description for the image file.

   e. Repeat step b to step d if you want to add multiple image files.

      To remove an image file entry, locate the entry and click **Remove**.

   f. Click **Next** after you add all the image files.
      The system displays the **Select Location** step.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2731

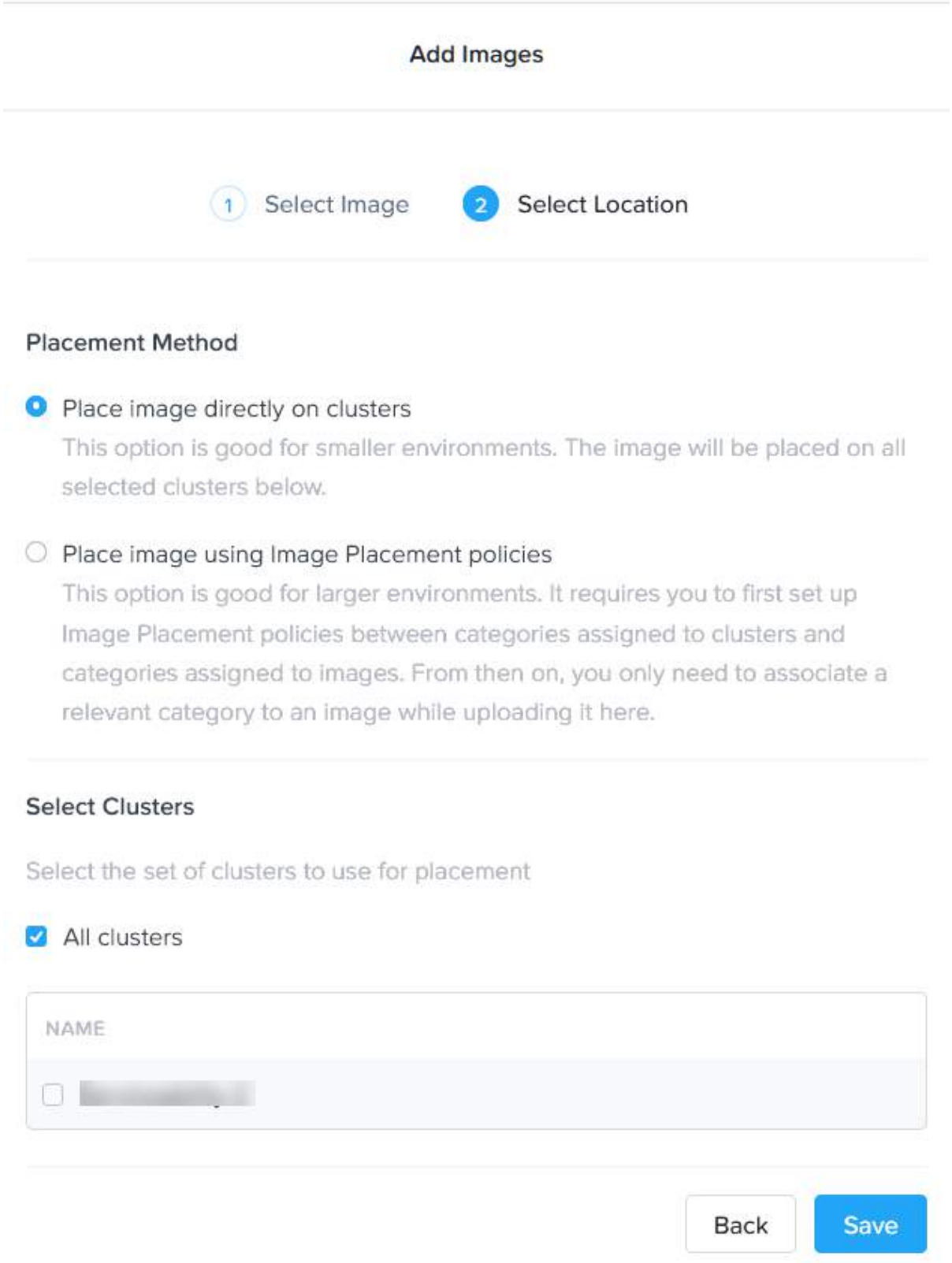


Figure 108: Add Images: Select Location

5. Specify the following information in the **Select Location** step:

   a. **Placement Method** - Select one of the following placement methods:

   - **Place image directly on clusters**- Used to place the images directly o the selected clusters.
   - **Place image using Image Placement policies** - Used to delegate image placement decisions to configured policies and assign categories to the images

   b. If you select:

   - **Place image directly on clusters** - Specify the following information:

     Select Clusters - Select the clusters in which you want to add the image file in the **Name** column.

     Note:

     - By default, the system selects all the registered clusters.
     - If you want to add the images to all registered clusters, ensure that you select all the clusters in the **Name** column.
     - If you want to upload to only a subset of the registered clusters, clear all clusters in the **Name** column, and only select the clusters you want from the list.

   - **Place image using Image Placement policies** - Specify the following information:

     Select Image Categories - Click inside the search box and select the category you want from the list. You can also type the name of the category to reduce the list to matching names.

     Note:

     - To select multiple categories, click Add icon beside each category name that you want to include in the categories.
     - To remove a category, click Remove icon beside each category name that you want to remove from the selected categories.
     - For information about how to create a category and assign a category value to an image, see Creating a Category on page 459 and Associating Images with Categories on page 491.

6. Click **Save**.
   The system adds the image files in batches and takes some time to enforce the image placement policies.

   Note: You can also suspend or resume the image placement policies based on your requirement. For more information, see Suspending or Resuming Enforcement of an Image Placement Policy on page 262.

Suspending or Resuming Enforcement of an Image Placement Policy

This section describes how to suspend or resume the enforcement of an Image Placement Policy in Prism Central.

Before you begin

The minimum supported versions to suspend or resume the enforcement of an image placement policy in Prism Central are AOS 6.6 for Prism Element (with bundled AHV version) and PC 2022.9 for Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2733

About this task

Enforcement of placement policy involves copying images between clusters using image data transfer tasks that are typically long-running tasks and consume a considerable amount of network bandwidth. If you need to manage your local bandwidth and resources while the enforcement of the image placement policy is still going on, you can suspend the enforcement of the image placement policy, and can resume the enforcement at a later point of time.

To suspend or resume the enforcement of an image placement policy, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default.
3. Select **Placement Policies** in the **Policies** tab.

   The following is an example showing the placement policies view:

Figure 109: Placement Policy View

4. Select the target policy checkbox for which you want to suspend or resume enforcement, and choose **Suspend Enforcement** or **Resume Enforcement** from the **Actions** dropdown menu.
   The policy enforcement is suspended or resumed based on the selected action.

Image Upload Verification

This section describes how to verify whether an image upload to multiple clusters succeeded.

When you add an image and select multiple clusters for initial placement of the image using the **Place image directly on clusters**, the status message box shows that the task is successful. The status message displays the successful completion of the task even if the image is successfully uploaded to only one cluster. Nutanix recommends you to go to the **Tasks** page and check whether the Image upload and Image update subtasks succeeded for all the clusters that you selected. It is possible that the Image upload or update subtasks for some of the clusters are failed.

Nutanix recommends that you use **Place image using Image Placement policies** option when you add images to multiple clusters. Image Placement policy based placement ensures that images propagate successfully to multiple clusters in a single operation.

For information about Image Placement policy, see Image Placement Policies on page 488 section.

For information about how to place the image on the registered clusters using image placement policies, see Adding an Image on page 248 section.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2734

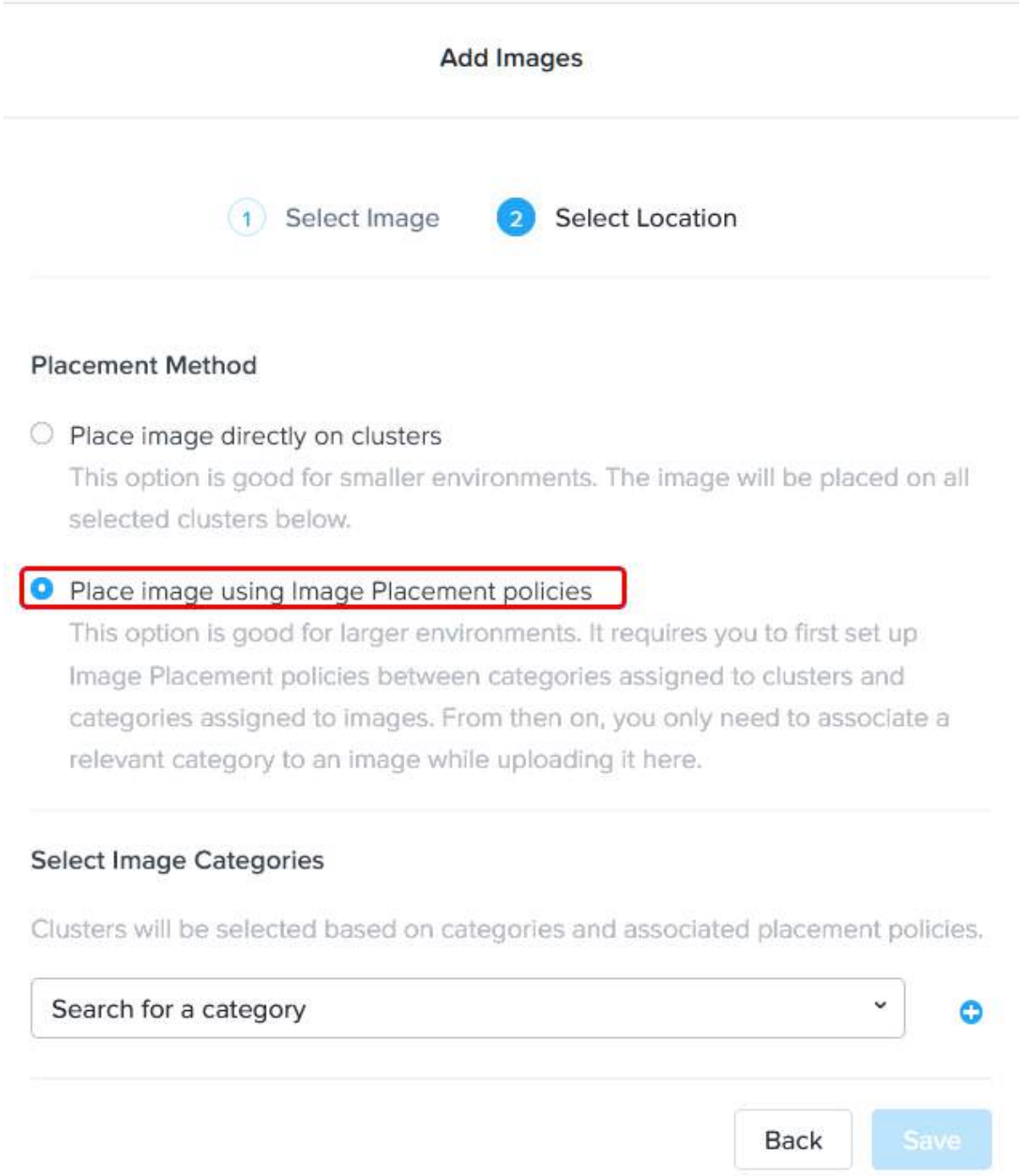


Figure 110: Image Placement Method selection for multiple clusters

Modifying an Image

This section describes how to modify images in Prism Central.

About this task

You can perform the following actions to modify the images in Prism Central:

- Update the image attributes.

- Delete the image
- Add image to Catalog.
- Manage image categories

To modify an image (delete, update, or add to catalog), perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default.
3. Select the target image checkbox, and choose any one of following actions from the **Actions** dropdown menu:
   - **Delete** to delete the image file.
   - **Update** to edit the image file.In the **Edit Image** window, update the image name, image description, or image type as desired, and click **Save**. For field details, see Adding an Image on page 248.
   - **Add Image to Catalog** to add an image to the catalog. For more information on how to add an image to the catalog, see Catalog Management on page 266.
   - **Manage Categories** to manage the image categories. In **Manage Categories** window, perform the following steps:
     1. Use the Add icon and Remove icon available under **Set Categories** field to add or remove the categories for the selected image.
     2. Click **Save**.

     For information about how to create an image category, see Creating a Category on page 459.

Importing Images to Prism Central

This section describes how to import images from registered clusters and manage the images centrally from Prism Central.

About this task

An image imported to Prism Central continues to reside on the cluster that owns it. Prism Central only creates and stores image metadata locally, and it uses that metadata when you perform an action on the image. After you import an image, the image remains visible on the cluster from which you imported it, however the system never allows you to update the image on the cluster. You can update the image only from Prism Central.

There is no impact on the following images when you import images in Prism Central:

- Any images that you choose not to import.
- Any images that you add subsequently to the cluster from its web console. These images remain editable on the cluster until you import them to Prism Central.

You can import the images in Prism Central using any of the following criteria in a single operation:

- All images from all registered clusters
- All images from a selection of clusters

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2736

- Selection of images from some of the clusters.

To import images from registered clusters, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default.
3. Click **Import Image**.
   The system displays the **Import Image** window.
4. In the **Import Images** window, select one of the following options:
   - **All Images** - To import all images from all registered clusters.
   - **Images On a Cluster** - To import all images from a selection of registered clusters.
   - **Select Images** - To import specific images from a given cluster. Click the link provided for the cluster, select the images that you want to import, and click **Done**.

     Repeat this step for all the clusters from which you want to import the specific images.
5. Click **Save** to begin import.
   Prism Central imports the metadata of the selected images and marks the images as read-only entities on the clusters.

   The image continues to stay in the container that hosted the disk before importing the image.

Policies for Image Management

You can define the Image Placement and Bandwidth Throttling policies for managing images. For information about Image Placement and Bandwidth Throttling policies, see Image Policy Management on page 487.

Catalog Management

Prism Central provides a catalog service to store VM snapshots and images. A Prism Central or self-service administrator creates this catalog of objects for self-service users (who have permissions to create a VM) to use them to deploy VMs in a project.

Note:

- The catalog service is a self-service feature that appears in Prism Central only when Prism Self-Service is enabled. For information about Prism Self-Service, see Prism Self Service Setup on page 530.
- You can create a custom role and enable or disable the Marketplace Item permissions to manage the Catalog Item entity permissions. For example, if you select **No Access** permission for the Marketplace Item entity for the custom role, the user with the custom role cannot access the **Catalog Item** page. For information about how to create a custom role with access to catalog items entity, see Creating A Custom Role information in the *AOS Security Guide*.

Catalog Items Summary View

To access the summary view of all the catalog items, perform the following steps:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2737

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Catalog Items** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The system displays **Catalog Items** page that enables you to view the catalog items available for all the projects in the cluster.

Figure 111: Catalog Items Page

The following table describes the fields that appear in the **Catalog Items** page. A dash (-) is displayed in a field when a value is not available or not applicable.

Table 46: Catalog Items Page - Field Description

Parameter	Description	Values
Name	Displays the catalog item name.	*<Catalog_Item_Name>*
Type	Displays the type of catalog item (Image or VM).	Image, VM
Description	Indicates the description for the catalog item	(description string)

Filters Pane - Catalog Items page

You can filter the information in the **Catalog Items** page based on the following fields that are available in the **Filter** pane. For information about how to use **Filters** option in Prism Central, see Prism Central GUI Organization on page 54.

Table 47: Filter Pane Field Description - Catalog Items page

Parameter	Description	Values
Name	Filters based on the catalog item name. It returns a list of catalog items that satisfy the name condition/ string.	*<Catalog_Item_Name>*
Description	Filters based on the description. It returns a list of catalog items whose description field satisfy the condition/string.	(description string)
Type	Filters based on the item type. Select one or more checkbox for the catalog items of the required types.	VM, Image

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2738

Adding a Catalog Item

This section describes how to add a VM snapshot or Image as a catalog item in Prism Central.

About this task

You can add the following entities as catalog items:

- *VM* - When you add a VM as the catalog item, a VM snapshot is created. The VM snapshot is available to users across all the self-service projects in the cluster. Users who have the requisite permissions can create VMs from the snapshot.
- *Image* - When you add an image as the catalog item, the image is available to users across all the self-service projects in the cluster. Users who have the requisite permissions can create VMs from the image.

> **Note:** After you add a VM or Image as the catalog item, a copy of these entities (VM snapshot or image) is added to the catalog. There is no impact to the catalog items (VM snapshot or image) even if the VM or image is deleted in Prism Central.

To add a VM snapshot or image as the catalog item, perform the following steps:

> **Note:** Nutanix recommends to power off the VM before you add a VM snapshot to the catalog.

Procedure

1. Log in to Prism Central.
2. Perform any of the following actions based on the type of catalog item you want to add:
   - » *Image* - Navigate to the **Images** page. For information about how to access the **Images** page, see Images Summary View on page 243.
   - » *VM* - Navigate to the **List** tab of the **VMs** page. For information about how to access the VMs **List** tab, see VMs Summary View on page 104.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2739

3. To add an image, perform the following actions:

   a. Select the target image checkbox, and choose **Add Image to Catalog** from the **Actions** drop-down menu.
   The system displays the **Add Image to Catalog** window.

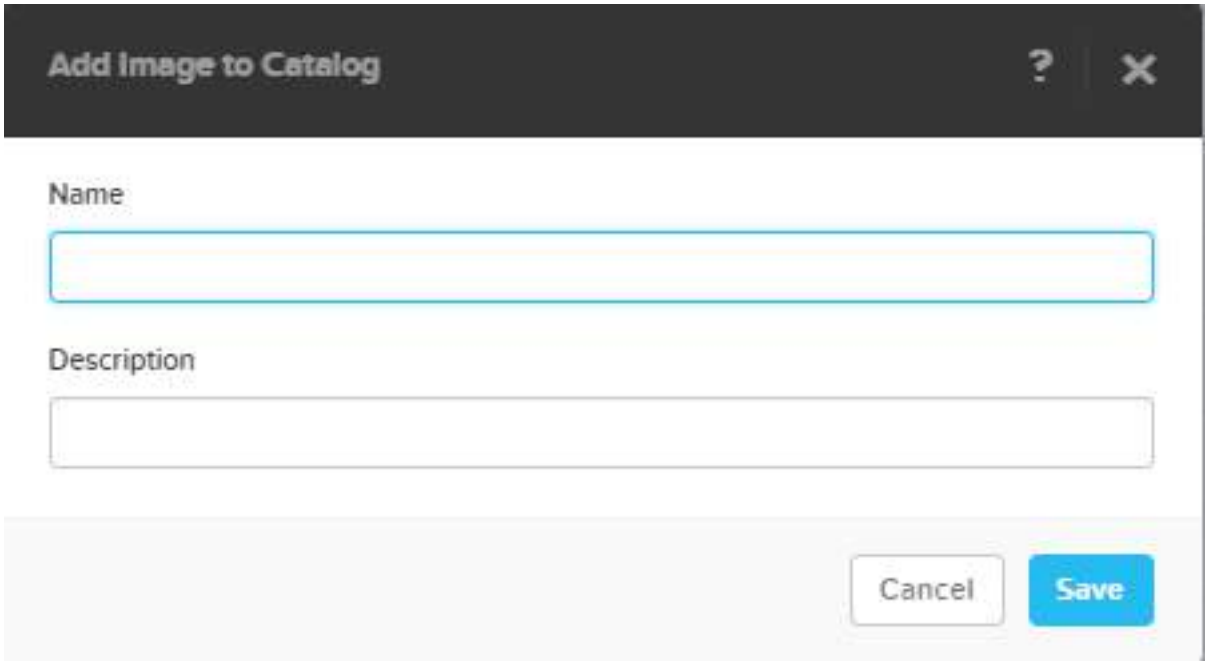


Figure 112: Add Image to Catalog Window

   b. Enter the following information in the **Add Image to Catalog** window:

      - **Name** - Enter a name for the image.
      - **Description** - Enter a description of the image.

   c. Click **Save**.
   The image is added as the catalog item.

4. To add a VM, perform the following actions:

   a. Select the target VM checkbox, and choose **Add to Catalog** from the **Actions** drop-down menu.
   The system displays the **Add VM to Catalog** window.

   b. Enter the following information in the **Add VM to Catalog** window:

      - **Name** - Enter a name for the VM.
      - **Description** (optional) - Enter a description of the VM.
      - **Guest Customization** - Select the following options for guest operating system (OS) for the VMs that you deploy using this VM template:.

        - From the **Script Type** drop-down list, select the setup script as **Sysprep (Windows)** to customize the Windows OS or **Cloud-init (Linux)** to customize the Linux OS.

          Note: If you select **No Customization** at the time of creating the template and allow the users to override the guest customization settings using **Allow users to override at VM Deployment?**

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2740

toggle field, it gives the maximum customization control to the users. In this case, the users can customize the script type and the configuration method.

- From the **Configuration Method** drop-down list, for each of these script types selected in **Script Type** field, select either upload a custom script or opt for a guided setup in the field.

  Important: The information that you enter is used to customize the OS of the VMs that are deployed using this template.

c. (Optional) If you select the **Script Type** as **Sysprep (Windows)** and the **Configuration Method** as **Guided Setup**, enter the following information:

- **Authentication**: Select the checkbox to allow the user who deploys the VM to set a username and password.
- **Locale**: Select the checkbox to allow the end user to specify the locale (language).
- **Hostname**: Select the appropriate radio button to specify the host name source: the deployed VM name, a name provided by the person deploying the VM, or restricted hostname access.
- **License Key**: Specify the license key source. Check the **Enter License Key** radio button and enter the key in the field to set the license key, check the **Allow end user to input License Key** radio button to let the user do it, or check the **No License Key** radio button to not require a license key.

d. (Optional) If you select the **Script Type** as **Cloud-init (Linux)** and the **Configuration Method** as **Guided Setup**, enter the following information:

- **Authentication**: Select the checkbox to allow the user who deploys the VM to set a username and password.
- **SSH Key** Select the checkbox to allow the user who deploys the VM to provide an SSH key.
- **Locale**: Select the checkbox to allow the end user to specify the locale (language).
- **Hostname**: Select the appropriate radio button to specify the host name source: the deployed VM name, a name provided by the person deploying the VM, or restricted hostname access.

e. (Optional) If you select the **Script Type** as **Sysprep (Windows)** and the **Configuration Method** as **Custom Script**, do one of the following:

» Click **Upload Script** to upload a script to customize the guest OS of the VMs.

» Copy the script and paste the script in the text box.

f. (Optional) If you select the **Script Type** as **Cloud-init (Linux)** and the **Configuration Method** as **Custom Script**, do one of the following:

» Click **Upload Script** to upload a script to customize the guest OS of the VMs.

» Copy the script and paste the script in the text box.

g. Click **Save**.
The VM snapshot is added as the catalog item.

Deleting a Catalog Item

This section describes how to delete a catalog item in Prism Central.

About this task

VM snapshots and images deleted from a catalog makes those items unavailable to project members.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2741

To delete a VM snapshot or image from the catalog items, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Catalog Items** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66
   The system displays **Catalog Items** page that enables you to view the catalog items available for all the projects across the registered clusters.
3. Select the target VM snapshot or Image catalog item, and click **Delete Catalog Item**.
   The selected catalog item is deleted from all the projects in the cluster.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2742

STORAGE ENTITIES

You can access the following entity items from the **Storage** entity of the **Infrastructure** application:

- Storage Containers (see Limitations for Storage Containers on page 294)
- Volume Groups (see Volume Group Management on page 301)
- vCenter Datastores (see External vCenter Server Integration on page 326)

For information about how to access the entities items available in **Storage** entities, see Application-specific Navigation Bar on page 66.

Storage Container Management

Storage Management (Prism Central)

Storage in a Nutanix cluster is organized into several components that allow you to manage capacity and performance. Nutanix clusters include storage pool, storage container, volume group, and virtual disk components. Prism Element allows you to manage all aspects of storage for a cluster, but you can also manage storage components directly from Prism Central.

A storage pool is created during cluster configuration. There is one storage pool per cluster. Storage efficiency features that include compression, deduplication, erasure coding, and replication factor are enabled at the storage container level.

The **Storage Containers** page displays information about all the storage containers across the registered clusters.

Note:

- A storage pool and three storage container are created automatically when the cluster is created.
- A storage container is created only if you have configured the Controller VMs (CVMs) with enough memory. The CVM allocation requirements differ depending on the models and features that are used at your site. For more information about the minimum CVM requirements, see Controller VM (CVM) Field Specifications information in *Acropolis Advanced Administration Guide*.
- The NutanixManagementShare, SelfServiceContainer, and a default-container are created by default.
  - The NutanixManagementShare storage container is a built-in storage container for Nutanix clusters for use with the Nutanix Files and Self-Service Portal (SSP) features. This storage container is used by Nutanix Files and SSP for file storage, feature upgrades, and other feature operations. The NutanixManagementShare storage container is not intended to be used as storage for vDisks, including Nutanix Volumes.
  - SelfServiceContainer is a built-in storage container within a Nutanix cluster that is used for storage by VMs created using Image service features such as Self-Service and OpenShift. SelfServiceContainer can also be used like any other container for regular VMs, volume groups, and images. General requirements for using container-level configurations such as compression, deduplication, erasure coding, and replication factor in SelfServiceContainer are the same as any other container.

    Important: To ensure proper operation of these features, do not delete these storage containers. Nutanix also recommends that you should not delete these storage containers even if you are not using these features.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2743

- The **Summary** tab in the **Storage Containers** page displays information about storage containers across the registered clusters. For details, see Storage Containers Summary View on page 273.
- The **Summary** tab in the individual storage container page displays the detailed information about the selected storage container. For more information, see Storage Container Details View on page 279.
- For information about storage management tasks that are performed through Prism Element web console, see the Storage Management chapter in the *Prism Element Web Console Guide*.

You can perform the following actions to manage a storage container from Prism Central:

- Create and manage storage directly from Prism Central when the hypervisor is either ESXi, Hyper-V or AHV. For more information, see the following sections:
  - Creating a Storage Container on page 294
  - Modifying a Storage Container on page 299
  - Deleting a Storage Container on page 301
- Enable inline erasure coding. For more information, see Enabling Inline Erasure Coding on page 292

Storage Containers Summary View

The **Summary** tab in **Storage Containers** page provides the information about all the storage containers across the registered clusters.

To access the summary view of all storage containers, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and go to **Storage** > **Storage Containers** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
3. Click the **Summary** tab.

   The system displays **Summary** page for all storage containers.

Figure 113: Summary Page - All Storage Containers

The **Storage Container** page includes five tabs on the left (**Summary**, **List**, **Alerts**, **Events**, and **Metrics**) with a display area below the selected tab.

The **Summary** tab of all storage containers displays the following widgets:

- **Highlighted Entities**: Displays a list of the storage containers with the highest usage of the <*parameter*> you select from the dropdown menu on the right of the widget. The <*parameter*> involves **IO Latency**, **IOPS**, and **Bandwidth**. Click **View All XX Storage Containers** link at the bottom to display the **List** tab.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2744

- **Alerts**: Displays a list of alerts related to storage container that are generated during the specified <*interval*> you select from the dropdown menu on the right of the widget. The <*interval*> involves **Last week**(default), **Last 24 hours**, and **Last 1 hour**. When an alert appears, you can click the graph to view a list of those alerts. Click any alert to display the details page for that alert.
- **Anomalies**: Displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified <*interval*> you select from the dropdown menu on the right of the widget. The <*interval*> involves **Last week**(default), **Last 24 hours**, and **Last 1 hour**. When an anomaly appears, you can click the graph to view a list of those anomalies. Click any anomaly to display the event page for that anomaly.

Lists Tab

The **List** tab displays the list of storage containers across all clusters.

Figure 114: Storage Containers List Tab

The following table describes the fields that appear in the **List** tab of **Storage Containers** page:

> **Note:** The fields vary based on the **View by** and **Group by** options. A dash (-) is displayed in a field when a value is not available or applicable. For more information about **View by** and **Group by** options, see Prism Central GUI Organization on page 54.

Table 48: Storage Containers List Tab - Field Description

Field	Description	Values
Select **General** from **View by** option.		
Name	Displays the name of the storage container. You can click the storage container name to view the detailed information for that storage container. For information about storage container details view, see Storage Container Details View on page 279.	*<Storage _Container_Name>*
Physical Usage	Displays the amount of used physical storage space. A bar also appears that graphically indicates the amount of used and free storage space available in the storage container. When you hover the cursor over the bar, the system displays a window that lists the used space, free space, and total space in the storage container.	xxx [GiB|TiB]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2745

Field	Description	Values
Cluster Fault Tolerance	Displays the fault tolerance, which is the number of failures the cluster can withstand if a node or a disk in the cluster fails. The cluster fault tolerance is specified when the cluster is created.	1N/1D, 1N&1D, 2N/2D
Replication Factor	Displays the replication factor, which is the number of maintained data copies. The replication factor is specified when the storage container is created.	Integer
Compression	Displays whether compression is enabled.	[Off|On]
Capacity Deduplication	Displays whether capacity deduplication is enabled, which allows data duplication compression on hard disks (HDD). Performance tier deduplication is a prerequisite for capacity deduplication.	[Off|On]
Erasure Coding	Displays whether erasure coding is enabled or not. For more information about Erasure Coding, see Erasure Coding on page 288.	[Off|On]
Cluster Name	Displays the name of the cluster in which the storage container resides. You can click the cluster name to view the detailed information for that cluster. For information about cluster details view, see Cluster Details View on page 405.	*<Cluster_Name>*
Select **Performance** from **View by** option.		
Name	Displays the name of the storage container. You can click the storage container name to view the detailed information for that storage container. For information about storage container details view, see Storage Container Details View on page 279.	*<Storage _Container_Name>*
Free Space (Physical)	Displays the amount of free physical space available in the storage container.	xxx [GiB|TiB]
Used Space (Physical)	Displays the amount of used physical space in the storage container.	xxx [GiB|TiB]
Total Space (Physical)	Displays the total amount of physical storage space in the storage container.	xxx [TiB]
IOPS	Displays the current I/O operations per second (IOPS) for the storage container. The controller IOPS, I/O bandwidth, and I/O latency fields record the I/O requests serviced by the Controller VM (CVM). The I/O can be served from memory, cache (SSD), or disk.	[0 - unlimited]
IO Bandwidth	Displays I/O bandwidth used per second for Controller VM-serviced requests in this storage container.	xxx [MBps|KBps]
IO Latency	Displays the average I/O latency for Controller VM-serviced requests in this storage container.	xxx [ms]
Select **Optimization** from **View by** option.		

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2746

Field	Description	Values
Name	Displays the name of the storage container. You can click the storage container name to view the detailed information for that storage container. For information about storage container details view, see Storage Container Details View on page 279.	*<Storage_Container_Name>*
Data Reduction Ratio	Displays the capacity optimization (as a ratio) that results from the combined effects of deduplication, compression, and erasure coding.	*xx*:1
Data Reduction Savings	Displays the amount of storage capacity saved from the combined effects of deduplication, compression, and erasure coding.	xxx [GiB|TiB]
Compression Delay	Displays the time delay to perform compression on the data.	xx [m]
Effective Free Space	Displays the amount of physical free space after data reduction.	xxx [GiB|TiB]
Overall Efficiency	Displays the capacity optimization (as a ratio) that results from the combined effects of data reduction (deduplication, compression, and erasure coding), cloning, and thin provisioning.	*xx*:1

You can perform the following actions for the storage containers in the **Lists** tab:

- Access the detailed information about an individual storage container. For more information, see Storage Container Details View on page 279.
- Filter the storage containers list based on available parameter values using **Filters** pane. For more information about **Filters** pane, see Filters Pane - Storage Containers Page on page 276.
- Export the table that contains the list of storage containers and their information to a file in a CSV format. For more information about **Export** option, see Export on page 59.
- Group the storage containers based on pre-defined criteria. For information about how to group the storage containers, see Group by on page 56.
- View storage containers based on pre-defined criteria or create a custom view. For information about available views and how to create a custom view, see View by on page 56.
- Create a storage container. For more information about how to create a storage container, see Creating a Storage Container on page 294.
- Perform the actions specific to storage container on a single or multiple storage containers using the **Actions** dropdown menu. For instructions on how to perform these actions, see Modifying a Storage Container on page 299 or Deleting a Storage Container on page 301.

  Note: The **Actions** dropdown menu is grayed out unless you select a storage container or if you select multiple storage containers.

Filters Pane - Storage Containers Page

The following table describes the fields available in the **Filters** pane:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2747

Table 49: Filter Pane Fields

Parameter	Description	Values
Name	Filters based on the storage container name. Select a condition from the dropdown list and enter a string in the field. The system returns a list of storage containers that satisfy the storage container name condition/string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	(storage container name string)
Cluster Name	Filters based on the cluster name. Select a condition from the dropdown list and enter a string in the field. The system returns a list of storage containers that satisfy the cluster name condition/ string.	(cluster name string)
Replication Factor	Filters based on the replication factor. Select the checkbox(es) for the desired replication factor (1, 2, 3). Only existing RF values appear. For example, if all containers are at RF 2, just a single checkbox for RF 2 appears. The number of storage containers currently in each setting are displayed in the **List** tab.	1, 2, 3
Capacity Deduplication	Filters based on the capacity deduplication setting. Select the checkbox(es) for the desired settings to return a list of storage containers with those settings. The number of storage containers currently in each setting are displayed in the **List** tab.	On, Off, None, Inline, Post Process
Erasure Coding	Filters based on the erasure coding setting. Select the checkbox(es) for the desired settings to return a list of storage containers with those settings. The number of storage containers currently in each setting are displayed in the **List** tab.	On, Off
Free Space (Physical)	Filters based on the available storage space for a storage container. Select the checkbox(es) for the desired range or enter an amount range in the "**From <low> to <high> GiB|TiB**" field. It returns a list of storage containers with available capacity in that range.	([xx] to [yy] GiB |TiB range)
Health	Filters based on the storage container health state. Select one or more states checkboxes to return a list of storage containers in those states. The number of storage containers currently in each state is displayed in the **List** tab.	Critical, Warning, Good

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2748

Parameter	Description	Values
Used Space (Physical)	Filters based on the used storage space for a storage container. Select the checkbox(es) for the desired range or enter an amount range in the "**From <low> to <high> GiB|TiB**" field. It returns a list of storage containers with used storage in that range.	([xx] to [yy] GiB |TiB range)
Total Space (Physical)	Filters based on the total available capacity for a storage container. Select the checkbox(es) for the desired range or enter an amount range in the "**From <low> to <high> GiB|TiB**" field. It returns a list of storage containers with maximum capacity in that range.	([xx] to [yy] GiB|TiB range)
IOPS	Filters based on the current IOPS. Check the box for the desired range or enter a range in the "**From <low> to <high> iops**" field. It will return a list of storage containers with IOPS in that range.	([xx] to [yy] IOPS range)
IO Bandwidth	Filters based on the I/O bandwidth used. Check the box for the desired range or enter a range in the "**From <low> to <high> MBps**" field. It will return a list of storage containers with I/O bandwidth usage in that range.	([xx] to [yy] MBpS range)
IO Latency	Filters based on the average I/O latency. Check the box for the desired range or enter a range in the "**from <low> to <high> ms**" field. It returns a list of storage containers with average I/O latency in that range.	([xx] to [yy] ms range)

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options that are available on the **Activity** > **Alerts** page, however it only displays the alerts related to storage containers across the registered clusters. For more information about alerts, see *Prism Central Alerts and Events Reference Guide*.

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options that are available on the **Activity** > **Events** page, however it only displays the events related to storage containers across the registered clusters. For more information about events, see *Prism Central Alerts and Events Reference Guide*.

Metrics Tab

The **Metrics** tab allows you to view performance metrics across the storage containers. Click the **Metrics** tab to display dropdown menu of available metrics, and select the metric name to display the relevant performance information.

> **Note:** The **Metrics** dropdown menu is hypervisor-specific, and might vary based on the hypervisors used in the cluster.

The following is an example showing the dropdown menu of the **Metrics** tab:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2749

Figure 115: Storage Containers Metrics Tab

Table 50: Metrics Tab Fields

Metric	Description
IOPS	Displays total, read, and write IOPS graphs listing current values and total containers (number). The current values are split into intervals (for example, less than 700, 700-1400, 1400-2000, more than 2000). **Note:** The same format also applies to the other metrics in this table.
IO Latency	Displays total, read, and write I/O latency rate graphs.
IO Bandwidth	Displays total, read, and write I/O bandwidth rate graphs.
Storage Usage	Displays storage usage graph.
Optimization	Displays replication factor, data reduction ratio, and overall efficiency graphs.

Storage Container Details View

To access the details view of an individual storage container, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Storage** > **Storage Container** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   By default, the system displays the **List** tab with storage containers across all the registered clusters.
3. Click the target <*Storage_Container_Name*> to view the **Summary** tab of an individual storage container.

   Note: Replace <*Storage_Container_Name*> with the actual storage container name at your site.

The following is an example showing the **Summary** tab of an individual storage container:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2750

Figure 116: Summary Tab - Individual Storage Container

The **Summary** tab of an individual storage container provides the following widgets:

- **Properties** - Displays summary information about the storage container. For information about the fields available in **Properties** widget, see Storage Properties Widget - Parameter Details on page 120.
- **Alert**- Displays a list of related alerts that occurred during the specified interval. Select either **Last week** (default), **Last 1 hour** or **Last 24 hours** from the dropdown menu on the top right corner of the widget.
- **Anomalies** - Displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified interval. Select either **Last week** (default), **Last 1 hour** or **Last 24 hours** from the dropdown menu on the top right corner of the widget. When an anomaly appears, you can click the graph to display a list of those anomalies. If you click an individual anomaly, the system displays the event page for that anomaly.
- **Usage** - Displays usage data for the storage container. For information about the fields available in **Usage** widget, see Storage Properties Widget - Parameter Details on page 120.
- **Optimization & Performance** - Displays optimization and performance data for the storage container. For information about the fields available in **Optimization & Performance** widget, see Storage Properties Widget - Parameter Details on page 120.

<*Action*> available above the widgets. Click the appropriate <*Action*> to run that administrative action on the storage container. For more information about how to perform any <*Action*>, see Modifying a Storage Container on page 299 and Deleting a Storage Container on page 301.

Storage Container Widgets - Field Details

The following table describes the fields in the **Properties**, **Usage**, and **Optimization & Performance** widgets. A dash (-) in a field indicates that there is not enough data to evaluate or a value is not assigned. The displayed fields vary by hypervisor.

Table 51: Storage Container Widgets - Field Description

Field	Description	Values
Properties widget		
Cluster	Displays the name of the cluster in which the storage container resides. You can click the name to view the detailed information about the cluster. For more information, see Cluster Details View on page 405.	(cluster name)
Replication Factor	Displays the replication factor, which is the number of maintained data copies. The replication factor is specified when the storage container is created.	[1-3]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2751

Field	Description	Values
Compression	Displays whether compression is enabled.	[Off|On]
Capacity Deduplication	Displays whether capacity deduplication is enabled, which allows data duplication compression on hard disks (HDD). Performance tier deduplication is a prerequisite for capacity deduplication.	[On, Off]
Erasure Coding	Displays whether erasure coding is enabled or not. For more information about Erasure Coding, see Erasure Coding on page 288.	[Off|On]
Filesystem allowlists	Displays the IP addresses for file systems that are allowed.	[IP addresses]
Compression Delay	Displays the delay (number of minutes) before data changes are compressed. A zero value indicates that compression is immediate (not delayed).	xx min
Thick Provision	Displays the reserved storage capacity for thick provisioned VMs.	xxx [GiB|TiB]
Effective Free Space	Displays the amount of logical free space after data reduction (logical free space x data reduction ratio).	xxx [GiB|TiB]
Usage widget		
Free Space (Physical)	Displays the amount of physical free space available in the storage container.	xxx [GiB|TiB]
Used Space (Physical)	Displays the amount of physical used space in the storage container.	xxx [GiB|TiB]
Reserved Capacity (Physical)	Displays the amount of physical reserved space in the storage container.	xxx [GiB|TiB]
Total Space (Physical)	Displays the amount of physical total space in the storage container.	xxx [GiB|TiB]
Optimization & Performance widget		
Data Reduction Ratio	Displays the capacity optimization (as a ratio) that results from the combined effects of deduplication, compression, and erasure coding.	*xx*:1
Data Reduction Savings	Displays the amount of storage capacity saved from the combined effects of deduplication, compression, and erasure coding.	xxx [GiB|TiB]
Overall Efficiency	Displays the capacity optimization (as a ratio) that results from the combined effects of data reduction (deduplication, compression, and erasure coding), cloning, and thin provisioning.	*xx*:1
IOPS	Displays the current I/O operations per second (IOPS) for the storage container. The controller IOPS, I/O bandwidth, and I/O latency fields record the I/O requests serviced by the Controller VM (CVM). The I/O can be served from memory, cache (SSD), or disk.	[0 - unlimited]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2752

Field	Description	Values
IO Bandwidth	Displays I/O bandwidth used per second for Controller VM-serviced requests in this storage container.	xxx [MBps|KBps]
IO Latency	Displays the average I/O latency for Controller VM-serviced requests in this storage container.	xxx [ms]
Erasure Coding	Displays whether erasure coding is enabled or not. For more information about Erasure Coding, see Erasure Coding on page 288.	[Off|On]

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options as the Alerts dashboard, however it is filtered to display the alerts only for the selected storage container (individual storage container). For more information about alerts, see Prism Central Alerts and Events Reference Guide.

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options as the Events dashboard, except it is filtered to display just events for this storage container. For more information about events, see Prism Central Alerts and Events Reference Guide.

Metrics Tab

The **Metrics** tab allows you to view usage metrics for the storage container. Click the **Metrics** tab to view graphs for all the metrics. The graph is a rolling time interval performance or usage monitor. The baseline range appears as a blue band in the graph.

> **Note:** The baseline range and identified anomalies are based on sophisticated machine-learning capabilities. For more information, see Behavioral Learning Tools in *Intelligent Operations Guide*. The machine-learning algorithm uses 21 days of data to monitor and predict performance. A graph or baseline band may not appear if less than 21 days of data is available.

You can perform the following actions in the **Metrics** tab:

- Place the cursor anywhere on the horizontal axis to display the value at that time.
- Select the duration (time interval) from the dropdown list on the right (last 1 hour, last 24 hours, last week, last 21 days).
- From the **Actions** dropdown menu that appears on the top-right corner of each metrics widget, you can perform the following operations:
  - Select **Add to Analysis** to add the selected metric to **Analysis** dashboard. For more information, see Analysis Dashboard in *Intelligent Operation Guide*.
  - Choose **Select Analysis Session** to assign the metric to a target session.
- Click the **Filters** option to select one or more appropriate metric checkboxes to display the selected metrics in the **Metrics** page.

The following table describes the metrics available in **Metrics** tab:

> **Note:** Metrics are hypervisor-dependant, and might not be available on all hypervisors.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2753

Table 52: Metrics Tab Fields

Metric	Description
Storage Controller IOPS	Displays the graph for total I/O operations per second (IOPS) for the storage controller.
Storage Controller Read IOPS	Displays the graphs for Read I/O operations per second (IOPS) for the storage controller.
Storage Controller Write IOPS	Displays the graph for Write I/O operations per second (IOPS) for the storage controller.
Storage Controller Latency	Displays the graph for total latency (in milliseconds) for storage controller
Storage Controller Read Latency	Displays the graph for read I/O latency (in milliseconds) for storage controller.
Storage Controller Write Latency	Displays the graph for write I/O latency (in milliseconds) for storage controller.
Storage Controller I/O Bandwidth	Displays the graph for total I/O bandwidth used per second (MBps or KBps) by storage controller.
Storage Controller Read I/O Bandwidth	Displays the graph of bandwidth used per second (MBps or KBps) for Read I/O operations by storage controller
Storage Controller Write I/O Bandwidth	Displays the graph of bandwidth used per second ((MBps or KBps) for Write I/O operations by storage controller.

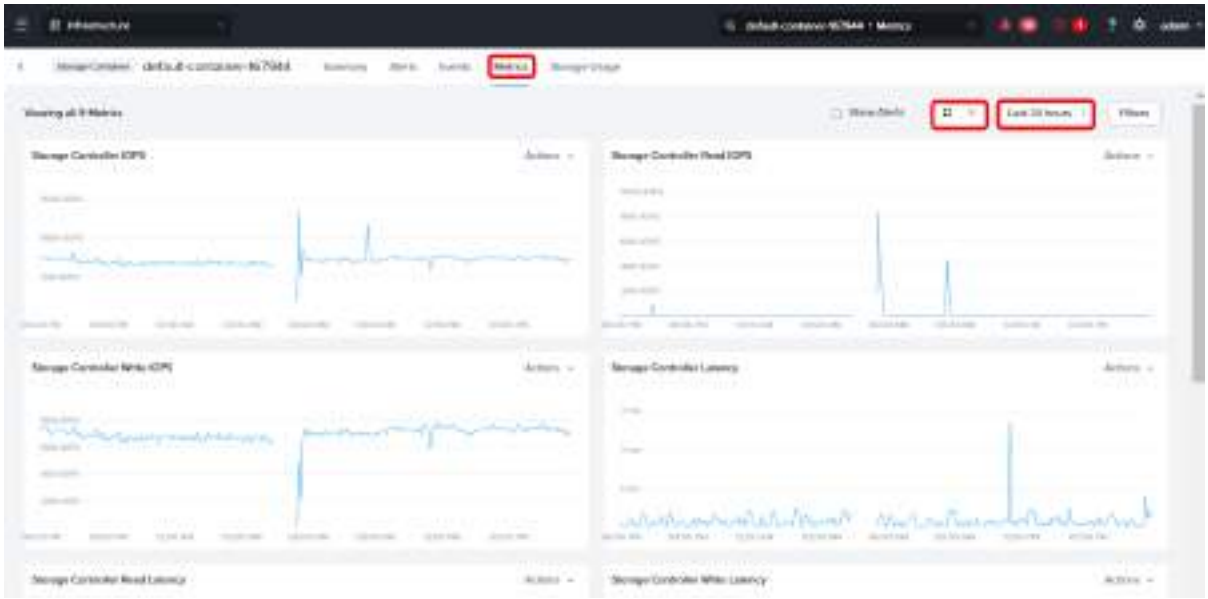


Figure 117: Metrics Tab

Storage Usage Tab

The **Storage Usage** tab displays the following graphs:

- **Usage Summary** graph - It displays a rolling time interval monitor of storage container storage usage that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2754

the horizontal axis displays the value at that time. For more in-depth analysis, you can add the monitor to the analysis page by clicking the blue link in the upper right of the graph.

- **Tier-wise Usage** graph - It displays a pie chart divided into the percentage of container storage space used by each disk tier (SSD and DAS-SATA).

Figure 118: Storage Container Usage Tab

Storage Components

Storage in a Nutanix cluster is organized into the following components.

Storage Tiers

Each type of storage hardware (SSD-PCIe (NVMe), SSD (SATA SSD), and HDD) is placed in a storage tier. You can determine the tier breakdown for disks in a storage pool through the web console . For more information, see Storage Table View information in *Prism Element Web Console Guide*.

Storage Pools

Storage pools are groups of physical disks from one or more tiers. Storage pools provide physical separation because a storage device can only be assigned to a single storage pool at a time. Nutanix recommends creating a single storage pool for each cluster. This configuration allows the cluster to dynamically optimize capacity and performance. Isolating disks into separate storage pools provides physical separation, but can create an imbalance of these resources if the disks are not actively used. When you expand your cluster by adding new nodes, the new disks can also be added to the existing storage pool. This scale-out architecture allows you to build a cluster that grows with your needs.

When you create a cluster, a default predefined storage pool is available. This pool includes the total capacity of all the disks on all the hosts in the cluster.

Storage Containers

A storage container is a subset of available storage within a storage pool. Storage containers are created within a storage pool to hold virtual disks (vDisks) used by virtual machines. For more information, see Creating a Storage Container. By default, storage is thinly provisioned, which means that the physical storage is allocated to the storage container as needed when data is written, rather than allocating the predefined capacity when the storage container is created. Storage efficiency features such as compression, deduplication, and erasure coding are enabled at the container level.

When you create a Nutanix cluster, the following storage containers are created by default:

- NutanixManagementShare: The NutanixManagementShare storage container is a built-in storage container for Nutanix clusters for use with the Nutanix Files and Self-Service Portal (SSP) features. This storage container is used by Nutanix Files and SSP for file storage, feature upgrades, and other feature operations. To ensure proper operation of these features, do not delete this storage container. Nutanix also recommends that you do not delete this storage container even if you are not using these features. The NutanixManagementShare storage container is not intended to be used as storage for vDisks, including Nutanix Volumes.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2755

- SelfServiceContainer: SelfServiceContainer is a built-in storage container within a Nutanix cluster that is used for storage by VMs created using Image service features such as Self-Service and OpenShift. SelfServiceContainer can also be used like any other container for regular VMs, volume groups, and images. General requirements for using container-level configurations such as compression, deduplication, erasure coding, and replication factor in SelfServiceContainer are the same as any other container. Nutanix recommends that you do not delete this storage container.
- Default-Container-XXXX: Default-Container-XXXX container is a built-in storage container used by VMs to store vDisks for user VMs and applications. You can rename the Default-Container or delete it and create a new one according to your naming convention.

Volume Groups

A volume group is a collection of logically related virtual disks (or volumes). A volume group is attached to VM either directly or using iSCSI. You can add vDisks to a volume group, attach them to one or more consumers, include them in disaster recovery policies, and perform other management tasks. You can also detach a volume group from one VM and attach it to another, possibly at a remote location to which the volume group is replicated.

You manage a volume group as a single unit. When a volume group is attached to a VM, the VM can access all of the vDisks in the volume group. You can add, remove, and resize the vDisks in a volume group at any time.

Each volume group is identified by a UUID, a name, and an iSCSI target name. Each disk in the volume group also has a UUID and a SCSI index that specifies ordering within the volume group. A volume group can be configured for either exclusive or shared access.

You can backup, protect, restore, and migrate volume groups. You can include volume groups in protection domains configured for asynchronous data replication (Async DR), either exclusively or with VMs. However, volume groups cannot be included in a protection domain configured for metro availability, in a protected vStore, or in a consistency group for which application consistent snapshots are enabled.

vDisks

A vDisk is created within a storage container or volume group to provide storage to the virtual machines. A vDisk shows up as a SCSI device when it is mapped to a VM.

Containers for VMware and Hyper-V (Datastores/SMB Shares)

In vSphere, a datastore is a logical container for files necessary for VM operations. Nutanix provides the choice by supporting both iSCSI and NFS protocols when mounting a storage volume as a datastore within vSphere. NFS has many performance and scalability advantages over iSCSI, and it is the recommended datastore type.

In Hyper-V environments, storage containers are mounted as an SMB share.

> **Note:** Using a Nutanix storage container as a general-purpose NFS or SMB share is not recommended. For NFS and SMB file service, use Nutanix Files.

NFS Datastores. The Distributed Storage Fabric (DSF) reduces unnecessary network chatter by localizing the data path of guest VM traffic to its host. This boosts performance by eliminating unnecessary hops between remote storage devices that is common with the pairing of iSCSI and VMFS. To enable vMotion and related vSphere features (when using ESX as the hypervisor), each host in the cluster must mount an NFS volume using the same datastore name. The Nutanix web console and nCLI both have a function to create an NFS datastore on multiple hosts in a Nutanix cluster.

To correctly map the local ESX datastore to the Nutanix container:

- Map the NFS share with 192.168.5.2 (internal IP address) and not the Controller VM IP address or cluster virtual IP address.
- The name of the datastore should be same as the name of the container.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2756

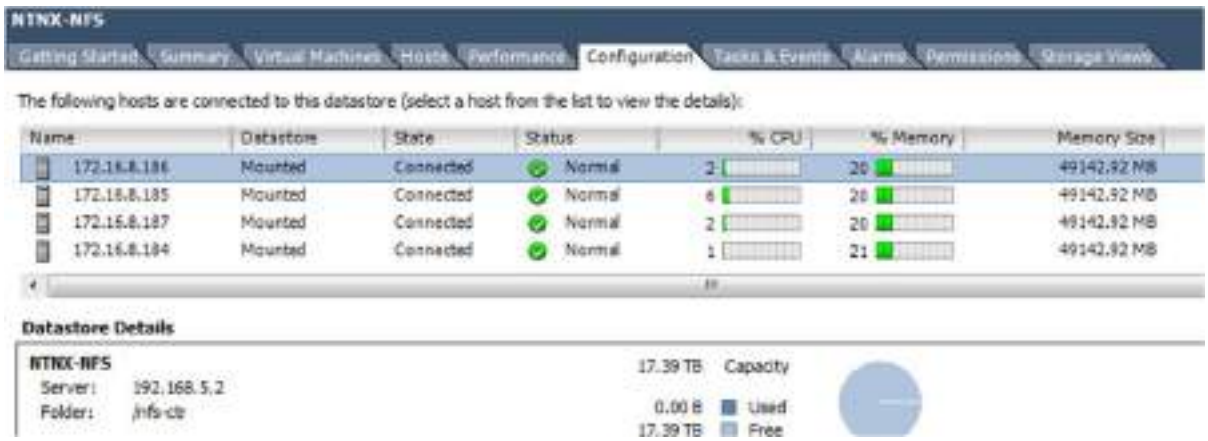


Figure 119: vSphere Configuration of NFS Datastore

SMB Library Share. The Nutanix SMB share implementation is the Hyper-V equivalent of an NFS Datastore with feature and performance parity with a vSphere configuration. The registration of a Nutanix storage container as an SMB Library share can be accomplished through a single powershell script, or through the Virtual Machine Manager GUI.

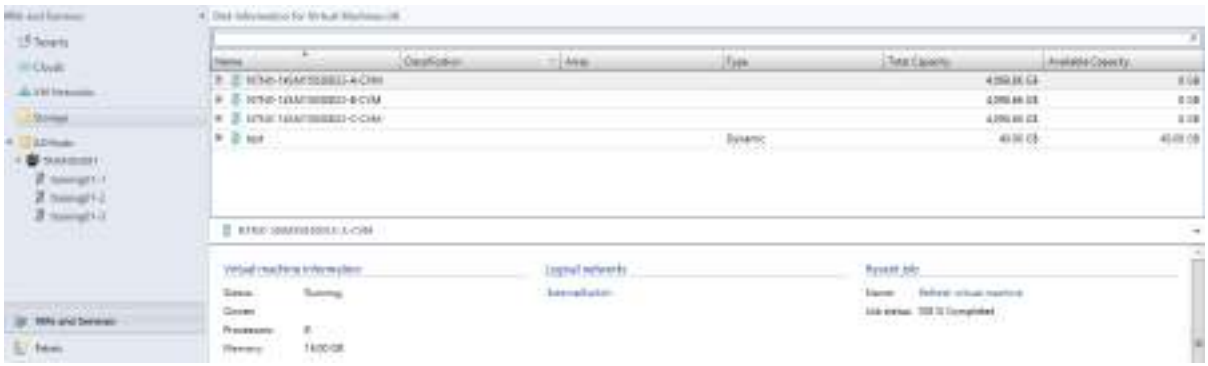


Figure 120: Hyper-V Configuration of an SMB Share

Storage Efficiency

Nutanix provides storage efficient capabilities that allows strategic management of storage resources to maximize capacity utilization, enhance performance, and ensure reliability.

In a Nutanix cluster, where data is distributed across multiple nodes, achieving efficiency is critical to reducing costs, optimizing resource usage, and maintaining scalability.

To minimize redundancy, conserve space, and enhance fault tolerance, a Nutanix cluster supports the following storage efficiency capabilities:

- Deduplication on page 287
- Compression on page 286
- Erasure Coding on page 288

Compression

You can enable compression on a storage container. Compression can save physical storage space and improve I/O bandwidth and memory usage—which may have a positive impact on overall system performance.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2757

> **Note:** If the metadata usage is high, compression is automatically disabled. If compression is automatically disabled, an alert is generated.

The following types of compression are available:

Post-process compression

Data is compressed after it is written. The delay time between write and compression is configurable, and Nutanix recommends a delay of 60 minutes.

Inline compression

Data is compressed as it is written. When you create a new storage container, inline compression is enabled by default for all license tiers. It is set to a delay of 0, compressing data immediately as it is written.

Data Reduction Ratios and Data Reduction Savings

You can view data reduction ratios and data reduction savings in Prism Central for any of the following entities:

- *For the entire cluster*

  Navigate to **Summary** tab in the **Clusters** page, and observe the **Data Reduction**column entry for the target cluster in **Storage Usage** widget. For information about how to access the **Clusters** page, see Clusters Summary View on page 398.

  > **Note:** The **Data Reduction Savings** for the entire cluster is visible only in the **Storage** dashboard in Prism Element. For more information, see Storage Overview View information in *Prism Element Web Console Guide*.

- *For an individual Storage Container*

  Navigate to the **Summary** tab of an individual storage container, and observe the **Data Reduction Ratio** and **Data Reduction Savings** fields in **Optimization & Performance** widget. For information about how to navigate to the **Summary** tab of an individual storage container, see Storage Container Details View on page 279.

Deduplication

Deduplication reduces space usage by consolidating duplicate data blocks on Nutanix storage when you enable capacity deduplication on a storage container.

> **Important:**
>
> - Deduplication is only supported on clusters with a minimum of three nodes.
> - If deduplication enabled on storage containers having protected VMs, the system lowers the replication speed.
> - Turning deduplication on for VAAI clone or linked clone environments is not recommended.

Capacity Deduplication

Enable capacity deduplication of persistent data to reduce storage usage. Capacity deduplication means deduplication performed on the data in hard disk storage (HDD).

> **Note:**
>
> - Capacity deduplication is not enabled by default.
> - Capacity deduplication is available if you have purchased a Nutanix Cloud Infrastructure (NCI) Starter or higher license.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2758

Important: Nutanix recommends that you configure the Controller VMs with at least 32 GiB of RAM and 300 GiB SSDs for the metadata disk for Capacity Deduplication.

How to enable Deduplication

Deduplication is enabled at the storage container level in Prism Central. For information about how to enable deduplication, see Creating a Storage Container (AHV) for AHV, Creating a Storage Container (ESXi) for ESXi or Creating a Storage Container (Hyper-V) for Hyper-V.

Deduplication Best Practices

The following table provides the scenarios where deduplication is recommended and where it is not recommended:

Enable deduplication	Do not enable deduplication
• Full clones • Physical-to-virtual (P2V) migration • Persistent desktops	• *Linked clones or Nutanix VAAI clones*: Duplicate data is managed efficiently by DSF so deduplication has no additional benefit • *Server workloads*: Redundant data is minimal so may not see significant benefit from deduplication

Erasure Coding

Erasure coding increases the usable capacity of a cluster. Instead of replicating data, erasure coding uses parity information to rebuild data in the event of a disk failure. The capacity savings of erasure coding are in addition to deduplication and compression savings.

Important: Erasure coding is supported on clusters with a minimum of 4 nodes when using replication factor 2 and a minimum of 6 nodes when using replication factor 3.

If you have configured 1N/1D cluster fault tolerance, two data copies are maintained. For example, consider a 6-node cluster with 4 data blocks (a b c d). In this example, we start with 4 data blocks (a b c d) configured with 1N/1D cluster fault tolerance.

The white text represents the data blocks and the green text represents the copies.

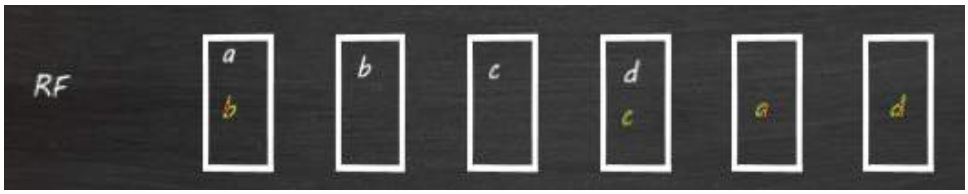


Figure 121: Data copies before Erasure Coding

When the data becomes cold, the erasure code engine performs an exclusive OR operation to compute parity “P” for the data.

Figure 122: During Computing Parity

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2759

After parity is computed, the data block copies are removed and replaced with the parity information. Redundancy through parity results in data reduction because the total data on the system is now a+b+c+d+P instead of 2 × (a+b+c +d).

> **Note:** Each block in the stripe is placed on a separate node to protect from a single node failure.

Figure 123: After Computation of Parity

If the node that contains data block c fails, block c is rebuilt using the rest of the erasure coded stripe (a b d and P) as displayed in the following example:

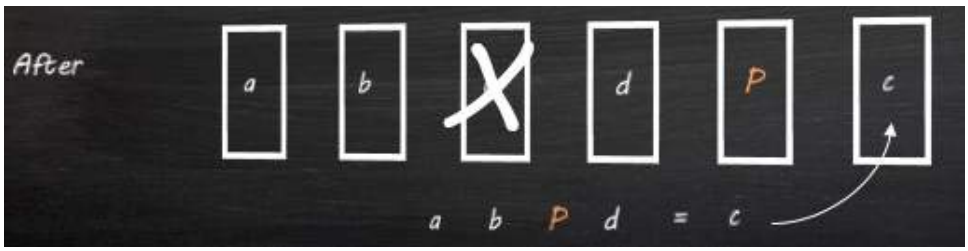


Figure 124: Post Node Failure

Block c is then placed on a node that does not have any other members of this erasure coded stripe.

> **Note:** When the cluster is configured with 2N/2D cluster fault tolerance, two parity blocks are maintained so that the erasure coded data has the same resiliency as the replicated data. An erasure coded stripe with two parity blocks can handle the failure of two nodes.

Example of Data Reduction Savings from Erasure Coding

The space savings from the erasure coding depends on the cluster size, cluster fault tolerance setting, and percentage of cold data.

You can view the data reduction savings from Erasure coding using any of the following methods:

- Access the Storage Container Details View, and observe the following fields:
  - **Erasure Coding** value as *On* in the **Properties** widget.
  - **Data Reduction Savings** in the **Optimization & Performance** widget.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2760

- Access the Storage Containers Summary View, and observe the **Data Reduction Savings** column for the target storage container using any of the following methods:
  - Click the **Lists** tab, and filter the storage containers based on the **Erasure Coding** value as *On*. The system displays the results in the **Lists** page.

    For information about how to use filters, see Filters Pane.
  - Select **Optimization** from the **View by** option and **Erasure Coding** from the **Group by** option. The system displays the results in the **Lists** page with **Erasure Coding: Off** and **Erasure Coding: On**.

In a 6-node cluster configured with replication factor 2, erasure coding uses a stripe size of 5 where 4 nodes are for data and 1 node is for parity. The sixth node in the cluster ensures that if a node fails, another node is available for rebuild. You can view the erasure coding usage savings from the storage container summary.

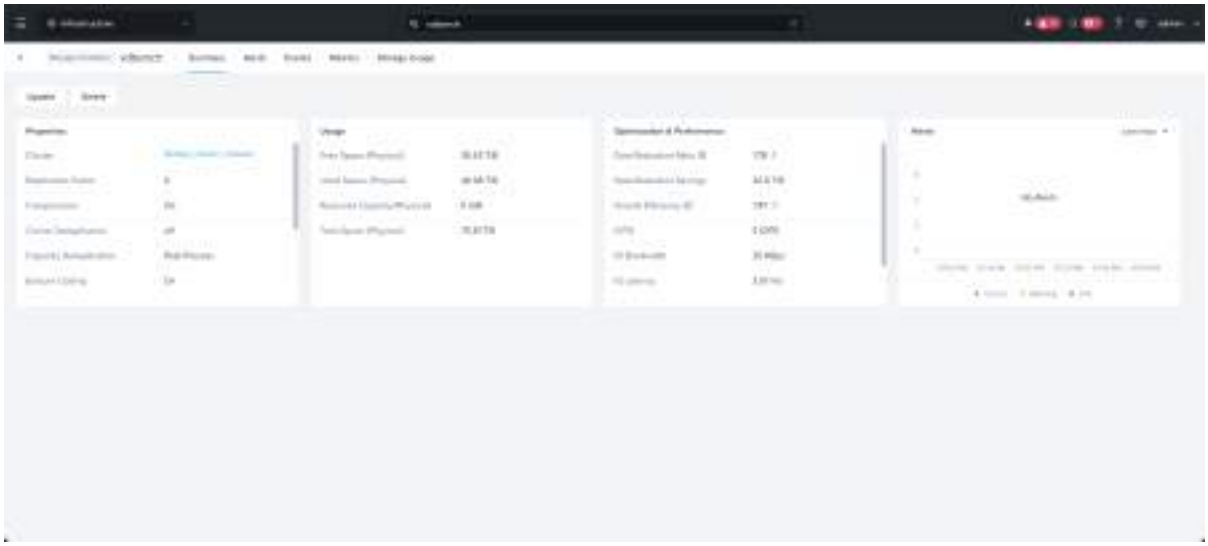


Figure 125: Storage Container Summary: Usage Savings Screen

Erasure coding stripe size adapts to the size of the cluster starting with the minimum 4 nodes with a maximum of 5 node stripe width. The following is an example displaying the various configurations of cluster size, possible stripe widths, and approximate savings that might occur when erasure coding is enabled.

Figure 126: Example of Space Saving from Erasure Coding on 20 TiB Nodes

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2761

Erasure Coding Best Practices and Requirements

Nutanix recommends the following best practices and requirements to implement Erasure Coding:

- A cluster must have at least four nodes/blocks/racks to enable erasure coding. The cluster can have all four flash nodes or a combination of flash and hybrid nodes, or all hybrid nodes. If erasure coding is enabled on a storage container, a minimum of four blocks for replication factor 2 or six blocks for replication factor 3 is required to maintain block awareness.
- The following table provides the information about the recommended minimum configuration for multiple node removal operations:

Table 53: Minimum Recommended Configuration for Erasure Coding

Desired Awareness Type	Cluster Fault Tolerance	Min. Units	Simultaneous Failure Tolerance
Node	1N/1D	4 nodes	1 node
Node	2N/2D	6 nodes	2 nodes
Block	1N/1D	4 blocks	1 block
Block	2N/2D	6 blocks	2 blocks
Rack	1N/1D	4 racks	1 rack
Rack	2N/2D	6 racks	2 racks

> **Note:** Ensure that you maintain a cluster size that is at least one node greater than the combined strip size (data + parity) to allow space to rebuild the strips if a node fails.

- AOS dynamically calculates the erasure coding strip sizes depending on the number of nodes, blocks, and racks. The maximum supported and recommended strip sizes are (4,1) or (4,2), depending on the nodes, blocks, and racks. Nutanix recommends that you do not change the strip size. Greater strip sizes increase the space savings; however, they also increase the cost of rebuild.
- Erasure coding effectiveness (data reduction savings) might reduce on workloads that have many overwrites outside of the erasure coding window. The default value for erasure coding window is seven days for write cold.
- Read performance is affected during rebuild and the amount depends on cluster strip size and read load on the system.
- Erasure coding is an asynchronous process, and hence the time taken to calculate and display space savings depends on the type and coldness of data. A minimum of two full curator scans are required to calculate the data savings.
- Ensure that you have replication factor+1 storage heavy or storage only nodes for all-flash clusters with storage heavy nodes. For example, if you have a four-node replication factor 2 enabled cluster, then you must add a minimum of three storage heavy nodes for optimum performance.

Inline Erasure Coding

Inline erasure coding creates erasure coding strips by erasure coding data without waiting for the data to become write cold.

There are two types of inline erasure coding:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2762

- *Same vDisk strips*: Strips that are created using the data blocks from the same vDisk. Nutanix recommends that you configure inline erasure coding type as same vDisk strips for workloads that do not require data locality.
- *Cross vDisk strips*: Strips that are created using the data blocks across multiple vDisks. Nutanix recommends that you configure inline erasure coding type as cross vDisk strips for workloads that require data locality.

By default, same vDisk strips are created when you enable inline erasure coding.

> **Note:** Inline erasure coding with same vDisk strips can be enabled for clusters running AOS version 5.18 or higher; and with cross vDisk strips can be enabled for clusters running AOS version 6.6 or higher.

Enabling Inline Erasure Coding

Inline erasure coding can be enabled only using nCLI. Inline erasure coding is added as a storage container parameter in Zeus.

Before you begin

> **Caution:**
>
> - Nutanix recommends that you enable inline erasure coding for Object storage containers only. To enable inline erasure coding for any other type of storage container, contact Nutanix Support.
> - Erasure coding must be enabled on the container to enable inline erasure coding. For information about how to enable erasure coding, see Creating a Storage Container on page 294.

Procedure

To enable inline erasure coding, perform the following actions:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2763

- Run the following nCLI command:

  ```
  ncli> container create name=container_name sp-id=storage_pool_id  erasure-code=on
   inline-ec-enabled=true
  ```

  Replace `container_name` and `storage_pool_id` with the storage container name and storage pool ID on which you want to enable erasure coding.

  - To explicitly configure inline erasure coding type, run the following nCLI commands:

    - For inline erasure coding type: *Same vDisk strips*

      ```
      ncli> container create name=container_name sp-id=storage_pool_id  erasure-
      code=on inline-ec-enabled=true inline-ec-type=same-vdisk-strips
      ```

    - For inline erasure coding type: *Cross vDisk strips*

      ```
      ncli> container create name=container_name sp-id=storage_pool_id  erasure-
      code=on inline-ec-enabled=true inline-ec-type=cross-vdisk-strips
      ```

    Replace `container_name` and `storage_pool_id` with the storage container name and storage pool ID on which you want to enable erasure coding.

  - To change an existing inline erasure coding type, run the following ncli commands:

    - To change to *Same vDisk strips*:

      ```
      ncli> container edit inline-ec-enabled=true inline-ec-type=same-vdisk-strips
       id=container_id
      ```

    - To change to *Cross vDisk strips*:

      ```
      ncli> container edit inline-ec-enabled=true inline-ec-type=cross-vdisk-strips
       id=container_id
      ```

    Replace `container_id` with the ID of the storage container.

- To verify if inline erasure coding is enabled, run the following nCLI command:

  ```
  ncli> container ls name=container_name
  ```

  Replace `container_name` with the name of the storage container on which you enabled inline erasure coding.

  The system displays Inline EC Enabled : true if inline erasure coding is enabled.

Capacity Reservation Best Practices

Capacity reservation allows you to guarantee that a storage container has a minimum amount reserved that is unavailable to other storage containers.

By default, each storage container has access to all of the unused storage in the storage pool. If a storage pool consists of multiple storage containers, one storage container might take all the remaining storage space and leave others with no available space. To make sure that there is space available for a storage container, you can enable capacity reservation.

The following best practices are applicable for capacity reservation:

- Reserve capacity for a storage container only if the storage pool consists of multiple storage containers. Unless there is a specific reason to have multiple storage containers, Nutanix recommends you to configure a single storage pool with a single storage container.
- Do not reserve more than 90% of the total space in the storage pool.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2764

- When you set an advertised capacity for a storage container, be aware that some extra space should be allocated beyond the projected size of any VMs placed in the container. This extra space is to allow room for data that is not yet garbage collected. The extra space is based on the workload and can be substantial, for example, 10% or more of the storage capacity in some cases.

Limitations for Storage Containers

Containers with replication factor 1 are not supported in Prism Central. You can create containers with replication factor 1 only from Prism Element.

> **Note:** You cannot update or delete the containers with replication factor 1 from Prism Central.

Creating a Storage Container

This section describes how to create a storage container in a cluster.

Before you begin

Ensure that the following prerequisites are met before you create a storage container in AHV cluster:

- The AHV cluster is configured to synchronize time with NTP servers. For information about how to configure the NTP server, see Configuring NTP Servers for Prism Central in *Prism Central Admin Center Guide*.
- The time on the Controller VMs and Files is synchronization to the current time. If the time on the Controller VMs and Files is ahead of the current time, cluster services might fail to start.

About this task

AOS automatically creates the following type of access to the storage container for each hypervisor:

- *AHV* - Storage container is accessible transparently for AHV.
- *ESXi* - Storage container is accessible as an NFS datastore. In this case, the access to the storage container requires access to the vSphere APIs. Ensure that you have appropriate license of vSphere to access the APIs.
- *Hyper-V* - Storage container is accessible as an SMB share.

Procedure

To create a storage container, follow these steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and go to **Storage** > **Storage Containers** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab as default.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2765

3. Click **Create Storage Container**, and enter the following information:

   a. **Name**: Enter a name for the storage container.

   > **Note:** This entity has the following naming restrictions.
   >
   > - Container Name Length: Maximum length is 75 characters.
   > - Supported Characters: Uppercase and lowercase standard Latin letters (A-Z and a-z), Simplified Chinese, decimal digits (0-9), dots (.), hyphens (-) , hash (#), and underscores (_).
   > - Case Sensitivity: Container names are case sensitive.

   b. **Clusters**: Select a cluster from the dropdown list.

   - If you select an ESXi cluster in the **Clusters** dropdown list, the system prompts you to specify the **NFS Datastore**.
   - If you select a Hyper-V cluster in the **Clusters** dropdown list, the system prompts you to specify any of the following mechanisms to make this storage container a default store for VM configuration and virtual hard disk files on Hyper-V:
     - **Make default on all Hyper-V hosts** - Used to make this storage container as a default store location for all the Hyper-V hosts.
     - **Make default on particular Hyper-V hosts** - Used to make this storage container as default store for selected Hyper-V hosts.

   c. **Max Capacity** *(Read-Only)*: Displays the amount of free physical space available in the selected cluster. For example, 3.48 TiB (Physical Unreserved Capacity).

4. Click **Advanced Settings** to configure the following additional parameters:

   a. **Cluster Fault Tolerance** *(Read-Only)*: Displays the fault tolerance of the cluster that you configured when you created the cluster.

   b. **Replication Factor**: Displays the number of copies of data in the container.

   The default value is based on the cluster fault tolerance that you select when you create the cluster. For more information on cluster fault tolerance, see Cluster Fault Tolerance in the *Prism Web Console Guide*.

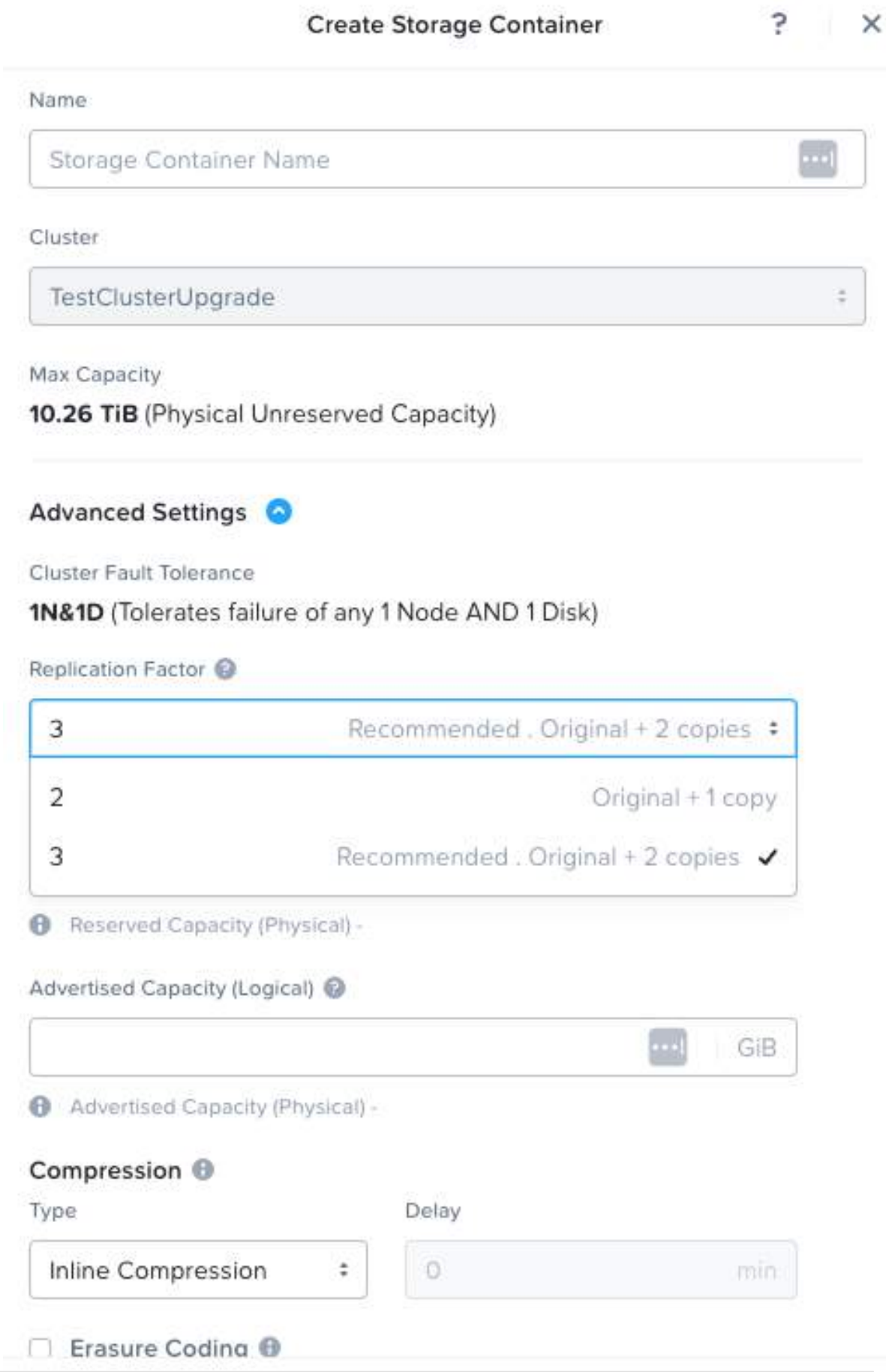
   To modify the replication factor, select the value from the dropdown menu. You can set the replication factor to 1, 2, or 3 depending on the fault tolerance of the cluster. For more information on replication factor, see Replication Factor in the *Prism Web Console Guide*.

   > **Note:**
   >
   > - You can modify the replication factor of a container in a cluster with 1N&1D or 2N/2D cluster fault tolerance. You cannot modify the replication factor of a container in a cluster with 1N/1D cluster fault tolerance; however, you can modify the replication factor of the container after you modify the fault tolerance of the cluster from 1N/1D to 2N/2D. For more information, see Managing Cluster Fault Tolerance on page 412.
   > - Nutanix supports a replication factor of 1, 2, or 3. Nutanix supports a replication factor of 1 if you enable the replication factor 1 setting only. For more information, see Enabling Replication Factor 1 in the *Prism Web Console Guide*. If you do not enable the replication factor 1 setting, Nutanix supports a replication factor of 2 or 3 depending on the fault tolerance configured in

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2766

the cluster. Setting the replication factor to 3 adds an extra layer of data protection at the cost of storing an additional copy of the data.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2767



Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.0075627 pg. 2768

c. **Reserved Capacity (Logical)**: Enter the capacity (in GiB) to reserve storage space for this storage container.

   You can reserve space for a storage container to ensure a minimum storage capacity is available. If you reserving space for a storage container, the reserved space is no longer available to other storage containers even if it is unused. For more information, see Capacity Reservation Best Practices on page 293.

   Reserved Capacity (Physical)*(Read-Only)*: Displays the amount of physical capacity that is reserved based on the logical reserved capacity value.

d. **Advertised Capacity (Logical)**: Enter the capacity (in GiB) to reserve the maximum storage space for this storage container.

   This field is used to set an advertised capacity, which is the maximum storage size that the storage container can use. This can be set to any value, but if you configure **Reserved Capacity**, ensure that you set the advertised capacity greater than or equal to the **Reserved Capacity** for the storage container. The hypervisor ensures that the storage does not go beyond the advertised capacity of the storage container.

   Advertised Capacity (Physical) *(Read-Only)*: Displays the amount of physical capacity that is advertised based on the logical advertised capacity value.

e. **Deduplication**: Select the **Capacity** checkbox under **Deduplication** to optimize performance by performing post-process deduplication of persistent data.

   Capacity deduplication is primarily recommended for full clone, persistent desktops, and physical to virtual migration use cases that need both storage capacity savings and performance savings from deduplication. For more information, see Capacity Deduplication on page 287 information.

f. **Compression**: Select the **Compression** checkbox to compress all the data in the storage container.

   For more information about data compression, see Compression on page 286.

   By default, **Inline compression** is selected in the **Type** field and **0** is selected in the **Delay** field (In Minutes) which indicates that the data is compressed immediately as it is written.

   To configure the delay time between the write and compression, under **Type** field, select **Post Process Compression** from the dropdown menu. For post-process compression, where data is compressed after it is written, Nutanix recommends that you set a delay of 60 minutes to delay the compression activity for 60 minutes after the initial write operation.

g. **Erasure Coding**: Select the **Erasure Coding** checkbox to enable erasure coding. Erasure coding increases the effective or usable capacity on a cluster. For more information about erasure coding, see Erasure Coding on page 288.

h. **Filesystem allowlists**: Enter the comma-separated IP address and netmask value in the form `ip_address/netmask`.

   An allowlist is a set of addresses that are allowed access to this storage container. Allowlists are used to allow appropriate traffic when unauthorized access from other sources is denied. If you set an allowlist at storage container level, the system overrides any global allowlist for this storage container.

   Setting an allowlist helps you provide access to the container via NFS. Some manual data migration workflows might require the allowlist to be configured temporally, while some third-party backup vendors might require the allowlist to be configured permanently to access the container via NFS.

   Caution:

   - User authentication is not available for NFS access, and the IP address in the allowlist has full read or write access to the data on the container.
   - Nutanix recommends to allow single IP addresses (with net mask such as 255.255.255.255) instead of allowing subnets (with netmask such as 255.255.255.0).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2769

5. Click **Create**.
   The system creates a storage container in the cluster.

Modifying a Storage Container

A storage container is a defined subset of available storage within a storage pool that can be modified as conditions change.

About this task

Storage containers can be modified to change how the data in that storage container is handled. For example, apply compression to the storage container.

> **Note:** You cannot rename a storage container if any of the following conditions is met:
>
> - The cluster is the AHV cluster.
> - Storage container include vdisks.

To modify a storage container, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select **Infrastructure** application from Application Switcher Function on page 45, and go to **Storage** > **Storage Containers** from the **Navigation Bar**.
   For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab as default.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2770

3. Select the target storage container checkbox, and choose **Update** from the **Actions** dropdown menu. The system displays the **Update Storage Container** window.

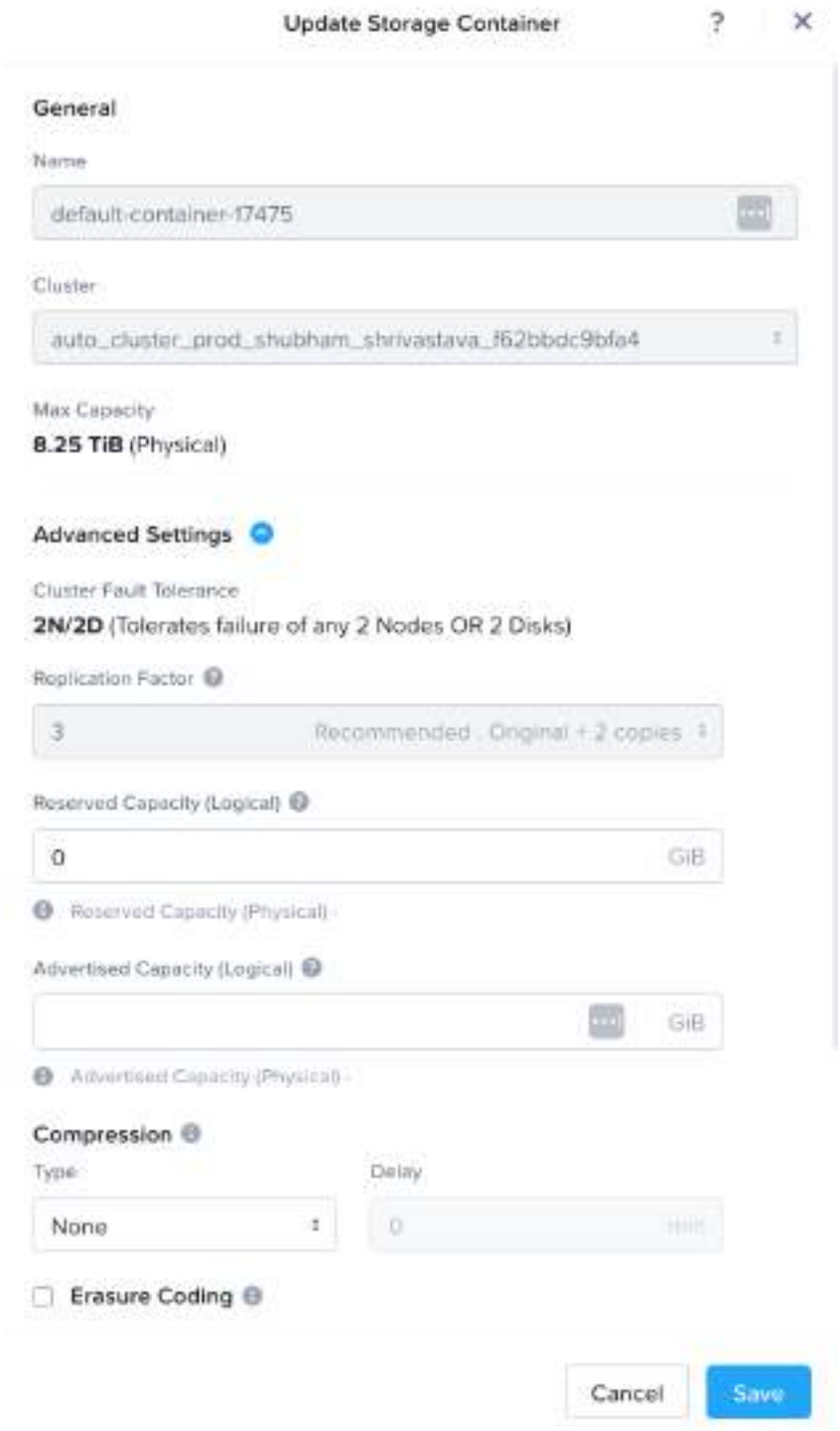


Figure 127: Update Storage Container

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2771

4. Update the storage container configuration as per your requirement, and click **Save**.

   The fields that appear in **Update Storage Container** and **Create Storage Container** windows are same. For field details, see Creating a Storage Container on page 294.

   Note:

   - If the compression policy is changed from compressed to uncompressed (or vice versa), the existing compressed (uncompressed) data in the storage container will be uncompressed (compressed) as a background process when the next data scan detects the data that needs this change.
   - You can modify the replication factor of a container in a cluster with 1N&1D or 2N/2D cluster fault tolerance. You cannot modify the replication factor of a container in a cluster with 1N/1D cluster fault tolerance; however, you can modify the replication factor of the container after you modify the fault tolerance of the cluster from 1N/1D to 2N/2D. For more information, see Managing Cluster Fault Tolerance on page 412.

Deleting a Storage Container

A storage container is a defined subset of available storage within a storage pool that can be deleted.

About this task

Note: A SelfServiceContainer storage container is created on the target cluster and used by Prism Self Service for storage and other feature operations. To ensure proper operation of these features, do not delete this storage container. For more information about Prism Self Service, see Prism Self Service Administration on page 530.

To delete a storage container, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Storage** > **Storage Containers** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab as default.
3. Select the target storage container checkbox, and choose **Delete** from the **Actions** dropdown menu.
   The system prompts you to confirm the delete action.
4. Click **Delete**.
   The selected storage container is deleted from the cluster.

Volume Group Management

Volumes act as one or more targets for client Windows or Linux operating systems running on a bare metal server or as guest VMs using iSCSI initiators. You can use any storage available in any new or existing Nutanix cluster for Volumes.

Note: Do not use volumes to create an iSCSI datastore to Hyper-V or ESXi hosts. This configuration is not supported.

- The **Summary** tab on the **Volume Groups** page displays information about volume groups across the registered clusters. For more information, see Volume Groups Summary View on page 302.
- The **Summary** tab on the individual volume group page displays the detailed information about the selected volume group. For more information, see Volume Group Details View on page 307.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2772

- For more information about volumes and volume groups, see Volumes Guide.

You can create and update volume groups directly from Prism Central web console.

- For information about how to create a volume group, see Creating a Volume Group on page 315.
- For information about how to modify a volume group, see Modifying a Volume Group on page 321.

You can configure CHAP secret password from the Prism Central web console. For more information, see Configuring Mutual CHAP Authentication on page 324

You can attach volume groups to guest VMs from the Prism Central web console. For more information, seeAttaching Volume Groups to Guest VMs on page 325

You can also define the Cluster Role Based Access Control (RBAC) for a volume group. For details, see Cluster RBAC for Volume Group on page 325

Volume Groups Summary View

The **Summary** tab in **Volume Groups** page displays information about volume groups across the registered clusters and allows you to access detailed information about each volume group.

To access the summary view of all volume groups, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Storage** > **Volume Groups** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The **Volume Groups** page includes these tabs on the top (**Summary**, **List**, **Alerts**, and **Metrics**) with a display area below the selected tab.

   The system displays the **List** tab by default with all the volume groups across registered clusters.
3. Click the **Summary** tab.

   The system displays **Summary** page.

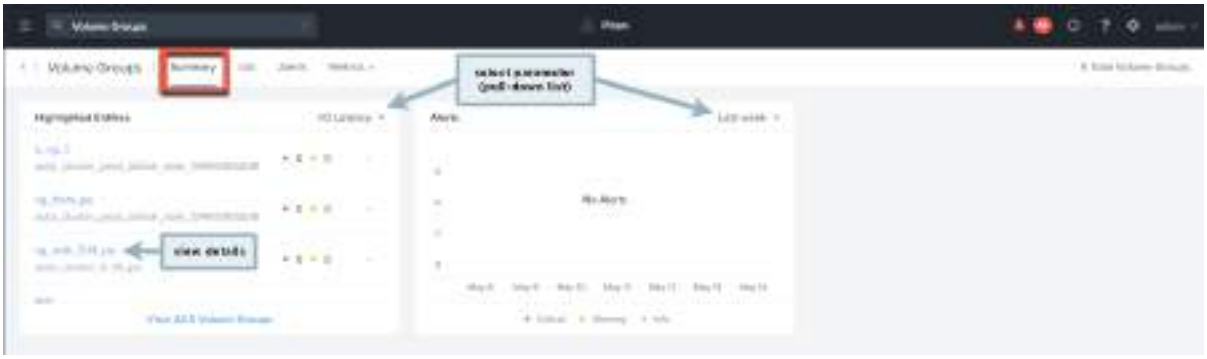


Figure 128: Summary Page - All volume Groups

The **Summary** tab of all volume groups displays the following widgets:

- **Highlighted Entities**: Displays a list of the volume groups with the highest usage of the parameter you select from the pull-down menu on the right of the widget. The options are **IO Latency**, **IOPS**, and **IO Bandwidth**. Click the name to display the details page for that volume group. Click the **View all XX Volume Groups** link at the bottom to display the **List** tab.
- **Alerts**: Displays a list of volume group-related alerts that occurred during the specified interval. Select **Last 24 hours** (default), **Last week**, or **Last Hour** from the drop-down menu.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2773

List Tab

The **List** tab displays the list of volume groups across all clusters.

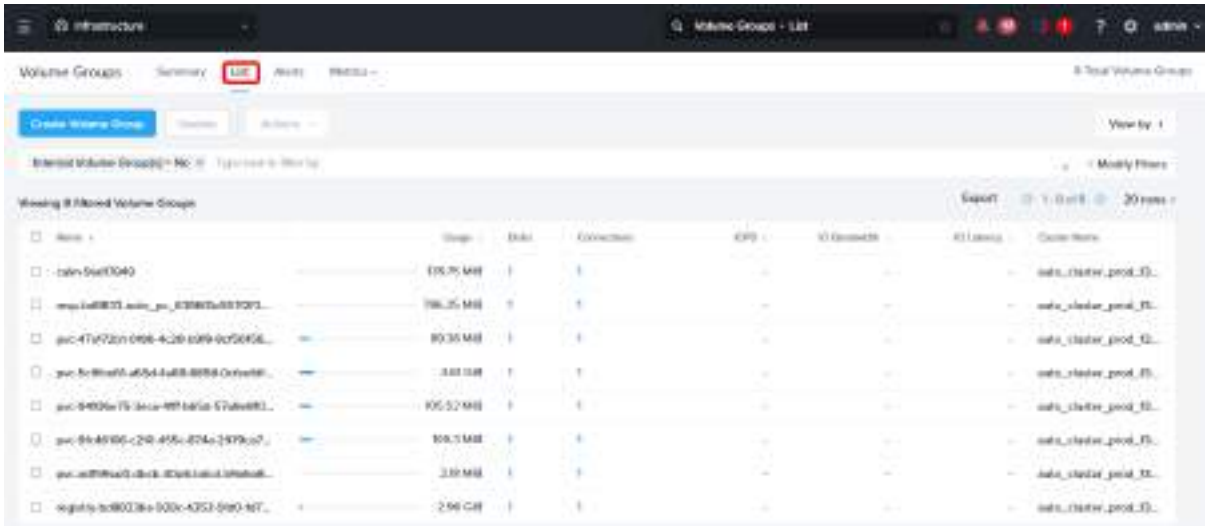


Figure 129: Volume Groups List Tab

The following table describes the fields that appear in the **List** tab of **Volume Groups** page:

> **Note:** The fields vary based on the **View by** and **Group by** options. A dash (-) is displayed in a field when a value is not available or applicable. For more information about **View by** and **Group by** options, see Prism Central GUI Organization on page 54.

Table 54: Volume Groups List Tab - Field Description

Parameter	Description	Values
Select **General** from **View by** option.		
Name	Displays the name of the volume group. You can click the volume group name to view the details page for that volume group. For information about volume group details, see Volume Group Details View on page 307. **Note:** An exclamation point appears if the cluster is running a pre-6.0 AOS version, which indicates the available information and actions are limited.	*<Volume _Group_Name>*
Usage	Displays the amount of used storage space. A bar also appears that graphically indicates the amount of used and free storage space available in the volume group. When you hover the cursor over the bar, the system displays a window that lists the used space, free space, and total space in the volume group.	xxx [GiB|TiB]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2774

Parameter	Description	Values
Disks	Displays the number of virtual disks in the volume group. You can click the number to view the **Virtual Disks** tab in the Volume Group Details View on page 307.	(integer)
Connections	Displays the number of external client connections to the volume group. You can click the number to view the **Connections** tab in the Volume Group Details View on page 307.	(integer)
IOPS	Displays the current I/O operations per second (IOPS) for the volume group. The controller IOPS, I/O bandwidth, and I/O latency fields record the I/O requests serviced by the Controller VM. The I/O can be served from memory, cache (SSD), or disk.	[0 - unlimited]
IO Bandwidth	Displays I/O bandwidth used per second for Controller VM-serviced requests in this volume group.	xxx [MBps|KBps]
IO Latency	Displays the average I/O latency for Controller VM-serviced requests in this volume group.	xxx [ms]
Cluster Name	Displays the name of the cluster in which the volume group resides. You can click the cluster name to view the cluster details. For information about cluster details, see Cluster Details View on page 405.	(cluster name)
Select **Data Protection** from **View by** option.		
Name	Displays the name of the volume group. You can click the volume group name to view the details page for that volume group. For information about volume group details, see Volume Group Details View on page 307. **Note:** An exclamation point appears if the cluster is running a pre-6.0 AOS version, which indicates the available information and actions are limited.	*<Volume _Group_Name>*
Category	Displays the category of the volume group. For information about categories in Prism Central, see Category Management on page 456.	String (Category name)
Consistency Group	Displays the consistency group of the volume group. For information about Consistency Groups in Prism Central, see Consistency Groups information in *Nutanix Disaster Recovery Guide* .	Yes/No
Protection Status	Displays the Protection Status of the volume group.	Protected/Unprotected
Protection Type	Displays the type of protection defined for the volume group.	Protection Policy

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2775

Parameter	Description	Values
Protection Policy	Displays the protection policy that is applicable for the VM. For more information about protection policies, see Nutanix Disaster Recovery Guide.	(String) Protection Policy Name
Recovery Plan	Displays the recovery plans that is applicable for the volume group. For more information about VG recovery plans, see Nutanix Disaster Recovery Guide.	(String) Recovery Plans Name

You can perform the following actions for the storage containers in the **Lists** tab:

- Access the detailed information about an individual volume group. For more information, seeVolume Group Details View on page 307.
- Filter the volume groups list based on available parameter values using **Filters** pane. For more information about **Filters** pane, see Filters Pane - Volume Groups Page on page 305.
- Export the table that contains the list of volume groups and their information to a file in a CSV format. For more information about **Export** option, see Export on page 59.
- Group the volume groups based on pre-defined criteria. For information about how to group the storage containers, see Group by on page 56.
- View volume groups based on pre-defined criteria or create a custom view. For information about available views and how to create a custom view, see View by on page 56.
- Create a volume group. For more information about how to create a storage container, see Creating a Volume Group on page 315.
- Perform the actions specific to storage container on a single or multiple storage containers using the **Actions** dropdown menu. For instructions on how to perform these actions, seeModifying a Volume Group on page 321.

  Note: The **Actions** dropdown menu is grayed out unless you select a volume group.

Filters Pane - Volume Groups Page

The following table describes the fields available in the **Filters** pane:

Table 55: Filter Pane Fields - Volume Groups

Parameter	Description	Values
Name	Filters based on the volume group name. Select a condition from the dropdown menu and enter a string in the field. The system returns a list of storage containers that satisfy the storage container name condition/string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	(volume group name string)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2776

Parameter	Description	Values
Usage	Filters on the used storage space for a volume group. Check the box for the desired range or enter an amount range in the "**from <low> to <high> GiB**" field. It returns a list of volume groups with used storage in that range.	([xx] to [yy] GiB range)
Cluster Name	Filters based on the cluster name. Select a condition from the dropdown menu and enter a string in the field. The system returns a list of storage containers that satisfy the cluster name condition/string.	(cluster name string)
Category	Filters based on category names. Enter a category name in the field and then check the box. As you type a dropdown menu appear to help you select the correct category. A new field appears where you can add more categories to the filter. The number of volume groups tagged to each selected category are displayed in the **List** tab.	(category name)
IOPS	Filters based on the current IOPS. Check the box for the desired range or enter a range in the ***From <low> to <high> iops*** field. It returns a list of volume groups with IOPS in that range.	([xx] to [yy] IOPS range)
IO Bandwidth	Filters based on the I/O bandwidth used. Check the box for the desired range or enter a range in the ***From <low> to <high> MBps*** field. It returns a list of volume groups with I/O bandwidth usage in that range.	([xx] to [yy] MBpS range)
IO Latency	Filters based on the average I/O latency. Check the box for the desired range or enter a range in the ***from <low> to <high> ms*** field. It returns a list of volume groups with average I/O latency in that range.	([xx] to [yy] ms range)
Internal Volume Group(s)	Filters based on the volume group names specified	Yes | No

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options that are available on the **Activity** > **Alerts** page, however it only displays the alerts related to storage containers across the registered clusters. For more information about alerts, see *Prism Central Alerts and Events Reference Guide*.

Metrics Tab

The **Metrics** tab allows you to view performance metrics across the volume groups. Click the **Metrics** tab to display dropdown menu of available metrics, and select the metric name to display the relevant performance information.

> **Note:** The **Metrics** dropdown menu is hypervisor-specific, and might vary based on the hypervisors used in the cluster.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2777

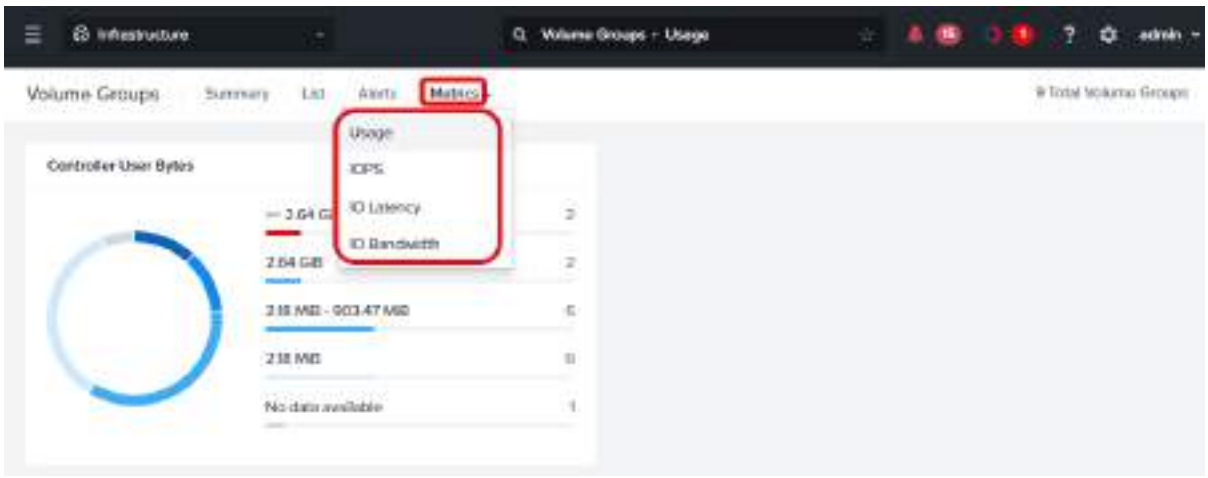


Figure 130: Volume Groups Metrics Tab

Table 56: Metrics Tab Fields

Metric	Description
Usage	Displays volume group usage graph.
IOPS	Displays total, read, and write IOPS graphs listing current values and total volume groups (number). The current values are split into intervals (for example, less than 700, 700-1400, 1400-2000, more than 2000). **Note:** The same format also applies to the other metrics in this table.
IO Latency	Displays total, read, and write I/O latency rate graphs.
IO Bandwidth	Displays total, read, and write I/O bandwidth rate graphs.

Volume Group Details View

To access the details view of an individual volume group, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Storage** > **Volume groups** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The system displays the **List** tab by default with all the volume groups across registered clusters.
3. Click the target <*Volume_Group_Name*> to view the **Summary** tab of an individual volume group.

   Note: Replace <*Volume_Group_Name*> with the actual storage container name at your site.

The following is an example showing the **Summary** tab of an individual volume group:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2778

Figure 131: Summary Tab - Individual Volume Group

The **Summary** tab of an individual volume group provides the following widgets:

- **Properties** - Displays summary information about the volume group. For information about the fields available in **Properties** widget, see Table 57: Volume Group Widgets - Field Description on page 308.
- **Usage and Performance** - Displays the usage and performance data for the volume group. For information about the fields available in **Usage and Performance** widget, see Table 57: Volume Group Widgets - Field Description on page 308.
- **Alert**- Displays a list of related alerts that occurred during the specified interval. Select either **Last week** (default), **Last 1 hour** or **Last 24 hours** from the dropdown menu on the top right corner of the widget.

<*Action*> available above the widgets. Click the appropriate <*Action*> to run that administrative action on the volume group. For more information about how to perform any <*Action*>, see Modifying a Volume Group on page 321.

Volume Group Widgets - Parameter Details

The following table describes the fields available in the **Properties** and **Usage and Performance** widgets. A dash (-) in a field indicates that there is not enough data to evaluate or a value is not assigned. The displayed fields vary by hypervisor.

Table 57: Volume Group Widgets - Field Description

Parameter	Description	Values
Properties widget		
IP Addresses	Displays the IP address assigned to the volume group.	(IP address)
Cluster	Displays the name of the cluster in which the volume group resides. You can click the name to view the detailed information about the cluster. For more information, see Cluster Details View on page 405).	(cluster name)
Flash Mode	Displays whether Flash Mode is enabled for the volume group.	[Enabled, Disabled]
Virtual Disks	Displays the number of virtual disks in the volume group. You can click the numeric value to view the **Virtual Disks** tab.	(integer)
Connections - External Clients	Displays the number of external client connections to the volume group. You can click the numeric value to view the **Connections** tab.	(integer)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2779

Parameter	Description	Values
iSCSI Target Name	Displays the name of the iSCSI target.	(ISCSI name)
Cluster	Displays the name of the cluster in which the volume group resides. You can click the cluster name to view the cluster details. For more information, see Cluster Details View on page 405.	(cluster name)
Usage and Performance Widget		
Free Space (Logical)	Displays the amount of logical (effective) free space available in the volume group. **Note:** Logical space accounts for the volume group replication factor. Replication factor 1 means the logical and physical spaces are the same, replication factor 2 means the logical space is half the physical space, and replication factor 3 means the logical space is a third of the physical space.	xxx [GiB|TiB]
Used Space (Logical)	Displays the amount of logical used space in the volume group.	xxx [GiB|TiB]
Total Space (Logical)	Displays the amount of logical total space in the volume group.	xxx [GiB|TiB]
IOPS	Displays the current I/O operations per second (IOPS) for the volume group. The controller IOPS, I/O bandwidth, and I/O latency fields record the I/O requests serviced by the Controller VM (CVM). The I/O can be served from memory, cache (SSD), or disk.	[0 - unlimited]
IO Bandwidth	Displays I/O bandwidth used per second for Controller VM-serviced requests in this volume group.	xxx [MBps|KBps]
IO Latency	Displays the average I/O latency for Controller VM-serviced requests in this volume group.	xxx [ms]
Storage Attributes		
Virtual Disks	Displays the number of virtual disks associated with the VG.	(integer)
Defined via	Displays the entity that defines the storage attributes of the VG. The storage attributes of the VG could be inherited from the storage properties of the cluster or applied by a Storage Policy. See Storage Policy Management on page 506 for more information.	(System Default, <Name of Storage Policy>
Replication Factor	Displays the Replication Factor selected.	Inherit from Container or 2 or 3

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2780

Parameter	Description	Values
Encryption	Displays the encryption mode selected.	Enabled or Inherit from Cluster
Compression	Displays the compression mode selected.	Inline or Post Process (if On) Off Inherit from Cluster
Throttled Throughput (IOPS)	Displays the throttled throughput value in terms of IOPS.	(Integer number)
Throttled Throughput (MB/s)	Displays the throttled throughput value in MBps.	(Integer number)

For information about Storage Policies, see Storage Policy Management on page 506.

Virtual Disks Tab

Click the **Virtual Disks** tab to view a list of virtual disks for the volume group.

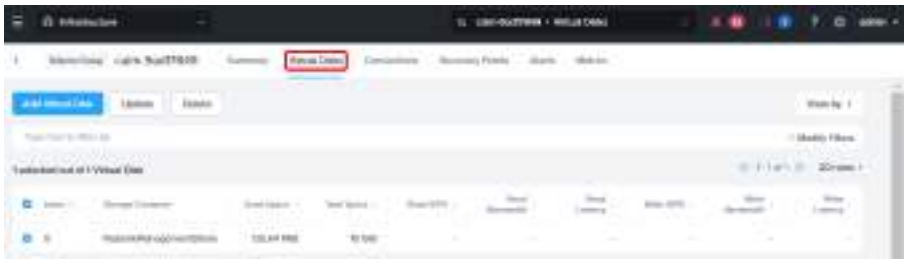


Figure 132: Virtual Disks Tab

You can perform the following actions for the virtual disks in the **Virtual Disks** tab:

- Filter the Virtual Disks list based on available field values using **Filters** pane. For more information about how to use the **Filters** pane, see Filters Pane on page 55.
- View Virtual Disks based on pre-defined criteria or create a custom view. For information about available views and how to create a custom view, see View by on page 56.
- Add, update, and delete a virtual disk. For more information about how to manage a virtual disk, see Modifying a Volume Group on page 321.

> **Note:** The available actions appear in bold; other actions are grayed out. For grayed out options, a tool tip explaining the reason is provided. The available actions depend on the current state of the selected VM(s).

The following table describes the fields that appear in the list. A dash (-) is displayed in a field when a value is not available or applicable:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2781

Table 58: Virtual Disks - Field Description

Fields	Description	Values
Select **General** from **View by** option.		
Index	Displays the index number assigned to the virtual disk.	(integer)
Storage Container	Displays the name of the storage container in which the virtual disk is located.	(container name)
Used Space	Displays the amount of used space in the virtual disk.	xxx [GiB|TiB]
Total Space	Displays the total amount of storage space in the virtual disk.	xxx [GiB|TiB]
Read IOPS	Displays the current read I/O operations per second (IOPS) for the virtual disk.	[0 - unlimited]
Read Latency	Displays the average read I/O latency for the virtual disk.	xxx [ms]
Read Bandwidth	Displays read I/O bandwidth used per second for the virtual disk.	xxx [MBps|KBps]
Write IOPS	Displays the current write I/O operations per second for the virtual disk.	[0 - unlimited]
Write Latency	Displays the average write I/O latency for the virtual disk.	xxx [ms]
Write Bandwidth	Displays write I/O bandwidth used per second for the virtual disk.	xxx [MBps|KBps]
Select **+Add Custom** from **View by** option to create a custom view with the following additional fields:		
IOPS	Displays the current total I/O operations per second for the virtual disk.	
IO Bandwidth	Displays the total I/O bandwidth used per second for the virtual disk.	
IO Latency	Displays the average I/O latency for the virtual disk.	
Nutanix File Path	Displays the path of the storage file in Nutanix File server. For information about Nutanix Files, see Nutanix Files User Guide.	File path. For example `/home/nutanix/`

The following table describes the **Filters** pane of **Virtual Disks** tab:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2782

Table 59: Filters Pane - Virtual Disks Tab

Field	Description	Values
Storage container	Filters based on the Storage Container name. Select a condition from the dropdown menu and enter a string in the field. The system returns a list of virtual disks that satisfy the Storage container name condition/string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	(storage container name string)
[Total|Used] Space	Filters based on the total or used storage space for a virtual disk. Enter an amount range in the **From : <low> To: <high> GiB** field. The system returns a list of virtual disks with total or used storage in that range.	([xx] to [yy] GiB range)
[Read|Write] IOPS	Filters based on the current read or write IOPS. Enter a range in the **From : <low> To: <high> IOPS** field. It returns a list of virtual disks with IOPS in that range.	([xx] to [yy] range)
[Read|Write] Bandwidth	Filters based on the read or write I/O bandwidth used. Enter a range in the **From : <low> To: <high> MBps** field. It returns a list of virtual disks with I/O bandwidth usage in that range.	([xx] to [yy] range)
[Read|Write] Latency	Filters on the average I/O latency. Enter a range in the **From : <low> To: <high> ms** field. It returns a list of virtual disks with average I/O latency in that range.	([xx] to [yy] range)

Connections Tab

Click the **Connections** tab to view a list of external client connections to the volume group.

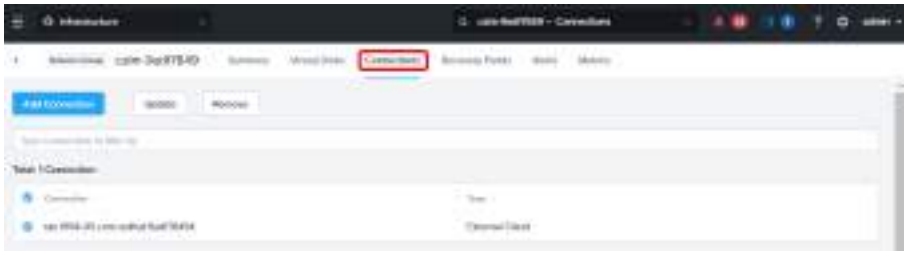


Figure 133: Connections Tab

You can add, update, and delete an external connection for the volume group. For more information about how to manage a volume group connection, see Modifying a Volume Group on page 321.

Note: The available actions appear in bold; other actions are grayed out. For grayed out options, a tool tip explaining the reason is provided. The available actions depend on the current state of the selected VM(s).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2783

The following table describes the fields that appear in the list. A dash (-) is displayed in a field when a value is not available or applicable:

Table 60: Connections - Field Description

Field	Description	Values
Connection	Displays the IP address or IQN of the external client.	(IP or IQN address)
Type	Displays the type of connection.	external client

Recovery Point Tab

Click the **Recovery Point** tab to view a list of recovery points created with the selected volume group.

Figure 134: Recovery Points Tab

You can clone, revert, replicate, and delete a recovery point of the volume group. For more information about how to manage a volume group recovery points, see Nutanix Disaster Recovery Guide.

The following table describes the fields that appear in the list. A dash (-) is displayed in a field when a value is not available or applicable:

Table 61: Recovery Point - Field Description

Field	Description	Values
Create Time (Name)	Displays the name of the VG recovery point. By default, the system displays the VG recovery point creation time as the name when you create a VG recovery point, however you can change it as per your requirement.	(Name)
Location	Displays the location where the VG recovery point is created in *AZ location:Cluster name* format.	Local AZ : auto_cluster_prod_f38293eb9649
Replicated From	Displays the location from where the VG recovery point is replicated in *AZ location:Cluster name* format.	
Reclaimable Space	Displays the space that can be reclaimed for the VG group recovery point.	(Integer) B. For example, 0 B

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2784

Field	Description	Values
Expiry	Displays the expiry time of the VG group recovery point.	Timestamp in hh:mm AM/PM, DD MM YYYY. For example, 7:57 PM, 18 Feb 2091
Owner	Displays the owner name.	-
Action	Displays the applicable actions for the VG recovery point.	-

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options as the Alerts dashboard, however it is filtered to display the alerts only for the selected volume group (individual volume group). For more information about alerts, see Prism Central Alerts and Events Reference Guide.

Metrics Tab

The **Metrics** tab allows you to view usage metrics for the storage container. Click the **Metrics** tab to view graphs for all the metrics. The graph is a rolling time interval performance or usage monitor. The baseline range appears as a blue band in the graph.

> **Note:** The baseline range and identified anomalies are based on sophisticated machine-learning capabilities. For more information, see Behavioral Learning Tools in *Intelligent Operations Guide*. The machine-learning algorithm uses 21 days of data to monitor and predict performance. A graph or baseline band may not appear if less than 21 days of data is available.

You can perform the following actions in the **Metrics** tab:

- Place the cursor anywhere on the horizontal axis to display the value at that time.
- Select the duration (time interval) from the dropdown menu on the right (Last 1 hour, Last 24 hours, and Last week).
- From the **Actions** dropdown menu that appears on the top-right corner of each metrics widget, you can perform the following operations:
  - Select **Add to Analysis** to add the selected metric to **Analysis** dashboard. For more information, see Analysis Dashboard in *Intelligent Operation Guide*.
  - Choose **Select Analysis Session** to assign the metric to a target session.
- Click the **Filters** option to select one or more appropriate metric checkboxes to display the selected metrics in the **Metrics** page.

The following table describes the metrics available in **Metrics** tab:

> **Note:** Metrics are hypervisor-dependant, and might not be available on all hypervisors.

Table 62: Metrics Tab Fields

Metric	Description
Usage	

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2785

Metric	Description
Controller IOPS	Displays the graph for total I/O operations per second (IOPS) for the controller.
Controller Read IOPS	Displays the graph for Read I/O operations per second (IOPS) for the controller.
Controller Write IOPS	Displays the graphs for Write I/O operations per second (IOPS) for the controller.
Controller AVG I/O Latency	Displays the graph for average latency of total I/O operations (in milliseconds) for controller
Controller AVG Read I/O Latency	Displays the graph for average latency of Read I/O operations (in milliseconds) for controller
Controller AVG Write I/O Latency	Displays the graph for average latency of Write I/O operations (in milliseconds) for controller
Controller I/O Bandwidth	Displays the graph for total I/O bandwidth used per second (MBps or KBps) by controller.
Controller Read I/O Bandwidth	Displays the graph of bandwidth used per second (MBps or KBps) for Read I/O operations by controller
Controller Write I/O Bandwidth	Displays the graph of bandwidth used per second ((MBps or KBps) for Write I/O operations by controller.

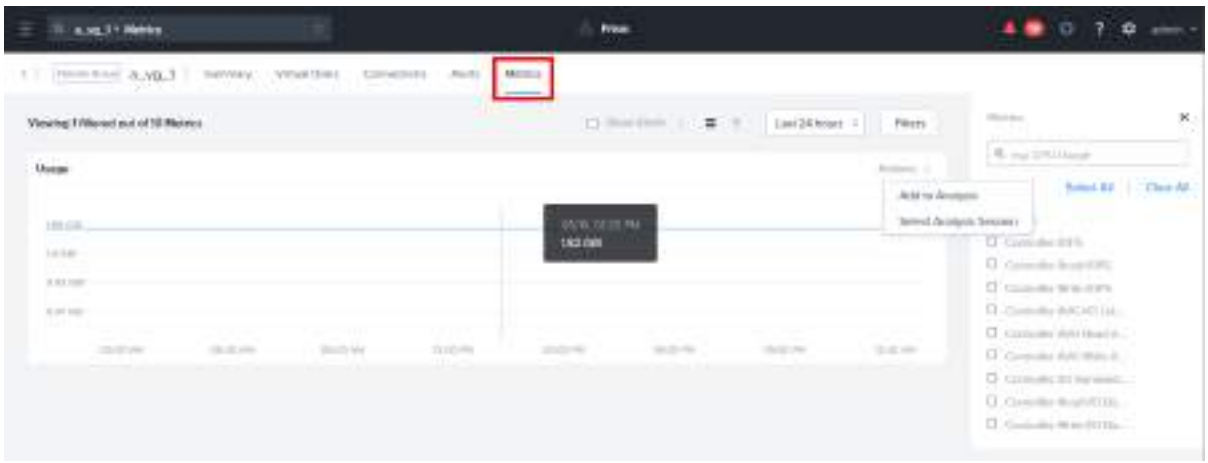


Figure 135: Metrics Tab

Creating a Volume Group

This section describes how to create a volume group in Prism Central.

Procedure

To create a volume group, perform the following steps:

1. Log in to Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2786

2. Select **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Storage** > **Volume Groups** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default with all the volume groups across registered clusters.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2787

3. Click **Create Volume Group**. The system displays the **Create Volume Group** window - **Configuration** step.

   a. In the **Configuration** step, perform the following actions:

   - **Name**: Enter a name for the volume group.
   - **Description**: Enter an optional description for the volume group.
   - **Cluster**: Select the cluster from the dropdown menu in which you want to create the volume group.

     The list includes all clusters registered with the Prism Central.
   - **iSCSI Target Name Prefix**: Enter the iSCSI target name prefix.
   - **Virtual Disks**: Click **Add Disk**. In the **Add Virtual Disk** window, select the target storage container from the **Storage Container** dropdown menu, enter the disk size (in GiBs) in the **Size** field, and then click **Add**.

     Repeat this action to add additional disks.

     To edit or delete a disk, click Edit icon or Delete icon available under **Actions** column.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2788

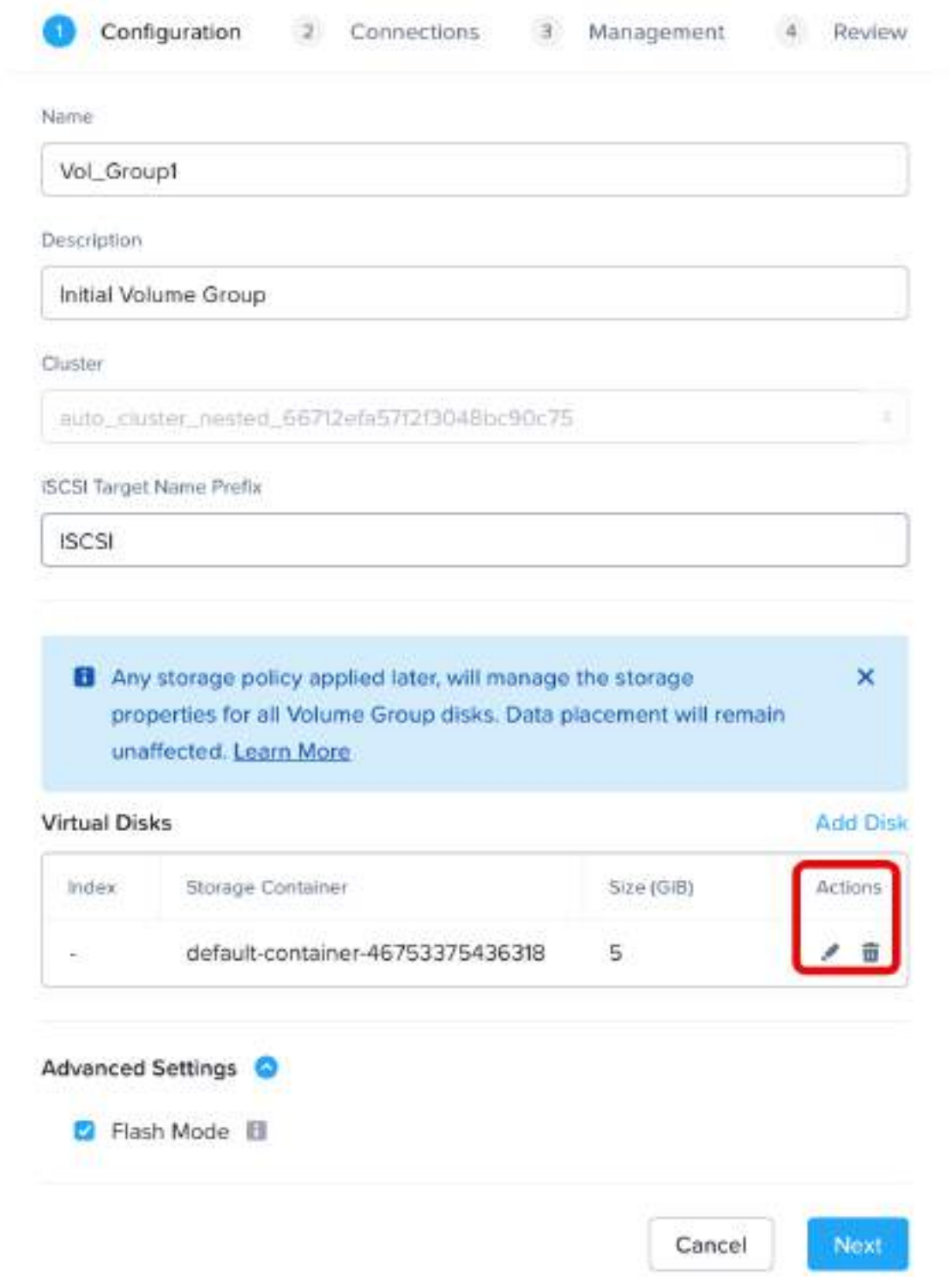


Figure 136: Edit Virtual Disk window

- **Advanced Settings** (optional): Select the **Flash Mode** checkbox to ensure no down migration of data occurs from the flash tier.

b. Click **Next**. The system displays the **Connections** step in **Create Volume Group** window.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2789

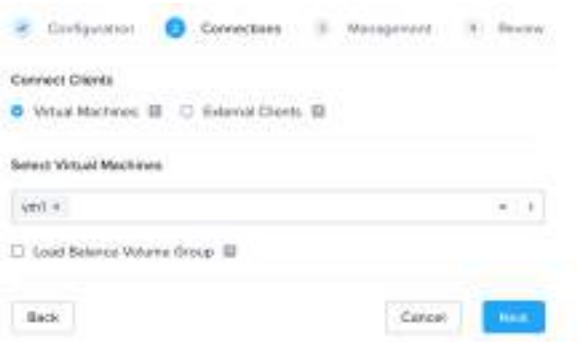


Figure 137: Connections - Virtual Machines

c. In the **Connections** step, perform the following actions:

- **Connect Clients**: Select either of the following options based on your requirement:
  - **Virtual Machines** - Allows you to configure direct attachment to VMs on the same cluster. If you select this option, set the following attributes:
    - **Select Virtual Machines**: Select one or more VMs using the dropdown menu.
    - (Optional) **Load Balance Volume Group**: Select the checkbox to enable load balancing between the selected VMs. Virtual disks in the volume group are evenly distributed between the CVMs instead of being hosted locally.

      Note: You cannot change the load balance configuration once you attach the VMs.
  - **External Clients** - Allows you to configure access to external clients or clients not residing on the same cluster.

    The following is an example showing the **External Clients** selection window:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2790

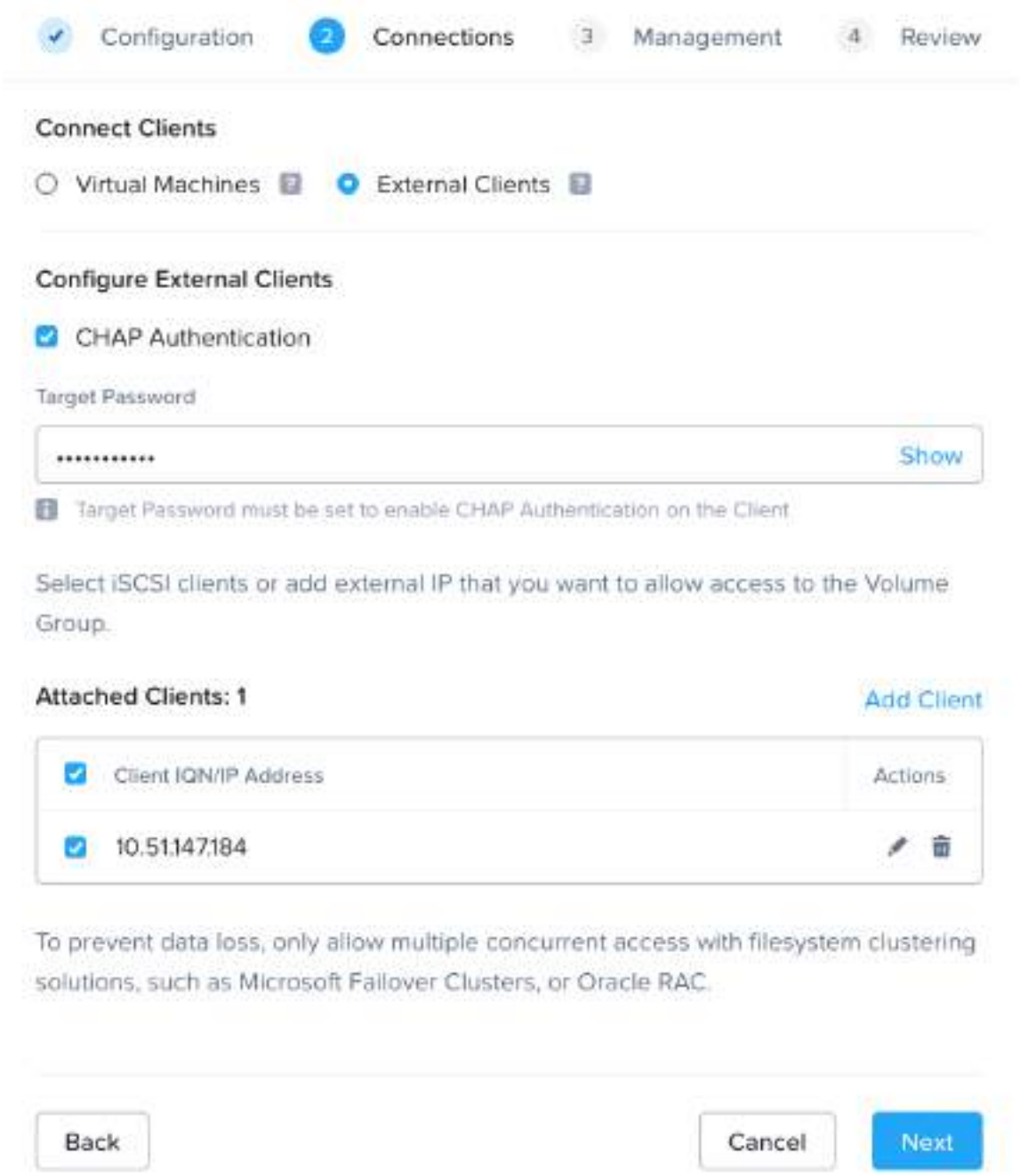


Figure 138: Connections - External Clients

If you select this option, set the following attributes:

- **Configure External Clients**: Select the **CHAP Authentication** checkbox to enable the Challenge Handshake Authentication Protocol (CHAP) on the external client, and enter the target password in the indicated field.
- **Attached Clients**: Configure the external clients as desired. The configured clients appears in a table.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2791

- To attach (detach) a client, select (clear) the box for that client in the table.
- To add a client, click the **Add Client** link. In the **Add External Client** window, enter the client IP address or IQN designator name in the **Client IQN/IP Address** field, select the **CHAP Authentication** checkbox , and enter password in the **Client Password** field, and then click **Add**. The added client appears in the table.
- To update a client, click the Edit icon for that client in the table. The **Edit External Client** window appears. Select (clear) the checkbox to enable (disable) the CHAP authentication, and then click **Save**.

  Note: The system does not allow you to change the client IQN/IP address.

d. In the **Management** step, perform the following actions:

- Turn on the **Enable 'Default-Storage' policy** switch to apply the default storage policy to the volume group that you are creating.

  The **Enable 'Default-Storage' policy** switch is turned off by default.

  For more information on the default storage policy, see Default Storage Policy on page 509.
- **Categories**: Search for the category to be assigned to the volume group. Select the checkboxes of the categories that you want to assign to the volume group.

  If you enabled the **Enable 'Default-Storage' policy** switch for the volume group in the previous step, then the **Storage:$Default** is displayed in the **Categories** dropdown menu. To assign more categories to the volume group, select the categories from the dropdown menu.

  Note:

  Do not assign any other category that is already associated with another storage policy to the entity, such as a VM or VG, if you want to enable the **Enable 'Default-Storage' policy** switch for that entity. If you enable the **Enable 'Default-Storage' policy** switch for an entity that is already associated with another category, the **Storage: $Default** category is enabled, but the storage policy associated with the other category overrides the default storage policy.

e. In the **Review** step, verify if all the field entries are correct.

f. Click **Create**.

The new volume group appears in the **Summary** page and **List** page of the **Volume Groups** window.

Modifying a Volume Group

This section describes how to modify volume groups from the Prism Central web console.

About this task

You can perform the following actions to modify the volume groups from the Prism Central web console.

- Update the volume group settings.
- Delete the volume group
- Manage volume group connections.
- Manage volume group virtual disks.
- Manage volume group categories

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2792

- Configure mutual CHAP authentication.
- Attach volume groups to guest VMs.
- Manage the following operations related to Nutanix Disaster Recovery setup.
  - Protect the volume group.
  - Create recovery points for the volume group.
  - Add volume group or volume group category to a recovery plan.

  For more information about the operations related to Nutanix Disaster Recovery setup, see Nutanix Disaster Recovery Guide.

Procedure

To modify a volume group, perform the following steps:

1. Log in to the Prism Central web console.
2. Select **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Storage** > **Volume Groups** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default with all the volume groups across registered clusters.
3. Select the target volume group checkbox, and click **Update**. The system displays the **Update Volume Group** window - **Configuration** step.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2793

4. Modify the volume group settings as required in **Configuration**, **Connections**, and **Management** steps. In the **Review** step, verify if all the field entries are correct and click **Save**. For field details, see Creating a Volume Group on page 315.

   To delete a volume group, you can select the target volume group and choose **Delete** from the **Actions** dropdown menu.

   > **Note:** If there are active connections, you must first remove the connections before deleting the volume group.

   You can perform the following actions to manage connections, virtual disks, and categories associated with the volume group:

   - To only update volume group connections, you can select the target volume group checkbox, and choose **Manage Connections** from the **Actions** dropdown menu. For field details, see Creating a Volume Group on page 315.

     The following is an example showing the **Manage Connections** window:

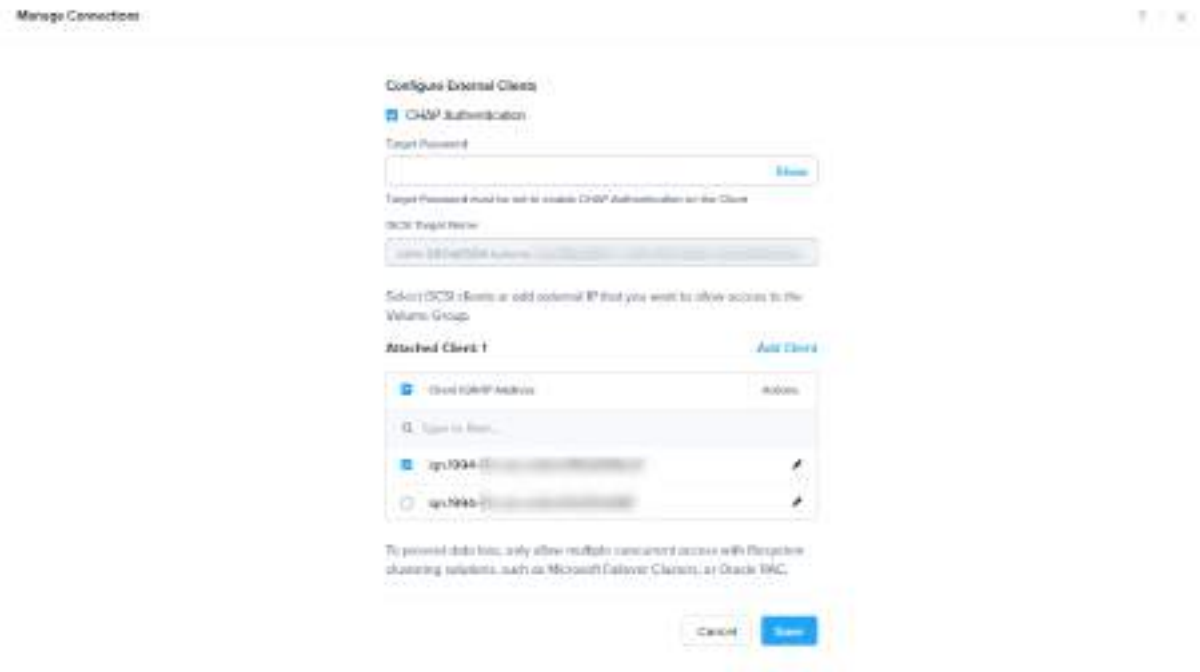


Figure 139: Manage Connections Window - Volume Group

   - To only add, update and remove volume group connections, navigate to **Connections** tab of the target volume group from Volume Group Details View on page 307 , and perform the following action:
     - Click **Add Connection** to add a volume group connection.
     - Select the target volume group connection, and click **Update** to update the volume group connection.
     - Select the target volume group connection, and click **Remove** to delete the volume group connection.

     For field details, see Creating a Volume Group on page 315.
   - To only update, add, and remove virtual disks attached to a volume group, navigate to **Virtual Disks** tab of the target volume group from Volume Group Details View on page 307, and perform the following actions:
     - Click **Add Virtual Disk** to add a virtual disk to the volume group.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2794

- Select the target volume group virtual disk, and click **Update** to update the volume group virtual disk.
- Select the target volume group virtual disk, and click **Delete** to delete the volume group virtual disk.

For field details, see Creating a Volume Group on page 315.

- To update volume group categories, you can select the target volume group checkbox, and choose **Manage Categories** from the **Actions** dropdown menu.

  In **Manage Categories** window, perform the following steps:

  1. Use the Add icon and Remove icon available under **Set Categories** field to add or remove the categories for the selected volume group
  2. Click **Save**.

  For information about how to create a volume group category, see Creating a Category on page 459.

Configuring Mutual CHAP Authentication

About this task

You must set the CHAP secret password in the Prism Central web console and then set the same password in the guest VMs hosting your initiators. It is important to use the same password as the target CHAP password; otherwise, the target CHAP password changes, and VM clients connecting to the target experience a loss of connectivity (in both clustered and non-clustered applications).

To set up mutual CHAP authentication in the Prism Central web console, do the following.

Procedure

1. Log in to the Prism Central web console.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Storage** > **Volume Groups** from the **Navigation Bar**.
3. Select a volume group to configure CHAP authentication and click **Update**.
4. In the **Connections** tab, select **CHAP Authentication**, enter the **Target Password** and then click **Save**.
5. Go to the **List** tab under **Storage** > **Volume Groups** and from the **View by** drop-down menu, select **General**.
6. Click the volume group and do the following under the **Connections** tab.
   a. Select the iSCSI client and click **Update** on the top.
   b. In the **Edit Connections** window, select **CHAP authentication** and enter the **Client Password**.

   > **Note:** The client password must be different from the target password, and length should be between 12 and 16 characters.

What to do next

Log in to the guest VM and configure CHAP on it. To set up mutual CHAP authentication in the Windows guest VMs, see Configuring CHAP Authentication in the *Volumes Guide*.

When you update the target password on the volume group, ensure that you update the associated recovery plan also with the new target password. If you do not update the new target password in the recovery plan, the new target password on the volume group is not retained after the failover.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2795

Attaching Volume Groups to Guest VMs

Procedure

1. Log in to the Prism Central web console.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Storage** > **Volume Groups** from the **Navigation Bar**.
3. Select the volume group and click **Manage Connections** from the **Actions** drop-down menu.
4. To connect different clients for clustered applications to synchronously replicated volume groups, click **Connect different clients**.

   Note: Clustered applications generally span over Nutanix clusters. Therefore, for volume groups protected with synchronous replication, you should have more external clients on the primary or the replicated volume groups.

5. Select the IQN or the IP Address of the volume groups you want to attach.
6. Click **Save**.

   Note: Alternatively, you can select the volume group, click **Update** from the **Actions** drop-down menu, and then click **Connect different clients** to attach the clients to the replicated volume groups.

   You can use the **Primary** and **Replicated** tabs in the **Update Volume Groups** page to connect an external client either with the primary instance or the replicated instance of the Volume Group. Thus, you can switch between **Primary** and **Replicated** tabs for client connections.

   Attaching a Guest VM to a volume group protected with a synchronous replication schedule.

   Select external clients and attach them using the add client option.

   In the **Add External Client** window, add the Client IQ or IP address and, if necessary, the CHAP authentication client password.

   The volume groups are connected to the guest VM. To view the connected volume groups, go to the **List** tab under **Storage** > **Volume Groups** and then select General from the **View by** drop-down menu on the right.

   For both the primary and dormant volume group attachment, log on to the guest VM, discover the iSCSI targets, and establish connections. To complete the iSCSI connections, refer to Windows Clients or Linux Clients.

Cluster RBAC for Volume Group

Cluster role-based access control (RBAC) for Volume Group feature enables a super-admin user to provide Prism Admin and Prism Viewer roles access to one or more clusters registered with Prism Central. A user with a Prism Admin role can view and update the entities like volume groups, virtual disks, and storage containers from the allowed clusters. However, a user with a Prism Viewer role can only view the entities.

Cluster RBAC is currently supported on an on-prem Prism Central instance hosted in a Prism Element cluster running AHV. After you enable the Micro Services Infrastructure feature on Prism Central, the Cluster RBAC feature is then automatically enabled.

Cluster RBAC for Volume Group feature is supported on AHV and ESXi clusters.

Note: Prism Central supports Cluster RBAC for VG feature from PC.2022.6 release.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2796

Table 63: List of Permissions for Prism Admin and Prism Viewer Roles

Role	Privileges
Prism Admin	Full administrator privileges except for creating or modifying the user accounts
Prism Viewer	View-only privileges

For information about how to configure cluster RBAC for volume group, see Configuring Cluster RBAC for Volume Group information in *Security Guide*.

External vCenter Server Integration

The VM management through Prism Central for ESXi provides a unified management interface for all of the external vCenter server instances. All the external vCenter server instances that are registered or not registered with any of the clusters are auto-discovered and displayed. If you have not registered the external vCenter server in Prism Element, you can register the clusters to the external vCenter server instances directly from Prism Central.

During the registration process, you have an option to select the ESXi clusters that you want to manage using Prism Central. For more information about registering external vCenter server, see Registering External vCenter Server (Prism Central) on page 336. After you successfully register external vCenter server instances, you can perform the following operations directly from Prism Central.

- Create, clone, update, and delete VMs.
- Create and delete NICs.
- Attach and delete disks.
- Power operations: Power on or off, reset, suspend, resume.
- Open and launch VM console.
- Enable and disable NGT.

> **Note:** Managing VMware guest tools is not supported through Prism Central.

> **Note:**
>
> - You can perform the power operations and launching of VM console even when external vCenter server is not registered.
> - If you are creating VM through Prism, configuration changes to the VM when it is powered on is enabled by default and it depends on the guest operating system that is deployed on the VM.

Rules and Guidelines

- Ensure that all the hosts in the cluster are managed by a single external vCenter server.
- Ensure that DRS is enabled on all the external vCenter server instances.
- Ensure that you are running ESXi and external vCenter server 5.5 or later releases.
- Ensure that you have homogeneous network configuration for all the external vCenter server instances. For example, network should have either 1G or 10G NICs.
- Ensure that you unregister the external vCenter server from the cluster before changing the IP address of the external vCenter server. After you change the IP address of the vCenter Sever, you must register the external vCenter server again with the new IP address.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2797

- The **vCenter Registration** page displays the registered vCenter Server. If for some reason the **Host Connection** field changes to *Not Connected*, it implies that the hosts are being managed by a different external vCenter server. In this case, there will be new vCenter entry with host connection status as Connected and you need to register to this external vCenter server. For more information about registering external vCenter server again, see Managing External vCenter Server Registration Changes (Prism Central) on page 340.

  Caution: If multiple external vCenter servers are managing the hosts of a single Nutanix cluster, you will not be able to perform the VM management operations. Move all the hosts into one external vCenter server.

Requirements and Limitations

- The E1000, E1000e, PCnet32, VMXNET, VMXNET 2, VMXNET 3 network adapter types (NICs) are supported.
- Only SCSI and IDE disks are supported. SATA and PCI disks are not supported.
- Creating a VM by using a template is not supported.
- Creating a VM by using image service is not supported.
- If a VM is deleted, all the disks that are attached to the VM get deleted.
- Network configuration (creation of port groups or VLANs) is not supported.

External vCenter Datastores Summary View

The **Summary** tab on the **External vCenter Datastores** page provides a dashboard of external vCenter datastores across registered vCenter instances.

To access the summary view of all external vCenter datastores, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Storage** > **External vCenter Datastores** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The system displays the **Lists** tab by default.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2798

3. Click the **Summary** tab.

   The system displays the **Summary** view of all the external vCenter datastores in the registered external vCenter server:

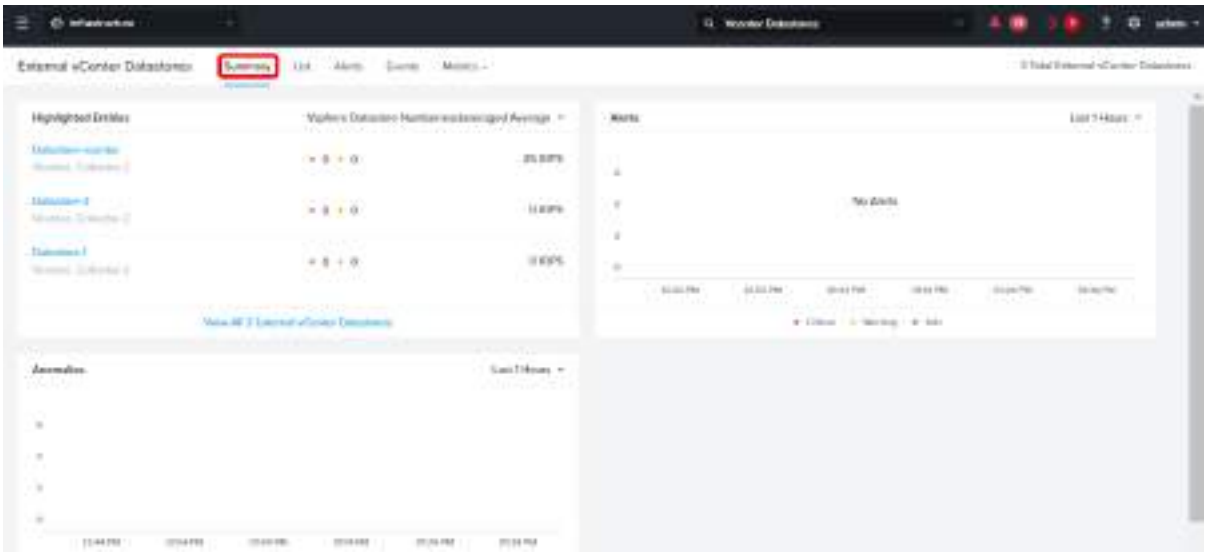


Figure 140: Summary View - All External vCenter Datastores

The **External vCenter Datastores** page includes five tabs on the left (**Summary**, **List**, **Alerts**, **Events**, and **Metrics**) with a display area below the selected tab.

> **Note:** This section describes the information and options that appear in the **Summary** page for all external vCenter datastores. For instructions about how to view and organize that information in various ways, see Prism Central GUI Organization on page 54.

The **Summary** tab for all external vCenter datastores displays the following three widgets:

- **Highlighted Entities**: Displays a list of the external vCenter datastores with the highest usage of the <*parameter*> you select from the dropdown menu on the right of the widget. The <*parameter*> involves only **vSphere Datastore Numberreadaveraged Average**. Click **View All XX External vCenter Datastores** link at the bottom to display the **List** tab.
- **Alerts**: Displays a list of external vCenter datastore-related alerts that are generated during the specified <*interval*> you select from the dropdown menu on the right of the widget. The <*interval*> involves **Last week**(default), **Last 24 hours**, and **Last 1 hour**. When an alert appears, you can click the graph to view a list of those alerts. Click any alert to display the details page for that alert.
- **Anomalies**: Displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified <*interval*> you select from the dropdown menu on the right of the widget. The <*interval*> involves **Last week**(default), **Last 24 hours**, and **Last 1 hour**. When an anomaly appears, you can click the graph to view a list of those anomalies. Click any anomaly to display the event page for that anomaly.

List Tab

The **List** tab displays the list of external vCenter datastores across all clusters.

To access the **List** tab of all external vCenter datastore:

1. Log in to Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2799

2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Storage** > **External vCenter Datastores** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The system displays the **List** tab by default with external vCenter datastore across all the registered clusters.

   Note: You can use the **View by** and **Group by** options to create your own customized view and add the necessary columns to that view. For more information on how to **View by** and **Group by** options, see Prism Central GUI Organization on page 54.

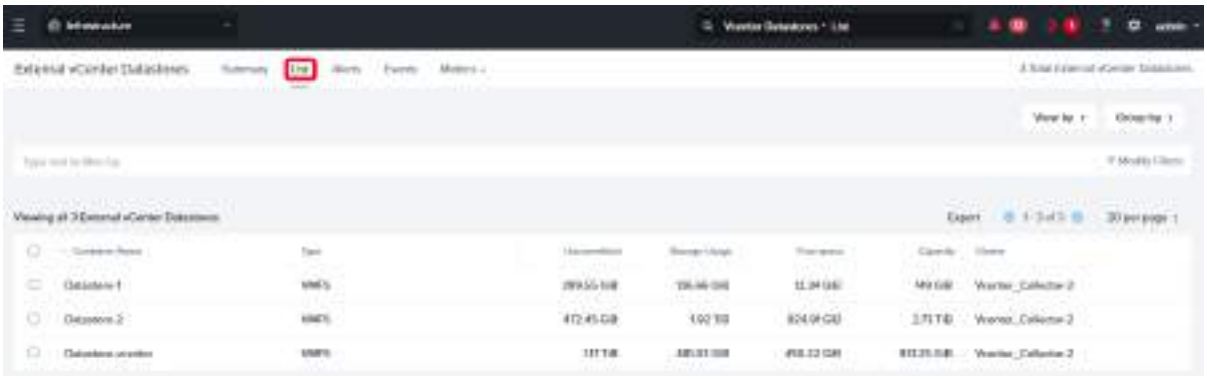


Figure 141: External vCenter Datastores - List Tab

The following table describes the fields that appear in the external vCenter datastore **List** tab.

Note: The fields vary based on the **View by** and **Group by** options. A dash (-) is displayed in a field when a value is not available or applicable. For more information about **View by** and **Group by** options, see Prism Central GUI Organization on page 54.

Table 64: External vCenter Datastores List Tab - Field Description

Field	Description	Values
Container Name	Displays the name of the datastore container. You can click the container name to view the detailed information for that container. For more information about datastore container details view, see External vCenter Datastore Details View on page 332.	(container name)
Type	Displays the file system type.	VMFS, NFS
Uncommitted	Displays the amount of uncommitted disk space.	xx [GiB|TiB]
Storage Usage	Displays the amount of used storage space.	xx [GiB|TiB]
Free Space	Displays the amount of free storage space.	xx [GiB|TiB]
Capacity	Displays the total amount of storage capacity.	xx [GiB|TiB]
Cluster	Displays the name of the cluster in which the datastore resides.	(cluster name)

You can perform the following actions for the external vCenter datastores in the **Lists** tab:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2800

- Access the detailed information about an individual external vCenter Datastore. For details, see External vCenter Datastore Details View on page 332.
- Filter the external vCenter datastores list based on available parameter values using **Filters** pane. For more information about **Filters** pane, see Filters Pane - External vCenter Datastores Page on page 330.
- Export the table that contains the list of external vCenter datastores and their information to a file in a CSV format. For more information about **Export** option, see Export on page 59.
- Group the external vCenter datastores based on pre-defined criteria. For information about how to group the external vCenter datastores, see Group by on page 56.
- View external vCenter datastores based on pre-defined criteria or create a custom view. For information about available views and how to create a custom view, see View by on page 56.

Filters Pane - External vCenter Datastores Page

The following table describes the fields available in the **Filters** pane:

Table 65: Filter Pane Fields

Parameter	Description	Values
Container Name	Filters based on the container name. Select a condition from the dropdown menu and enter a string in the field. The system returns a list of containers that satisfy the container name condition/ string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	(name string)
Cluster	Filters on the cluster name. Enter a string in the field to display a list of clusters that satisfy the name string.	(cluster name)
Storage Usage	Filters on the amount of used storage space. Check the box(es) for the desired range or enter a range in the "**from <low> to <high> TiB**" field. The number of containers in each range is displayed on the right of the line.	([xx] to [yy] range)
Capacity	Filters based on the amount of total storage capacity.	([xx] to [yy] range)
Free Space	Filters based on the amount of free storage space.	([xx] to [yy] range)
Uncommitted	Filters based on the amount of uncommitted storage space.	([xx] to [yy] range)
Type	Filters based on file system type.	VMFS, NFS

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options that are available on the **Activity** > **Alerts** page, however it only displays the vCenter Datastore-related alerts across the registered clusters. For more information about alerts, see *Prism Central Alerts and Events Reference Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2801

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options that are available on the **Activity** > **Events** page, however it only displays the vCenter Datastore-related events across the registered clusters. For more information about events, see *Prism Central Alerts and Events Reference Guide*.

Metrics Tab

The **Metrics** tab allows you to view performance metrics across the external vCenter datastores. Click the **Metrics** tab to display dropdown menu of available metrics, and select the metric name to display the relevant performance information.

> **Note:** The **Metrics** dropdown menu is hypervisor-specific, and might vary based on the hypervisors used in the cluster.

The following is an example showing the dropdown menu of the **Metrics** tab:

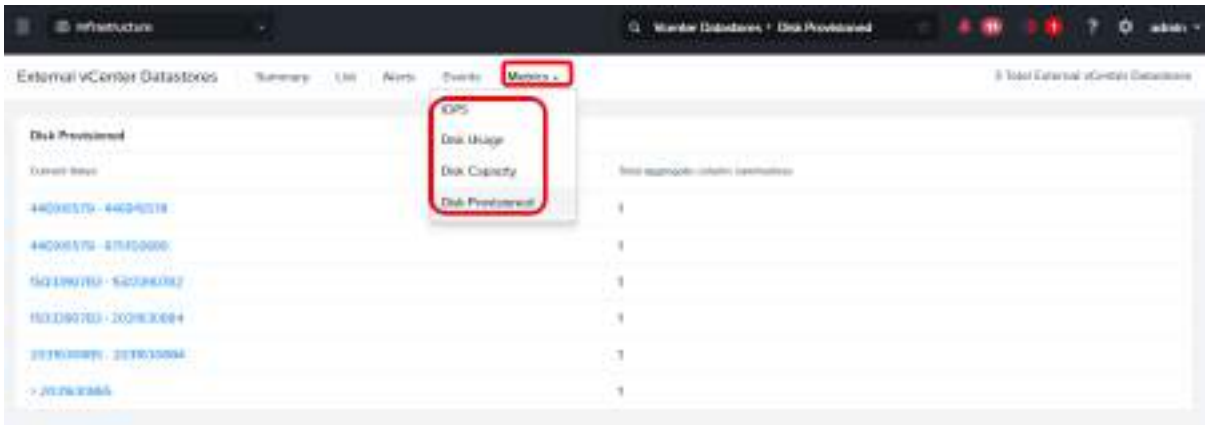


Figure 142: External vCenter Datastores Metrics Tab

The following table describes the dropdown menu of the **Metrics** tab:

Table 66: Metrics Tab Dropdown Menu

Metric	Description
IOPS	Displays the number of read and write IOPS for the listed number of containers. You can click the IOPS value to view the **Summary** tab with a filtered list of containers for the selected IOPS value. The **Total aggregate column summaries** field displays the number of containers for which the IOPS value is applicable.
Disk Usage	Displays the disk usage amount for the listed number of containers. You can click the disk usage amount to view the **Summary** tab with a filtered list of containers for the selected disk usage amount. The **Total aggregate column summaries** field displays the number of containers for which the disk usage value is applicable.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2802

Metric	Description
Disk Capacity	Displays the disk capacity for the listed number of containers. You can click the disk capacity to view the **Summary** tab with a filtered list of containers for the selected disk capacity. The **Total aggregate column summaries** field displays the number of containers for which the disk capacity value is applicable.
Disk Provisioned	Displays the provisioned disk space for the listed number of containers. You can click the provisioned value to view the **Summary** tab with a filtered list of containers for the selected provisioned value. The **Total aggregate column summaries** field displays the number of containers for which the disk provisioned value is applicable.

External vCenter Datastore Details View

Summary Tab

The **Summary** tab of an individual external vCenter datastore consists of a dashboard that provides the detailed information about the external vCenter datastore.

To access the **Summary** tab of an individual external vCenter datastore:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Storage** > **Storage Container** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   By default, the system displays the **List** tab with external vCenter datastores across all the registered clusters.
3. Click the target <*vCenter_Datastore_Name*> to view the **Summary** tab of an individual external vCenter datastore.

> **Note:** Replace <*vCenter_Datastore_Name*> with the actual external vCenter datastore name at your site.

The following is an example showing the **Summary** tab of an individual external vCenter datastore:

Figure 143: Summary Tab - Individual External vCenter Datastore

The **Summary** tab of an individual external vCenter datastore provides the following widgets:

- **Properties** - Displays summary information about the external vCenter datastore. For information about the fields available in **Properties** widget, see External vCenter Datastore Widgets - Parameter Details on page 333.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2803

- **Alerts**- Displays a list of related alerts that occurred during the specified interval. Select either **Last week** (default), **Last 1 hour** or **Last 24 hours** from the dropdown menu on the top right corner of the widget.
- **Anomalies** - Displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified interval. Select either **Last week** (default), **Last 1 hour** or **Last 24 hours** from the dropdown menu on the top right corner of the widget. When an anomaly appears, you can click the graph to display a list of those anomalies. If you click an individual anomaly, the system displays the event page for that anomaly.
- **Metrics** - Displays the average metrics information for **Last 15 minutes avg** for the external vCenter datastore (container) that includes **IOPS Read**, **IOPS Writes**, **Disk Usage**, **Disk Capacity**, and **Disk Provisioned** fields. For information about the fields available in **Metrics** widget, see External vCenter Datastore Widgets - Parameter Details on page 333.

External vCenter Datastore Widgets - Parameter Details

The following table describes the fields in the **Properties** and **Metrics** widgets. A dash (-) in a field indicates that there is not enough data to evaluate or a value is not assigned. The displayed fields vary by hypervisor.

Table 67: External vCenter Datastore Widgets - Field Description

Field	Description	Values
Properties widget		
Capacity	Displays the total amount of storage capacity.	xx [GiB|TiB]
Storage Usage	Displays the amount of used storage space.	xx [GiB|TiB]
Free Space	Displays the amount of free storage space.	xx [GiB|TiB]
Uncommitted	Displays the amount of uncommitted disk space.	xx [GiB|TiB]
Cluster	Displays the name of the cluster in which the datastore resides. Click on the cluster name to displays details about that cluster.	(cluster name)
Type	Displays the file system type.	VMFS, NFS
Metrics widget		
IOPS Reads	Displays the average number of read IOPS for the selected container in last 15 minutes.	Integer (IOPS)
IOPS Writes	Displays the average number of write IOPS for the selected container in last 15 minutes.	Integer (IOPS)
Disk Usage	Displays the average disk usage amount for the selected container in last 15 minutes.	Integer (MiB)
Disk Capacity	Displays the total disk capacity for the selected container.	Integer (GiB)
Disk Provisioned	Displays the average provisioned disk space for the selected container in last 15 minutes.	Integer (MiB)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2804

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options as the Alerts dashboard, however it is filtered to display the alerts only for the selected external vCenter datastore (individual external vCenter datastore). For more information about alerts, see *Prism Central Alerts and Events Reference Guide*.

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options as the Events dashboard, except it is filtered to display just events for this external vCenter datastore. For more information about events, see Prism Central Alerts and Events Reference Guide.

Metrics Tab

The **Metrics** tab allows you to view usage metrics for the external vCenter datastore. Click the **Metrics** tab to view graphs for all the metrics. The graph is a rolling time interval performance or usage monitor. The baseline range appears as a blue band in the graph.

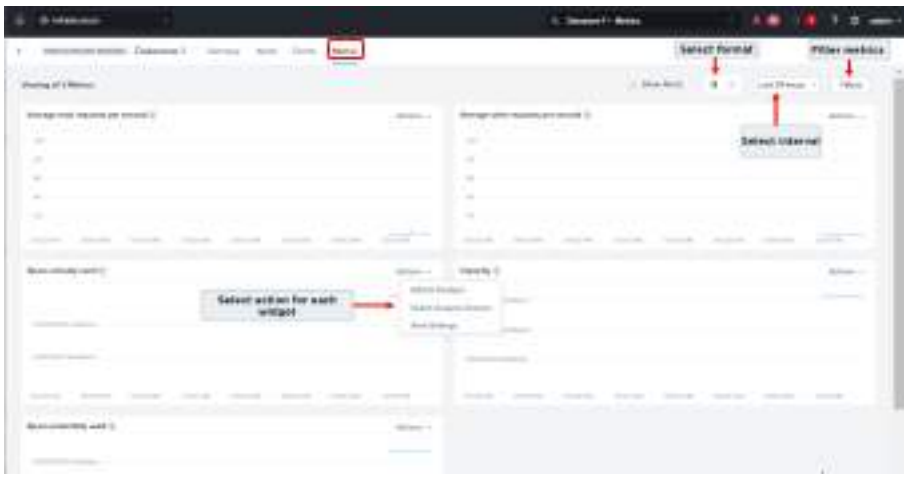


Figure 144: Metrics Tab

> **Note:** The baseline range and identified anomalies are based on sophisticated machine-learning capabilities. For more information, see Behavioral Learning Tools) in *Intelligent Operations Guide*. The machine-learning algorithm uses 21 days of data to monitor and predict performance. A graph or baseline band may not appear if less than 21 days of data is available.

You can perform the following actions in the **Metrics** tab:

- Place the cursor anywhere on the horizontal axis to display the value at that time.
- Select the duration (time interval) from the dropdown menu on the right (last 1 hour, last 24 hours, last week, last 21 days).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2805

- From the **Actions** dropdown menu that appears on the top-right corner of each metrics widget, you can perform the following operations:
  - Select **Add to Analysis** to add the selected metric to **Analysis** dashboard. For more information, see Analysis Dashboard in *Intelligent Operation Guide*.
  - Choose **Select Analysis Session** to add the metric to an existing or new analysis session. The system displays the **Select A Session** window.

Figure 145: Session Window

    Select the target session from the **Session** dropdown menu, and then click **Add to Session**.
  - Select **Alert Settings** to create a custom alert policy for the metric. For more information about how to create a custom alert policy, see Prism Central Alerts and Events Reference Guide.
- Click the **Filters** option to select one or more appropriate metric checkboxes to display the selected metrics in the **Metrics** page.

The following table describes the metrics available in **Metrics** tab:

> **Note:** Metrics are hypervisor-dependant, and might not be available on all hypervisors.

Table 68: Metrics Tab Fields

Metric	Description
Average read requests per second	Average number of read commands issued per second to the external vCenter datastore during the collection interval.
Average write requests per second	Average number of write commands issued per second to the external vCenter datastore during the collection interval.
Space actually used	Amount of space actually used by the virtual machine or the external vCenter datastore. It might be less than the amount provisioned at any given time, depending on whether the virtual machine is powered-off, whether snapshots have been created or not, and other such factors. Available from a datastore and virtual machine target entities.
Capacity	Configured size of the external vCenter datastore. Available from an external vCenter datastore entity only.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2806

Metric	Description
Space potentially used	Amount of storage set aside for use by an external vCenter datastore or a virtual machine. Files on the external vCenter datastore and the virtual machine can expand to this size, but not beyond it. Available from an external vCenter datastore and virtual machine target entities.

Registering External vCenter Server (Prism Central)

All the external vCenter server instances that are registered to Prism Element are listed in Prism Central. If you do not want to manage your cluster through Prism Central, you have an option to de-select the clusters from Prism Central.

Before you begin

Ensure that you have external vCenter server extension privileges as these privileges provide permissions to perform external vCenter server registration for the Nutanix cluster.

About this task

Important: Observe the following points about registering the external vCenter server with Prism Central:

- Nutanix does not store external vCenter server credentials.
- Whenever a new node is added to a cluster, vCenter Sever registration for the new node is automatically performed.

Procedure

To register an external vCenter server, perform the following steps:

1. Log in to Prism Central.
2. Select **Infrastructure** application from the Application Switcher Function on page 45.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2807

3. Navigate to **Prism Central Settings** > **Setup** > **vCenter Registration** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   You can also click the Settings icon, and navigate to **Setup** > **vCenter Registration**.

   The system displays the **vCenter Registration** page.

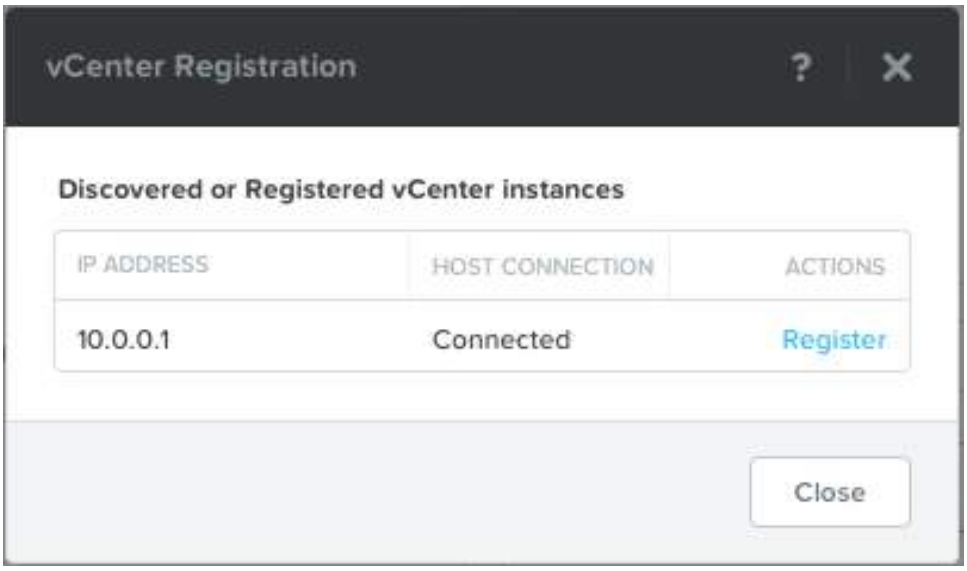


Figure 146: vCenter Registration

- The **vCenter Registration** window lists all the external vCenter server instances that are registered or not registered with the clusters.
- If you have not registered the external vCenter server in Prism Element, you can register the clusters to the external vCenter server instances directly from Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2808

4. Click **Register** to register the external vCenter server.

   - The external vCenter server that is managing the hosts in the cluster is auto-discovered and its IP address is auto-populated in the **IP Address** field.
   - The port number field is also auto-populated with 443. Do not change the port number. For the complete list of required ports, see Port Reference.

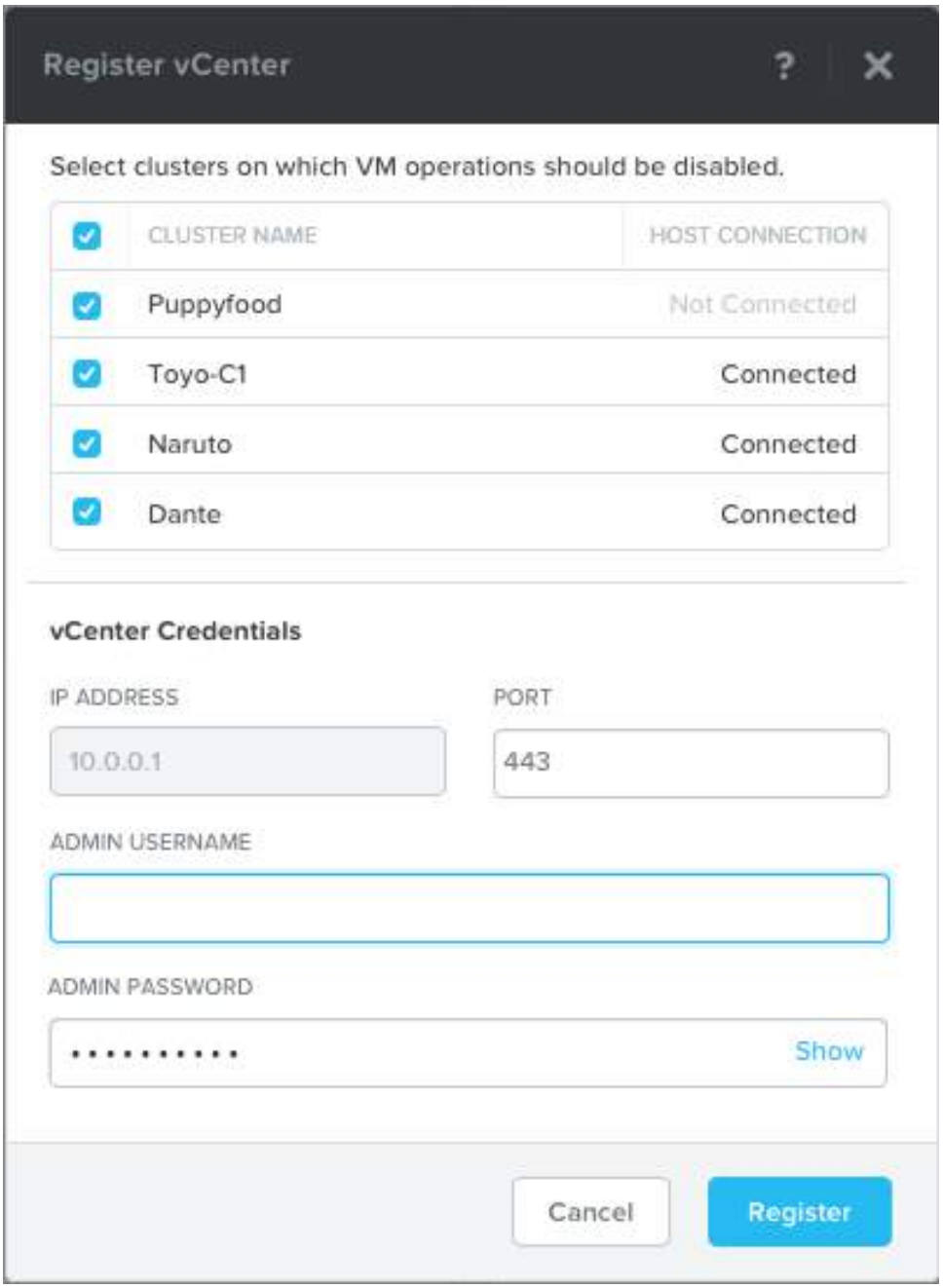


Figure 147: Cluster Selection

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2809

5. Specify the following information in the **Register vCenter** window:

   - Select the checkbox(es) of the clusters that you want to manage from Prism Central. You can also clear the checkbox(es) of the clusters that you do not want to manage from Prism Central.
   - Enter the administrator user name and password of the external vCenter server in the **Admin Username** and **Admin Password** fields.

6. Click **Register** to register the external vCenter server in Prism Central with selected clusters.

   During the registration process a certificate is generated to communicate with the external vCenter server. If the registration is successful, a relevant message is displayed in the **Tasks** page. For more information about how to access **Tasks** page, see Tasks View on page 452.

   The system displays the **Host Connection** field as *Connected*, which implies that all the hosts are managed by the registered external vCenter server.

Unregistering a Cluster from the External vCenter Server (Prism Central)

This section describes how to unregister your clusters from the external vCenter server.

About this task

- Ensure that you unregister the external vCenter server from the cluster before changing the IP address of the external vCenter server. After you change the IP address of the vCenter Sever, you should register the external vCenter server again with the new IP address with the cluster.
- The **vCenter Registration** page displays the registered external vCenter server. If the system displays the **Host Connection** field as *Not Connected* for any external vCenter server instance, it implies that the clusters (hosts) are managed from a different external vCenter server. In this case, the system also displays a new external vCenter server instance with **Host Connection** field as *Connected* and you need to register to this external vCenter server instance. For more information about how to reregister a external vCenter server, see Managing External vCenter Server Registration Changes (Prism Central) on page 340.

Procedure

To unregister the cluster from the external vCenter server, perform the following steps:

1. Log in to Prism Central.
2. Select **Infrastructure** application from the Application Switcher Function on page 45.
3. Navigate to **Prism Central Settings** > **Setup** > **vCenter Registration** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   You can also click the Settings icon, and navigate to **Setup** > **vCenter Registration**.

   The system displays the **vCenter Registration** page.
4. Click the Edit icon under **Actions** field, and clear the checkbox(es) of the clusters that you want to unregister from the external vCenter server.
5. Enter the administrator user name and password of the external vCenter server in the **Admin Username** and **Admin Password** fields, and Click **Unregister**.

   If the credentials are correct, the selected clusters are unregistered from the external vCenter server, and a relevant message is displayed in the **Tasks** dashboard. For information about how to access the Tasks dashboard, see Tasks View on page 452.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2810

Managing External vCenter Server Registration Changes (Prism Central)

This section describes how to unregister an existing external vCenter server instance and reregister a new external vCenter server instance.

About this task

> **Important:** After you change the IP address of the vCenter Sever or if the system displays the **Host Connection** field as *Not Connected* , it implies that current external vCenter server is not managing the clusters (hosts). In this case, you must reregister the new external vCenter server instance with Prism Central.

Procedure

To re-register the external vCenter server with Prism Central, perform the following steps:

1. Log in to Prism Central.
2. Select **Infrastructure** application from the Application Switcher Function on page 45.
3. Navigate to **Prism Central Settings** > **Setup** > **vCenter Registration** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   You can also click the Settings icon, and navigate to **Setup** > **vCenter Registration**.

   The system displays the **vCenter Registration** page.
4. Click **Unregister** under **Actions** field to unregister the external vCenter server from Prism Central.
5. Click **Register** to reregister the new external vCenter server instance.

   For more information about how to register a external vCenter server with Prism Central, see Registering External vCenter Server (Prism Central) on page 336.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2811

NETWORK AND SECURITY ENTITIES

You can access the following networking and security entity items from the **Network and Security** entity of the **Infrastructure** application. For information on how to access the entity items available in **Network and Security** entity, see Application-specific Navigation Bar on page 66.

- **Subnets**: This page displays the subnets and the operations you can perform on subnets. For more information, see Subnets on page 341.
- **Virtual Private Clouds**: This page displays the VPCs and the operations you can perform on VPCs. For more information, see Virtual Private Clouds Summary View on page 357.
- **Floating IPs**: This page displays a list of floating IP addresses that you are using in the network. It allows you to request for floating IP addresses from the free pool of I addresses available to the clusters managed by the Prism Central instance. For more information, see Floating IPs Summary View on page 376.
- **Connectivity**: This page allows you to manage the following networking capabilities. For more information, see Connectivity on page 378.
  - **Gateways**: This page provides a list of network Gateways you have created and configured, and the operations you can perform on the network Gateways. For more information, see Gateways Summary View on page 378.
  - **VPN Connections**: This page provides a list of VPN connections you have created and configured, and the operations you can perform on the VPN connections. For more information, see VPN Connections Summary View on page 381.
  - **Subnet Extensions**: This page provides a list of subnets that you have extended at the Layer 2 level using VPN (point-to-point over Nutanix VPN) or VTEP (point-to-multi-point including third party). For more information, see Subnet Extensions Summary View on page 386.
  - **BGP Sessions**: This page provides a list of BGP sessions you have created and configured, and the operations you can perform on the BGP sessions. For more information, see BGP Sessions Summary View on page 390.
- **Security Policies**: This page provides a list of security policies you configured using Flow Segmentation. For more information, see Security Policies on page 394.
- **Security Dashboard**: This page provides dynamic summary of the security posture across all registered clusters. For more information, see Security Dashboard on page 394.

For information on how to configure network connections, see Network Configuration..

Subnets (Overlay IP subnets), Virtual private clouds, floating IPs, and Connectivity are Flow virtual networking features. These features support flexible app-driven networking that focuses on VMs and applications instead of virtual LANs and network addresses. Flow virtual networking powers network virtualization to offer a seamless network experience with enhanced security. It is disabled by default. It is a software-defined network virtualization solution providing overlay capabilities for the on-premises AHV clusters.

Security policies drives the Flow Segmentation features for secure communications. For more information, see Flow Microsegmentation Guide.

Subnets

You can perform the following actions to manage a subnet from Prism Central.

- Creating a Subnet
- Updating a Subnet

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2812

- Deleting a subnet
- Creating a subnet extension
- Assigning a Category Value to a Subnet
- Migrating VMs between VLAN and VPC networks

Subnets Summary View

The **Subnets** page displays the list of subnets across all the registered clusters.

To access the **Subnets** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Network & Security** > **Subnets** from the **Navigation Bar**.

   The **Subnets** page opens displaying the **List** tab. This tab provides information about all the subnets configured for the registered clusters.

   > **Note:** For information on the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

The following table describes the fields that appear in the **Subnets** page.

> **Note:** The fields vary based on the **View by** and **Group by** options. A dash (-) is displayed in a field when a value is not available or applicable. For more information, see the View by on page 56 and Group by information.

Table 69: Subnets – Field Description

Field	Description	Values
Name	Displays the subnet name.	(subnet name)
External Connectivity	Displays whether or not the subnet has external connectivity configured.	(Yes/No)
Type	Displays the subnet type.	VLAN or VLAN`Basic` or Overlay
VLAN ID	Displays the VLAN identification number.	(ID number)
VPC	Displays the name of the VPC in which the subnet is used.	(Name of VPC)
Virtual Switch	Displays the virtual switch that is configured for the VLAN you selected. The default value is the default virtual switch `vs0`. **Note:** The virtual switch name is displayed only if you add a VLAN ID in the VLAN ID field.	(virtual switch name)
IP Prefix	Displays the IPv4 address of the network with the prefix.	(IPv4 Address/Prefix)
Cluster	Displays the name of the cluster for which this subnet is configured.	(cluster name)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2813

Field	Description	Values
Hypervisor	Displays the hypervisor that the subnet is hosted on.	(Hypervisor)

You can perform the following actions from the **Subnets** page:

- Click the name of a subnet to open the subnet details page, which displays the detailed information about the subnet. For more information, see Subnet Details View on page 344.
- Create a subnet by clicking **Create Subnet**. For more information, see Creating a Subnet in the *Flow Virtual Networking Guide*.
- Migrate VMs between VLAN network and VPC network by clicking **Migrate**. For more information, see Migrating VMs between VLAN Backed and VPC Subnets in the *Flow Virtual Networking Guide*.
- Configure network connections for a cluster by clicking **Network Config**. For more information, see Network Configuration.
- Group the subnets based on pre-defined criteria. For more information, see Group by on page 56.
- View subnets based on a pre-defined criteria or create a custom view. For more information, see View by on page 56.
- Filter the subnets list based on a variety of parameter values using the **Filters** pane. For more information, see Filters Pane - Subnets page.
- Perform the following subnet-specific actions on a single or multiple subnets using the **Actions** dropdown menu. The **Actions** dropdown appears when one or more subnets are selected.

Table 70: Subnet Actions

Action	Description
Update	Click this action to update the subnet. For more information, see Updating a Subnet in the *Flow Virtual Networking Guide*.
Extend	Click this action to create a subnet extension. For more information, see Layer 2 Virtual Subnet Extension Over VTEP in the *Flow Virtual Networking Guide*.
Manage Categories	Click this action to associate the subnet with a category or change the categories that the subnet is associated with. For more information, see Assigning a Category on page 460.
Delete	Click this action to delete the subnet. For more information, see Deleting Subnets, Policies, or Routes in the *Flow Virtual Networking Guide*.

Filters Pane - Subnets page

You can filter the information in the **Subnets** page based on the following fields that are available in the **Filters** pane. For information on how to use the Filters pane, see the Filters Pane information.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2814

Table 71: Filter Pane Field Description - Subnets page

Field	Description	Values
Name	Filters based on the subnet name. It returns a list of subnets that satisfy the name condition/string.	(Subnet name string)
External Connectivity	Filters based on whether the subnet has external connectivity configured or not.	(Yes/No)
Type	Filters based on the subnet type.	(VLAN/VLAN (External)/ Overlay
VLAN ID	Filters based on VLAN identification number.	(ID number)
VPC	Filters based on the name of the VPC in which the subnet is used.	(Name of VPC)
Cluster	Filters based on the name of the cluster for which this subnet is configured.	(cluster name)
Hypervisor	Filters based on the hypervisor that the subnet is hosted on.	ESXi/AHV/Hyper-V/XenServer/Mixed Hypervisor/Null Hypervisor

Subnet Details View

The Subnet details page consists of a dashboard that provides the detailed information about the subnet.

The details page has the **Summary**, and **Throughput** tabs.

To access the details page of an individual subnet:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Network & Security** > **Subnets** from the **Navigation Bar**.

   Prism Central displays the **Subnets** page that contains information about all the subnets configured for the registered clusters.
3. Click a subnet to open the details page of the subnet.

   The **Summary** tab opens displaying the detailed information about the subnet in widgets.

> **Note:** For information on the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

Summary Tab

The **Summary** tab provides detailed information about the subnet in widgets. A dash (-) is displayed in a field when a value is not available or applicable.

The **Summary** tab has the following widgets:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2815

Widget Name	Information provided
Properties	Provides the following: • Type — Displays the type of network like VLAN or Overlay. • VLAN ID — Displays the VLAN ID. This parameter is displayed only for VLAN networks. • VPC — Displays the VPC name. This parameter is displayed only for Overlay networks. • Cluster — Displays the cluster that the VLAN network is configured on. This parameter is displayed only for VLAN networks. • IP Address Prefix — Displays the IP address prefix configured for the network. This parameter is displayed for both VLAN and Overlay networks.
IP Address Pools	Provides the following: • The IP address Pool Range assigned to the network. • The total number of used and available IPs in the cluster. • Used IPs in Subnet — Displays the number of used IPs in the subnet. • Used IPs in Pools — Displays the number of used IPs in the pool. • Free IPs in Pools — Displays the number of free IPs in the pool. • Free IPs in Subnet — Displays the number of free IPs in the subnet.
Domain Settings	Provides the following DHCP settings configured for a VM in a subnet: • Domain Name Servers — Displays the total number of DNS IP addresses. • Domain Search — Displays the VLAN domain name. • Domain Name — Displays the domain name. • TFTP Server Name — Displays the name of the TFTP server where you host the host boot file. • Boot File Name — Displays the name of the boot file that the VMs need to download from the TFTP host server.

The **Summary** tab provides the following options, at the top of the page. For more information, see the *Subnet Actions* table in Subnets Summary View on page 342.

- **Update**
- **Extend**
- **Manage Categories**
- **Delete**

Throughput Tab

The **Throughput** tab provides a graphical representation of the throughput of the subnet.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2816

Network Configuration

Each VM network interface is bound to a virtual network, and each virtual network is bound to a single VLAN. The **Network Configuration** window displays information about the configured virtual networks.

To access the **Network Configuration** window:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Network & Security** > **Subnets** from the **Navigation Bar**.

   This displays the **Subnets** page.
3. Click **Network Config**.

   This displays the **Network Configuration** window.

The **Network Configuration** window includes three tabs.

- The **Subnets** tab displays a list of the configured VLAN subnets.
- The **Internal Interfaces** tab displays a list of LAN interfaces.
- The **Virtual Switch** tab displays a list of virtual switches configured, including the default system-generated virtual switch vs0.

The following table describes the fields in each tab.

Table 72: Network Configuration – Field Description

Parameter	Description	Values
Subnets Tab		
Subnet Name	Displays the name of the subnet.	(name)
Virtual Switch	Displays the name of the virtual switch in the form vs#, for example vs0 for virtual switch 0 which is the default virtual switch.	(vs<number>)
VLAN ID	Displays the VLAN identification number for the network in the form vlan.#, for example vlan.27 for virtual LAN number 27.	(ID number)
Used IP Addresses	Displays the number of IP addresses in the subnet that are used, for example IP address of a VM or any other entity. This parameter is applicable only when you have configured a managed network or subnet.	(number of IP addresses)
Free IPs in Subnets	Displays the number of free or unused IP addresses in the subnet. This parameter is applicable only when you have configured a managed network or subnet.	(number of IP addresses)
Free IPs in Pool	Displays the number of free or unused IP addresses in the configured pool. This parameter is applicable only when you have configured a managed network or subnet.	(number of IP addresses)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2817

Parameter	Description	Values
Actions	Action link for editing or deleting a network configuration.	(Edit/Delete)
Internal Interfaces Tab		
Descriptive Name	Displays a name for the LAN.	(LAN name)
Subnet (Gateway IP / Prefix Length)	Displays the subnet that the internal interface belongs to in the form `<IP Address>`/<number (prefix)>	(IP Address/prefix number)
Features	Displays the features available on the internal interfaces.	
Interface	Displays the interface designation such as eth0 or eth1.	(interface name)
Virtual Switch		
Name	Displays the name of the switch in the form vs#	(vs<number>)
Bridge	Displays the name of the bridge associated with the virtual switch in the form br#, for example br0 for the default bridge.	(br<number>)
MTU (bytes)	Displays the MTU set for the virtual switch in bytes. The default MTU is 1500.	(number)
Bond Type	Displays the uplink bond type associated with the virtual switch. For more information, see the *Bond Types* table in Creating a Virtual Switch on page 349.	(<bond_type>)

LAG and LACP on the ToR Switch

For more information, see Enabling LACP and LAG (AHV Only) on page 354.

Creating VLAN Connections

Prism Central allows you to create a VLAN connection for a selected cluster.

About this task

To create one or more VLAN connections (subnets), perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Network & Security** > **Subnets** from the **Navigation Bar**.
   This displays the **Subnets** page.
3. Click **Network Config**.
   This displays the **Network Configuration** window.
4. In the **Subnets** tab of the **Network Configuration** window, click **Create Subnet**.

   This displays the **Create Subnet** window.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2818

5. Perform the following in the indicated fields:

   a. **Subnet Name**: Enter a name for the subnet.

   b. **Virtual Switch**: Select the virtual switch for the subnet from the dropdown menu.

      You can associate the default virtual switch vs0 or create a virtual switch. For information on how to create a virtual switch, see Creating a Virtual Switch on page 349.

      For more information about virtual switch, see Layer 2 Network Management in the *AHV Administration Guide*.

   c. **VLAN ID**: Enter a number in the range of 0-4094. Enter 0 for the native VLAN.

      This field is the VLAN identifier complying with the IEEE 802.1Q.

      The value appears as, for example, vlan.1 or vlan.27 in displays.

   d. **Enable IP Address Management**: Select the checkbox to have the cluster control IP addressing in the subnet.

      Selecting this checkbox displays additional fields. If the checkbox is not selected, no network management is attempted and it is assumed that the management for this virtual LAN is handled outside the cluster.

   e. **Network IP Prefix**: Enter the IP address of the gateway for the network and prefix with the network prefix (CIDR notation, for example, 10.1.1.0/24).

   f. **Gateway IP Address**: Enter the VLAN default gateway IP address.

   g. **DHCP Settings**: Select this checkbox to display the fields for defining a domain.

      Selecting this checkbox displays fields to specify DNS servers and domains. Clearing this checkbox hides those fields.

   h. **Domain Name Servers (Comma Separated)**: Enter a comma-delimited list of DNS servers.

   i. **Domain Search (Comma Separated)**: Enter a comma-delimited list of domains.

   j. **Domain Name**: Enter the VLAN domain name.

   k. **TFTP Server Name**: Enter the host name or IP address of the TFTP server from which virtual machines can download a boot file. Required in a Pre-boot eXecution Environment (PXE).

   l. **Boot File Name**: Name of the boot file to download from the TFTP server.

6. To define a range of addresses for automatic assignment to virtual NICs, click **+ Create Pool** (under **IP Address Pools**) and enter the following in the **Add IP Pool** window that is displayed:

   > **Note:** If no pool is provided, the user must assign IP addresses to VMs manually.

   a. Enter the starting IP address of the range in the **Start Address** field.

   b. Enter the ending IP address of the range in the **End Address** field.

   c. Click **Submit** to close the window and return to the **Create Subnet** window.

7. To configure a DHCP server, select the **Override DHCP server** checkbox and enter an IP address in the **DHCP Server IP Address** field.

   This address (reserved IP address for the Acropolis DHCP server) is visible only to VMs on this network and responds only to DHCP requests. If this checkbox is not selected, the **DHCP Server IP Address** field is not displayed and the DHCP server IP address is generated automatically. The automatically generated address is `network_IP_address_subnet.254`, or if the default gateway is using that address, `network_IP_address_subnet.253`.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2819

8. Click **Save** to configure the network connection, close the **Create Subnet** window, and return to the **Network Configuration** window.

Modifying VLAN Connections

Prism Central allows you to modify an existing VLAN connection for a selected cluster.

About this task

Perform the following steps to modify an existing VLAN connection (defined on an Acropolis managed cluster):

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Network & Security** > **Subnets** from the **Navigation Bar**.
   This displays the **Subnets** page.
3. To modify a VLAN connection, select the checkbox associated with the VLAN connection and click **Update** from the **Actions** dropdown menu.
   This displays the **Update Subnet** window which contains the same fields as the **Create Subnet** page (see Creating VLAN Connections on page 347).
4. Modify the field values and click **Update** to save the changes, and return to the **Subnets** page.

Perform the following steps to delete an existing VLAN connection.

5. To delete a VLAN connection, select the checkbox associated with the VLAN connection and click **Delete** from the **Actions** dropdown menu.
6. In the prompt window that is displayed, click **Delete**. The VLAN connection is removed from the list.

Creating a Virtual Switch

You can create a Virtual Switch (VS) using the **Create Virtual Switch** window in Prism Central.

About this task

Perform the following steps to create a virtual switch.

For more information about virtual switch, see the Layer 2 Network Management section in the *AHV Administration Guide*.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Network & Security** > **Subnets** from the **Navigation Bar**.
   This displays the **Subnets** page.
3. Click **Network Config**.
   This displays the **Network Configuration** window.
4. Select the **Virtual Switch** tab, and then click **Create VS**.
5. In the **Create Virtual Switch** window that is displayed, provide the necessary information in the **General** step.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2820

Field	Description
Virtual Switch Name	Enter a name for the virtual switch.
Description	Provide a description for the virtual switch that helps identify the virtual switch.
Physical NIC MTU (bytes)	MTU must be a value in the range 1280 to 9216 inclusive.
Select Configuration Method	Select one of the two methods that you can use to implement the VS configuration: • **Standard (Recommended)**: This method ensures no disruptions occur to the workloads by putting the hosts in maintenance mode and migrating the VMs out of the host before applying the configuration. This process requires a longer duration of time to complete. The time required depends on the number and configuration of VMs. In this method, the VS configuration is deployed in the rolling update process. • **Quick**: This method interrupts the workloads running on the hosts. Use this method only if you are not running production workloads because it may result in network interruptions. In this method, the VS configuration is deployed in a rolling update process but the nodes are not put in maintenance mode before modifying the VS configuration on the node. **Note:** The **Quick** option in no longer available for creating a virtual switch. You can use the **Quick** method while updating a virtual switch.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2821

6. Click **Next** to go to the **Uplink Configuration** step.

   In the **Uplink Configuration** step, provide the following details:

Figure 148: Create Virtual Switch - Uplink Configuration tab

Field	Description and Value
Bond Type	Select an appropriate bond type. For information about the bond types, see the *Bond Types* table.
Select Hosts	Select the hosts that can host VMs.
Select Uplink Ports	Select the criteria that need to be satisfied for the uplink ports. The available uplink ports that satisfy the criteria are displayed in the (Host port) table at the bottom of this tab.
Show	(Port Type) Select one of the following: **Connected and Unconnected Uplink Ports**: Select this option to use ports that are not currently connected but may be connected later. **Only Connected Uplink Ports**: Select this option to use only the connected ports. You must also select the switches with LLDP in the **On Switches (with LLDP)** dropdown menu.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2822

Field	Description and Value
Uplink Port Speeds	Select a speed to display the ports that have the selected speed. You can select **10G** or **All Speeds**. The speeds displayed depend on the NIC type that is installed on the host. Based on your selection the columns in the (Host Port) table change dynamically to display the ports with the speeds you selected.
(Host Port) table	Based on your selections in **Select Uplink Ports**, a table displays the hosts that have the uplink ports that satisfy the selected criteria. Select the ports you need for this configuration from the list. Click the down arrow on the right side of the table to display the ports listed for each host. **Note:** A port listing is greyed out if it is unavailable because it is already associated with another virtual switch. Click **Select All** to select all the ports available and listed. Click **Clear All** to clear all the ports available and listed.

Table 73: Bond Types

Bond Type	Use Case	Maximum VM NIC Throughput	Maximum Host Throughput
Active-Backup	Recommended. Default configuration, which transmits all traffic over a single active adapter.	10 GB	10 GB
Active-Active with MAC pinning Also known as balance-slb	Works with caveats for multicast traffic. Increases host bandwidth utilization beyond a single 10 Gb adapter. Places each VM NIC on a single adapter at a time. Do not use this bond type with link aggregation protocols such as LACP.	10 GB	20 GB
Active-Active Also known as LACP with balance-tcp	LACP and link aggregation required. Increases host and VM bandwidth utilization beyond a single 10 Gb adapter by balancing VM NIC TCP and UDP sessions among adapters. Also used when network switches require LACP negotiation. The default LACP settings are: • Speed—Fast (1s) • Mode—Active fallback-active-backup • Priority—Default. This is not configurable.	20 GB	20 GB

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2823

Bond Type	Use Case	Maximum VM NIC Throughput	Maximum Host Throughput
No Uplink Bond	No uplink or a single uplink on each host. Virtual switch configured with the No uplink bond uplink bond type has 0 or 1 uplinks. When you configure a virtual switch with any other bond type, you must select at least two uplink ports on every node.	-	-

Note: The Maximum VM NIC Throughput and Maximum Host Throughput values are not restricted to the value provided in this table. The values in the table are indicated for an assumption of 2 x 10 Gb adapters.

For more information about uplink configuration, see Virtual Switch Workflow in the *AHV Administration Guide*.

7. Click **Create** to create the virtual switch.

   Click **Cancel** to exit without creating the virtual switch.

   Click **Back** to go back to the **General** step.

What to do next

Important:

You can migrate or convert the bridges other than br0 in the cluster to virtual switches after you upgraded the minimum or compatible version of AOS and AHV. You can convert the other bridges only on Prism Element web console or using aCLI. You can convert only one bridge at a time. You need to repeat the workflow for every bridge to be converted to a virtual switch.

For more information about converting the bridges other than br0, see Migrating Bridges after Upgrade in *Prism Element Web Console Guide*.

- If you select the **Active-Active** NIC-teaming policy, you must enable LAG and LACP on the corresponding ToR switch for each node in the cluster one after the other. For more information, see Enabling LACP and LAG (AHV Only) on page 354.

Updating a Virtual Switch

You can update an existing Virtual Switch (VS) using the **Edit Virtual Switch** window in Prism Central.

About this task

Perform the following steps to update an existing virtual switch.

For more information about virtual switch, see Layer 2 Network Management in the *AHV Administration Guide*.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Network & Security** > **Subnets** from the **Navigation Bar**.
   This displays the **Subnets** page.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2824

3. Click **Network Config**.
   This displays the **Network Configuration** window.

4. Select the **Virtual Switch** tab, and click the *Edit* icon associated with the virtual switch you want to update.
   This displays the **Edit Virtual Switch** window.

5. Update the necessary information for the virtual switch by following all the instructions mentioned in Steps 5 through 7 of Creating a Virtual Switch on page 349.

What to do next

> **Important:**
>
> You can migrate or convert the bridges other than br0 in the cluster to virtual switches after you upgraded the minimum or compatible version of AOS and AHV. You can convert the other bridges only on Prism Element web console or using aCLI. You can convert only one bridge at a time. You need to repeat the workflow for every bridge that you want to convert to a virtual switch.
>
> For more information about converting the bridges other than br0, see Migrating Bridges after Upgrade in *Prism Element Web Console Guide*.

- If you select the **Active-Active** NIC-teaming policy, you must enable LAG and LACP on the corresponding ToR switch for each node in the cluster one after the other. For more information, see Enabling LACP and LAG (AHV Only) on page 354.

Enabling LACP and LAG (AHV Only)

This section describes the procedure to enable LAG and LACP in AHV nodes and the Top-of-Rack (ToR) switch or any switch that is directly connected to the Nutanix node.

Procedure

To enable LACP and LAG, perform the following steps:

1. Login to the Prism Element web console and go to **Settings** > **Network Configuration** > **Virtual Switch**.
   You can also login to Prism Central, select the **Infrastructure** application from Application Switcher Function, and go to **Network & Security** > **Subnets** > **Network Configuration** > **Virtual Switch** from the navigation bar.
   The system displays the **Virtual Switch** tab.

2. Click the Edit icon ( ) for the target virtual switch on which you want to configure LACP and LAG.
   The system displays the **Edit Virtual Switch** window.

3. In the **General** tab, choose **Standard (Recommended)** option in the **Select Configuration Method** field, and click **Next**.

   > **Important:** When you select the **Standard** method, only the hosts that have been updated are restarted.
   >
   > The **Standard** configuration method puts each updated node in maintenance mode before applying the updated settings. After applying the updated settings, the node exits from maintenance mode. For more information, see Virtual Switch Workflow.

4. In the **Uplink** Configuration tab, select `Active-Active` in the **Bond Type** field, and click **Save**.

   > **Note:** The `Active-Active` bond type configures all AHV hosts with the fast setting for LACP speed, causing the AHV host to request LACP control packets at the rate of one per second from the physical switch. In addition,

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2825

the `Active-Active` bond type configuration sets LACP fallback to `Active-Backup` on all AHV hosts. You cannot modify these default settings after you have configured them in Prism, even by using the CLI.

This completes the LAG and LACP configuration on the cluster. At this stage, cluster starts the Rolling Reboot operation for all the AHV hosts. Wait for the reboot operation to complete before you put the node and CVM in maintenance mode and change the switch ports.

For more information about how to manually perform the rolling reboot operation for an AHV host, see Rebooting an AHV Node in a Nutanix Cluster.

Perform the following steps on each node, one at a time:

5. Put the node and the Controller VM into maintenance mode.

   Note: Before you put a node in maintenance mode, see Verifying the Cluster Health and carry out the necessary checks.

   The Step 6 in Putting a Node into Maintenance Mode using Web Console section puts the Controller VM in maintenance mode.

6. Change the settings for the interface on the switch that is directly connected to the Nutanix node to match the LACP and LAG settings made in the Edit Virtual Switch window above.

   For more information about how to change the LACP settings of the switch that is directly connected to the node, refer to the vendor-specific documentation of the deployed switch.

   Nutanix recommends you perform the following configurations for LACP settings on the switch:

Table 74: Nutanix Recommendations for LACP Settings

Nutanix Recommendations	Description
Enable LACP fallback	Nutanix recommends you enable LACP fallback to set up a workaround for the port, using which the port establishes a link before the switch receives the LACP Bridge Protocol Data Units (BPDUs). The LACP fallback helps avoid link failures if either AHV host or switch that is connected to the AHV node does not negotiate LACP. LACP fallback provides seamless discovery of new nodes in an active or passive capacity setup and reduces the impact on the node operation. When LACP fallback is enabled, you can have a minimal business impact as VMs and applications remain healthy in case of an LACP status mismatch between the AHV host and the ToR switch port. As LACP fallback ensures connectivity during initial deployment, so it is crucial when you do not have LACP in discoveryOS. **Caution:** When LACP fallback occurs, the port runs in fallback mode, and this might lead to an unbalanced utilization of ports and lack of redundancy in your site deployment. Based on your internal networking policies, you can decide whether LACP fallback is helpful for you, and enable or disable it.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2826

Nutanix Recommendations	Description
Consider the LACP time options *(slow and fast)*	If the switch has a fast configuration, Nutanix recommends you set the LACP time to fast on AHV host. Nutanix recommends the LACP time to match on both; switch and AHV host, for L2 failure detection at the same time on the switch and AHV host. If the switch has a fast configuration, set the LACP time to fast on AHV host. When the LACP time setting matches on AHV host and switch, the detachment of a failed interface occurs at the same time, and both switch and the AHV host do not use the failed interface. When the LACP time is set to: • *fast* - Failure detection occurs faster within 3 seconds • *slow* - Failure detection occurs slowly and takes up to 90 seconds The matching LACP time helps to prevent the outage.

7. Verify that LACP negotiation status is `Negotiated`.

   Perform the SSH to the CVM as a nutanix user, and run the following commands:

   ```
   nutanix@CVM$ ssh root@[AHV host IP] "ovs-appctl bond/show bond-name"
   ```

   ```
   nutanix@CVM$ ssh root@[AHV host IP] "ovs-appctl lacp/show bond-name”
   ```

   - Replace the following attributes in the above commands:
     - `bond-name` with the actual name of the uplink port such as br0-up in the above commands.
     - `[AHV host IP]` with the actual AHV host IP at your site.
   - Search for the string `negotiated` in the status lines.

8. Remove the node and Controller VM from maintenance mode. For more information, see Exiting a Node from the Maintenance Mode using Web Console.

   The Controller VM exits maintenance mode during the same process.

What to do next

Do the following after completing the procedure to enable LAG and LACP in all the AHV nodes the connected ToR switches:

- Verify that the status of all services on all the CVMs are Up. Run the following command and check if the status of the services is displayed as **Up** in the output:

  ```
  nutanix@cvm$ cluster status
  ```

- Log in to the Prism Element web console of the node and ensure that the **Cluster Resiliency / Fault Tolerance Status** widget displays **OK**.

Virtual Private Clouds

You can manage the virtual private clouds (VPCs) you have created and configured, from the **Virtual Private Clouds** page.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2827

Virtual Private Clouds Summary View

The **Virtual Private Clouds** page displays the list of virtual private clouds (VPCs) across all the registered clusters.

To access the **Virtual Private Clouds** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Network & Security** > **Virtual Private Clouds** from the **Navigation Bar**.

   The **Virtual Private Clouds** page opens displaying the **List** tab. This tab provides a list of virtual private clouds you have created and configured, and the operations you can perform on them.

> **Note:** For information on the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

The following table describes the fields that appear in the **Virtual Private Clouds** page.

> **Note:** The fields vary based on the **View by** and **Group by** options. A dash (-) is displayed in a field when a value is not available or applicable. For more information, see the View by on page 56 and Group by information.

Table 75: Virtual Private Clouds – Field Description

Field	Description
Name	Displays the name of the VPC. The **Name** of a VPC is suffixed with `Transit VPC` when you configure the VPC as a transit VPC.
Associated External Subnets	Displays the external subnet that the VPC is assigned to.
Categories	Displays the number of categories associated with the VPC.
Externally Routable IP Addresses	Displays the externally routable IP address.
Hypervisor	Displays the hypervisor that the VPC is hosted on.
Inter VN Traffic	Displays the traffic flowing between the virtual networks or VPCs.
Internet Traffic	Displays the traffic flowing to and from the Internet.
IPv4 Gateway	Displays the IPv4 gateway IP address.
IPv4/Subnet	Displays the IPv4 network IP with subnet prefix. For example, 10.20.30.0/24.
On-Prem Traffic	Displays the traffic flowing in the on-premises network.
VLAN ID	Displays the VLAN identification number. VLAN ID is a parameter used for Transit VPC networking in Nutanix Cloud Cluster with Microsoft Azure.

You can perform the following actions for the VPCs from the **Virtual Private Clouds** page:

- Click the name of a VPC to open the VPC details page, which displays the detailed information about the VPC. For more information, see Virtual Private Cloud Details View on page 358.
- Create a VPC by clicking **Create VPC**. For more information, see Creating Virtual Private Cloud in the *Flow Virtual Networking Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2828

- Update or delete an existing VPC using the **Actions** dropdown menu. The **Actions** dropdown appears when one or more VPCs are selected. For more information, see Updating Virtual Private Cloud or Deleting a Virtual Private Cloud in the *Flow Virtual Networking Guide*.
- View VPCs based on pre-defined criteria or create a custom view. For more information on the **View by** option, see View By information.
- Filter the VPC list based on a variety of parameter values using **Filters** pane. For more information, see Filters Pane - Virtual Private Clouds Page.

Filters Pane - Virtual Private Clouds Page

You can filter the information in the **Virtual Private Clouds** page based on the following fields that are available in the **Filters** pane. For information on how to use the Filters pane, see the Filters Pane information.

Table 76: Filter Pane Field Description - Virtual Private Clouds page

Field	Description	Values
Name	Filters based on the VPC name. It returns a list of IP addresses that satisfy the name condition/string.	(Virtual private cloud name string)
Associated External Subnets	Filters based on the external subnet that the VPC is assigned to.	(External Subnet)

Virtual Private Cloud Details View

The Virtual Private Cloud (VPC) details page consists of a dashboard that provides the detailed information about the VPC.

The details page has the **Summary**, **Subnets**, **Policies**, **Routes**, and **Metrics** tabs.

To access the details page of an individual VPC:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Network & Security** > **Virtual Private Clouds** from the **Navigation Bar**.

   Prism Central displays the **Virtual Private Clouds** page that contains information about all the VPCs configured for the registered clusters.
3. Click a VPC to open the details page of the VPC.

   The **Summary** tab opens displaying the detailed information about the VPC in widgets.

> **Note:** For information on the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

Summary Tab

The **Summary** tab provides detailed information about the VPC in widgets.

The **Summary** tab has the following widgets:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2829

Widget Name	Information provided
External Connectivity	Provides the following: • Associated External Subnets — Displays the number of external subnets associated with the VPC. • Externally Routable IP Addresses — Displays the external routable IP addresses associated with the VPC.
Transit VPC	Displays **Yes** if the VPC is a Transit VPC. Displays **No** if the VPC is not a Transit VPC.
Domain Name Servers (DNS)	Displays the IP address or the FQDN of the DNS servers used by the VPC.
Associations	Provides the following: • Subnets (Overlay) — Displays the number of subnets associated with the VPC. • Policies — Displays the number of policies associated with the VPC. • Routes — Displays the number of routes associated with the VPC.
Floating IP Addresses	Provides the following: • Assigned Floating IPs — Displays the floating IP addresses assigned to the VPC. • Available Floating IPs — Displays the available floating IP addresses that can be assigned to the VPC.

Subnets Tab

The **Subnets** tab displays the list of subnets added to the VPC.

The following table describes the fields that appear in the **Subnets** tab.

Table 77: Subnets Tab – Field Description

Field	Description
Name	Displays the subnet name.
IP Range	Displays the IP address range configured for the subnet.
DHCP IP Pool	Displays the IP address pool range assigned to the subnet.
Default Gateway IP	Displays the IP address used as the default gateway by the entities in the subnet.
Actions	Action link for editing or deleting the subnet.

You can perform the following actions for a subnet from the **Subnets** tab:

- Click the name of the subnet to open the subnet details page, which displays the detailed information about the subnet. For more information, see Subnet Details View on page 344.
- Create a subnet by clicking **Create Subnet**. For more information, see Creating a Subnet in the *Flow Virtual Networking Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2830

- Update an existing subnet using the **Delete** option associated with the subnet. For more information, see Updating a Subnet in the *Flow Virtual Networking Guide*.
- Delete an existing subnet using the **Delete** option associated with the subnet. For more information, see Deleting Subnets, Policies, or Routes in the *Flow Virtual Networking Guide*.

Policies Tab

The **Policies** tab displays information about the security-based traffic shaping policies you configured.

The following table describes the fields that appear in the **Policies** tab.

> **Note:** The fields vary based on the **View by** option. A dash (-) is displayed in a field when a value is not available or applicable. For more information, see the View by on page 56 information.

Table 78: Policies Tab – Field Description

Field	Description
Description	Displays the user-provided description of the policy.
Action	Displays the appropriate action for the implementation of the policy. • Permit: Permits traffic and services based on the parameters set. • Deny: Denies traffic and service based on the parameters set. • Re-route: Sends matching traffic to the next-hop IP address specified by the Reroute IP.
Priority	Displays the traffic priority.
Rule	Displays the **Permit** or **Deny** rule set for the priority.
Rule Type	Displays whether the rule is system generated or user defined.
Traffic	Displays the traffic type that the priority and rule should be applied to.
Virtual Network	Displays the ID of the subnet.
Source	Displays the source IP or subnet for which you want to manage traffic.
Destination	Displays the destination IP or subnet for which you want to set the priority.
Source Subnet	Displays the subnet IP and prefix designated as the source for the policy.
Destination Subnet	Displays the subnet IP and prefix designated as the destination for the policy.
Reroute Address	Displays the IP address to which the traffic is re-routed.
Bidirectional Policy	Displays whether the policy is bidirectional or not.
Protocol	Displays the type of protocol for which the policy is configured.
Protocol Number	Displays the protocol number for which the policy is configured.
ICMP Type	Displays the type of ICMP message associated with the policy.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2831

Field	Description
ICMP Code	Displays the ICMP code of the policy.
Byte Count	Displays the total number of traffic bytes that matches the given policy. The count is updated periodically.
Packet Count	Displays the total number of traffic packets that matches the given policy. The count is updated periodically.

You can perform the following actions for a policy from the **Policies** tab:

- Create a policy by clicking **Create Policy**. For more information, see Creating a Policy in the *Flow Virtual Networking Guide*.
- Perform the following actions using the **Actions** dropdown menu. The **Actions** dropdown appears when one or more policies are selected.
  - **Update**: Update the policy. For more information, see Updating a Subnet in the *Flow Virtual Networking Guide*.
  - **Delete**: Delete the policy. For more information, see Deleting Subnets, Policies, or Routes in the *Flow Virtual Networking Guide*.
  - **Clear Counters**: Reset the counters for the selected policy.
  - **Clear All Counters**: Reset the counters for all the policies.
- View policies based on pre-defined criteria or create a custom view. For more information on the **View by** option, see View By information.

Routes Tab

The **Routes** tab displays the list of static routes added to the VPC.

The following table describes the fields that appear in the **Routes** tab.

> **Note:** The fields vary based on the **View by** option. A dash (-) is displayed in a field when a value is not available or applicable. For more information on the View by option, see View by on page 56 information.

Table 79: Routes Tab – Field Description

Field	Description
Destination Prefix	Displays the IP address and prefix of the destination.
Next Hop	Displays the next hop network or subnet for the traffic exiting the VPC.
Priority	Displays the traffic priority.
Type	Displays the type of route, local or static.
Status	Displays the status of the route, whether it is active or not

You can perform the following actions for a route from the **Routes** tab:

- View routes based on pre-defined criteria or create a custom view. For more information on the View by option, see View by on page 56 information.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2832

- Perform the following actions using the **Manage Static Routes** option:
  - **Add Static Route**: Create a static route. For more information, see Creating Static Routes in the *Flow Virtual Networking Guide*.
  - Update an existing static route. For more information, see Updating Static Routes in the *Flow Virtual Networking Guide*.
  - Delete a static route. For more information, see Deleting Subnets, Policies or Routes in the *Flow Virtual Networking Guide*.

Metrics Tab

The **Metrics** tab displays detailed information about the VPC metrics.

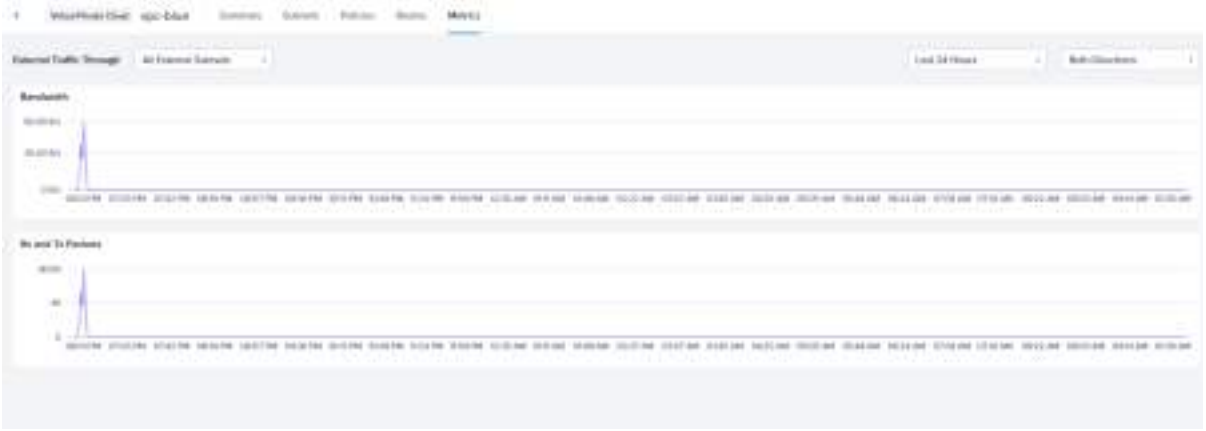


Figure 149: Metrics Tab

The following table describes the fields that appear in the **Metrics** tab.

Table 80: Metrics Tab – Field Description

Field	Description
External Traffic Through	Select **All External Networks** (default) or **(name_of_external_network_associated_with_the_VPC)** from the dropdown menu. The page displays the metrics based on your selection.
Last (time_period)	Select the period for which you want to display the metrics. The dropdown menu provides the following options: • **Last 24 Hours (default)** • **Last One Hour** • **Last Week**

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2833

Field	Description
Direction of traffic	Select the direction of traffic for which you want to display the metrics. The dropdown menu provides the following options: • **Both directions** (default) — Includes both directions, Ingress and Egress. • **Ingress** — Traffic entering the externally connected subnet. • **Egress** — Traffic leaving the externally connected subnet.
Bandwidth	Displays graphically the bandwidth utilization of the VPC on a timeline as set in the **Last (time_period)** parameter.
Rx and Tx Packets	Displays graphically the received and transmitted packet volume on a timeline as set in the **Last (time_period)** parameter.

Traffic Mirroring

Traffic Mirroring enables you to mirror traffic from the interfaces of the AHV hosts to the virtual NIC (vNIC) of guest VMs. Traffic Mirroring mirrors the packets from a set of source ports to a set of destination ports. You can mirror inbound, outbound, or bidirectional traffic flowing on a set of source ports. You can then use the mirrored traffic for security analysis and to gain visibility of traffic flowing through the set of source ports. Traffic Mirroring is a useful tool for troubleshooting packets and necessary for compliance.

> **Important:** If your cluster is not registered to Prism Central, you can use aCLI to configure the Traffic Mirroring session on an AHV host. For more information, see Configuring Traffic Mirroring on an AHV Host section in AHV Administration Guide.

Prism Central allows you to select the following entity types for source and destination:

- Source:
  - Individual host ports
  - Bonded host ports
  - Virtual machines

    > **Note:** You can only select up to four entities in total for all the source type entities.
- Destination: Virtual Machines

  > **Note:** You can select up to two destination type entities.

Source Ports

Prism Central supports the following types of source ports in a Traffic Mirroring session:

- A bond port that is already mapped to a virtual switch (vs) such as vs0, vs1, or any other vs that you created
- A non-bond port that is already mapped to a vs such as vs0, vs1, or any other vs that you created
- An uplink port that is not assigned to any vs or bridge on the host
- A virtual port attached to a VM

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2834

Important Considerations

Consider the following before you create Traffic Mirroring sessions:

- Prism Central supports Traffic Mirroring from physical and VM interfaces. Therefore, a source port can be a physical or VM interface.
- Prism Central supports Traffic Mirroring to destination guest VMs running on the same AHV host (to which the source ports belong) or on a remote AHV host.
- VM interface port/bond supports Traffic Mirroring to a destination on a remote host.
- Physical source port/bond interface does not support Traffic Mirroring to a destination on a remote host.
- In a single Traffic Mirroring session, if both remote and local host destinations are available, the physical source port/bond interface is mirrored only to the local destination, while the VM interface port/bond is mirrored to both remote and local destinations.
- Nutanix does not support Traffic Mirroring on Nutanix clusters connected to AWS or Azure.
- Prism Central supports different types of source ports in one session. For example, you can create a session with br0-up (bond port) and eth5 (single uplink port) on the same host as two different source ports in the same session. You can have two different bond ports in the same session.
- Delete the Traffic Mirroring session before you delete the Traffic Mirroring destination VM or vNIC. Otherwise, the state of the Traffic Mirroring session is displayed as an error.
- If you migrate a destination VM, delete the vNIC, or if the physical port is down, the Traffic Mirroring session displays an error status.
- If all vNICs are migrated to the same host, the traffic mirror session displays active status. However, if the session has physical NICs (pNICs), the Traffic Mirroring session displays an error status.
- You cannot configure the direction of the traffic if the ports are not managed by a virtual switch.
- You can select one source VM vNIC for a single Traffic Mirroring session.
- You can select one destination VM vNIC for a single Traffic Mirroring session.

Traffic Mirroring Session Scale

Traffic Mirroring session supports the following scale:

Table 81: Traffic Mirroring Session Scale

Entities	Scale
Source ports or entities	4 entities per Traffic Mirroring session
Destination ports or entities	2 entities per Traffic Mirroring session
Maximum number of Traffic Mirror sessions	1,000 per cluster
Maximum number of Active Sessions	2 per host

Traffic Mirroring Summary View

The Traffic Mirroring page displays information about all the Traffic Mirroring sessions created across registered clusters.

To access the summary view of all the Traffic Mirroring sessions, perform the following steps:

1. Log in to Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2835

2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Network & Security** > **Traffic Mirroring** from the **Navigation Bar**.

   The **Traffic Mirroring** page opens displaying the **List** tab. This tab provides information about all the Traffic Mirroring sessions configured for the clusters.

   > **Note:** For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

The following table describes the fields that are displayed in the **List** tab.

> **Note:** The fields vary based on the **View by** option. A dash (-) is displayed in a field when a value is not available or applicable. For more information, see the View by on page 56 information.

Table 82: Traffic Mirroring - Field Description

Field	Description	Values
Name	Displays the Traffic Mirroring session name.	(Traffic Mirroring session name)
Source (Ingress)	Traffic entering the source.	(source VM, MAC address)
Source (Egress)	Traffic leaving the source.	(source VM, MAC address)
Destinations	Displays the destination virtual machine with MAC address.	(destination VM, MAC address)
State	Displays the current operational status of the Traffic Mirroring session.	(Enabled, Disabled)

You can perform the following actions from the **List** tab:

- Click the name of a Traffic Mirroring session to open the details page, which displays detailed information about the Traffic Mirroring session.
- Create a Traffic Mirroring session by clicking **Create Mirror Session**. For more information, see Creating a Traffic Mirroring Session on page 368.
- Download the table of Traffic Mirroring sessions in CSV format by clicking **Export**.
- View the reports based on pre-defined criteria or create a custom view. For more information, see View by on page 56.
- Filter the Traffic Mirroring session list based on a variety of parameter values using the **Modify Filters** pane. For more information, see
- Perform the following actions on a Traffic Mirroring session using the **Actions** dropdown menu.

Table 83: Traffic Mirror Session Actions

Action	Description
Disable Session	Click this action to disable the Traffic Mirroring session. For more information, see Disabling a Traffic Mirroring Session on page 373.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2836

Action	Description
Enable Session	Click this action to enable the Traffic Mirroring session. For more information, see Enabling a Traffic Mirroring Session on page 374.
Update	Click this action to update the Traffic Mirroring session. For more information, see Updating a Traffic Mirroring Session on page 374.
Delete	Click this action to delete the Traffic Mirroring session. For more information, see Deleting a Traffic Mirroring Session on page 375.

Filters Pane - List Tab

You can filter the information in the **List** tab based on the following fields available in the **Filters** pane. For information about how to use the **Filters** pane, see the Filters Pane information.

Table 84: Filter Pane Field Description - Traffic Mirroring Session

Field	Description	Values
Name	Filters based on the application instance name. Select the checkbox, and choose a condition from the dropdown menu (**Contains**, **Equal to**, **Not Equal to**, **Doesn't contain**, **Starts with**, **Ends with**, or) and enter a string in the field.	(Traffic Mirroring Session name string)
State	Filters based on the state of the Traffic Mirroring session. Select the checkbox for Enabled, or Disabled, or both.	Enabled, Disabled

Traffic Mirroring Details View

The Traffic Mirroring details page consists of dashboard widgets that provide detailed information about the Traffic Mirroring sessions.

To access the details page of an individual Traffic Mirroring session, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Network & Security** > **Traffic Mirroring** from the **Navigation Bar**.

   The **Traffic Mirroring** page opens displaying the **List** tab. This tab provides information about all the Traffic Mirroring sessions configured for the clusters.
3. Click the name of a Traffic Mirroring session to open the details page.

   The **Summary** tab opens displaying the detailed information about the Traffic Mirroring session in widgets.

The following figure shows the **Summary** page of an individual **Traffic Mirroring Session**:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2837

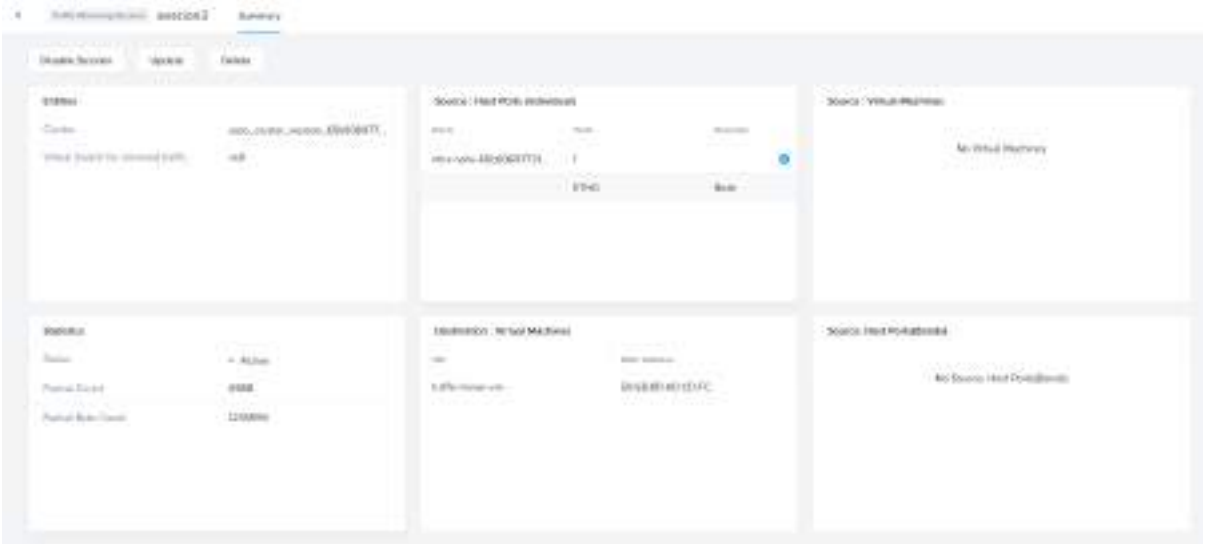


Figure 150: Traffic Mirroring Session Details View

The **Summary** page has the following widgets:

Table 85: Traffic Mirroring Session Summary Tab Widgets

Widget	Parameters
Entities	• Cluster: Displays the cluster name. • Virtual Switch for Mirrored Traffic: Displays the virtual switch used for Traffic Mirroring.
Source: Host Ports ((Individual)	• Hosts: Displays the host name. • Ports: Displays the host port details. • Direction: Displays the traffic direction of the host port.
Source: Virtual Machines	• VM: Displays the name of the source virtual machine. • MAC Address: Displays the MAC address of the source virtual machine.
Statistics	• Status: Displays the operational status of the Traffic Mirroring session. • Packet Count: Displays the packet count mirrored and received from the destination. • Packet Byte Count: Displays the packet byte count derived from the packet count.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2838

Widget	Parameters
Destination: Virtual Machines	• VM: Displays the name of the destination virtual machine. • MAC Address: Displays the MAC address of the destination virtual machine.
Source: Host Ports(Bonds)	• Hosts: Displays the host name. • Bonds: Displays the bond name. • Ports: Displays the details of the bonds on the host port. • Direction: Displays the direction of the traffic on the host port bonding.

You can perform the following actions from the Summary tab:

- Disable an existing Traffic Mirroring session by clicking **Disable Session**.
- Update an existing Traffic Mirroring session by clicking **Update**.
- Delete an existing Traffic Mirroring session by clicking **Delete**.

Creating a Traffic Mirroring Session

Prism Central allows you to create a Traffic Mirroring session to mirror inbound, outbound, or bidirectional traffic on a set of source ports.

Before you begin

Ensure that you configure the traffic mirror type on the vNIC of the destination VM. For more information about adding a traffic mirror type vNIC to the destination VM, see Creating a VM through Prism Central (AHV) on page 130.

About this task

Follow these steps to create a Traffic Mirroring session that replicates the traffic from a set of source ports to a set of destination ports:

Procedure

1. Log in to Prism Central.
2. From the Application Switcher Function on page 45, select the **Infrastructure** application and from the navigation bar, select **Network & Security** > **Traffic Mirroring**.
   The **Traffic Mirroring** page opens displaying the **List** tab. This tab provides information about all the Traffic Mirroring sessions configured for the registered clusters.
3. Click **Create Mirror Session**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2839

4. In the **General** tab, enter the following information:

   a. **Name**: Enter a name for the Traffic Mirroring session.

   b. **Description**: Enter an optional description for the Traffic Mirroring session.

   c. **Cluster**: From the dropdown menu, select the cluster.

   d. **Virtual Switch for mirrored traffic**: From the dropdown menu, select the virtual switch where the Traffic Mirroring session is to be created.

   > **Note:** Nutanix recommends utilizing a non-default Virtual Switch with Maximum Transmission Unit (MTU) configured between 1600-9000 for Traffic Mirroring to a destination on the remote host. The default virtual switch **VS0**, can also be used for SPAN with MTU set to 1600 bytes. For more information on MTU, see Requirements and Limitations of Flow Virtual Networking and Configuring Virtual Switch for VPC Traffic Types.

5. Click **Next**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2840

6. In the **Source & Destination** tab, follow these steps to select the individual host ports:

   a. From the **Source Type(s)** dropdown menu, select **Host Ports (Individual)**.

   b. On the **Hosts Ports (Individual)** panel, click **Select Host Ports**.
   Select Host Ports (Individual) window appears.

   c. Click the down arrow icon next to the host name.
   The system displays **NICs** associated with the host along with the drop-down menu to select the **Traffic Direction**.

   d. Under **NICs**, select the checkbox of the Ethernet port to mirror the traffic for.

   e. Under **Traffic Direction**, from the dropdown menu, select the direction of the traffic.
   The **Traffic Direction** dropdown menu provides the following options:

   - **Both** (default): Includes both directions, Ingress and Egress.
   - **Ingress**: Traffic entering the source port.
   - **Egress**: Traffic leaving the source port.

   > **Note:** Traffic direction is unavailable if the ports are not managed by a virtual switch (vs).

   f. Click **Save**.

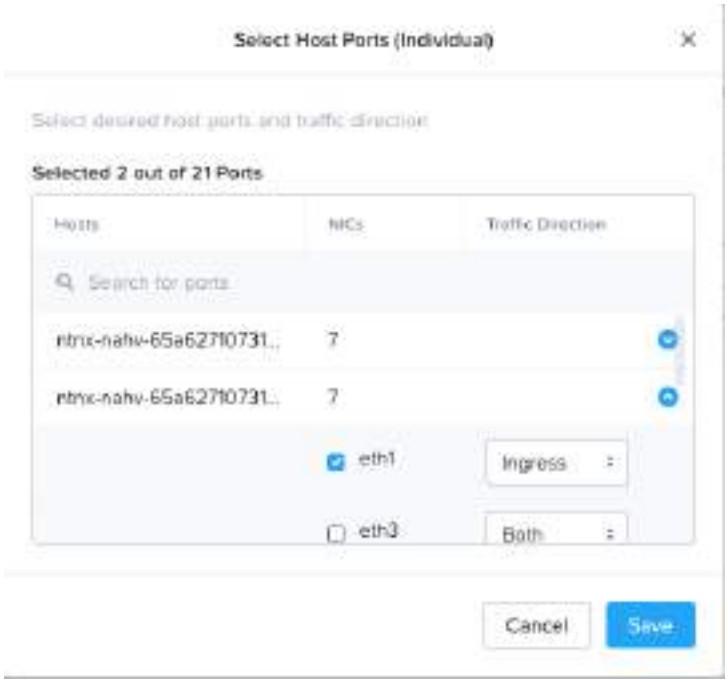


Figure 151: Individual Host Ports - Source

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2841

7. In the **Source & Destination** tab, follow these steps to select the bonded host ports:

   a. From the **Source Type(s)** dropdown menu, select **Host Ports (Bond)**.

   b. On the **Hosts Ports (Bond)** panel, click **Select Host Ports**.
   Select Host Ports (Bond) window appears.

   c. Click the down arrow icon next to the host name.
   The system displays **Bonds** and **Ports** associated with the host along with a drop-down menu to select the **Traffic Direction**.

   d. Under **Bonds**, select the checkbox of the bonded port to mirror the traffic for.

   e. Under **Direction**, from the dropdown menu, select the direction of the traffic.
   The **Direction** dropdown menu provides the following options:

   - **Both** (default): Includes both directions, Ingress and Egress.
   - **Ingress**: Traffic entering the source port.
   - **Egress**: Traffic leaving the source port.

   f. Click **Save**.

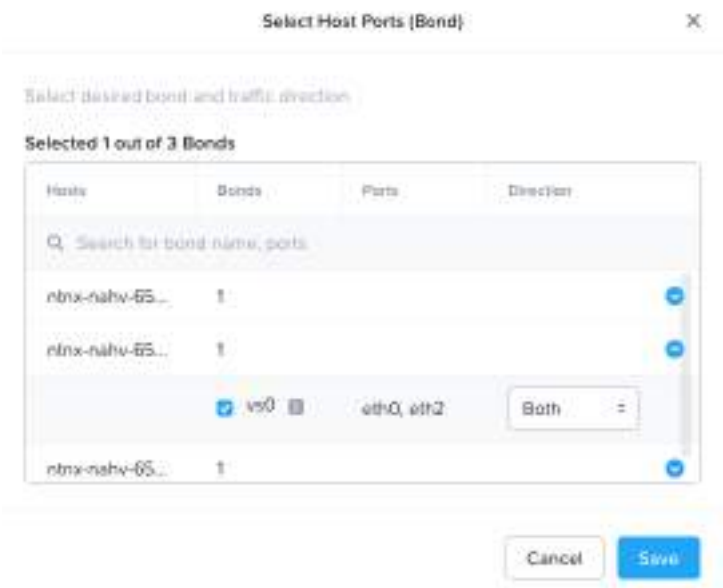


Figure 152: Bonded Host Ports - Source

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2842

8. In the **Source & Destination** tab, follow these steps to select the host virtual machines:

   a. From the **Source Type(s)** dropdown menu, select **Virtual Machines**.

   b. On the **Virtual Machines** panel, click **Select Virtual Machines**.
   Select Virtual Machines window appears.

   c. Under **Virtual Machine**, from the dropdown menu, select the source virtual machine.

   d. Under **MAC Address**, from the dropdown menu, select the MAC address.

   e. Under **Direction**, from the dropdown menu, select the direction of the traffic.
   The **Direction** dropdown menu provides the following options:

      - **Both** (default): Includes both directions, Ingress and Egress.
      - **Ingress**: Traffic entering the source VM.
      - **Egress**: Traffic leaving the source VM.

   f. (Optional) To add an additional VM, click **Add VM**.

   g. Click **Save**.

Figure 153: Virtual Machine - Source

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2843

9. In the **Source & Destination** tab, follow these steps to select the destination virtual machines:

   a. Under destination, click **Select Virtual Machines**.
   Select Virtual Machines window appears.

   b. Under **Virtual Machine**, from the dropdown menu, select the destination virtual machine.

   c. Under **MAC Address**, from the dropdown menu, select the MAC address.

   d. (Optional) To add an additional VM, click **Add VM**.

   e. Click **Save**.

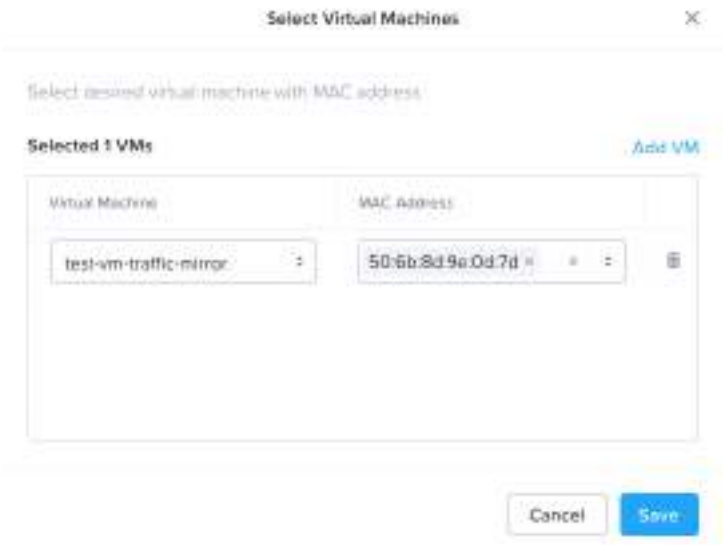


Figure 154: Virtual Machine - Destination

10. Click **Next**.

11. In the **Summary** tab, verify the Traffic Mirroring session details and do one of the following:

   » To create a session, click **Create Session**.

   » To create and enable a session, click **Create and Enable Session**.

Disabling a Traffic Mirroring Session

Prism Central allows you to disable an existing Traffic Mirroring session.

About this task

You can disable a Traffic Mirroring session to stop mirroring the traffic to the destination VM.

Procedure

1. Log in to Prism Central.

2. From the Application Switcher Function on page 45, select the **Infrastructure** application and from the navigation bar, select **Network & Security** > **Traffic Mirroring**.
   The **Traffic Mirroring** page opens displaying the **List** tab. This tab provides information about all the Traffic Mirroring sessions configured for the registered clusters.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2844

3. Select the checkbox of the Traffic Mirroring session you want to disable.
4. From the **Actions** dropdown menu, select **Disable Session**.
   Prism Central displays the **Disable Session** window.
5. Click **Disable Session**.

Enabling a Traffic Mirroring Session

Prism Central allows you to enable a Traffic Mirroring session.

About this task

You can enable a Traffic Mirroring session that you have created to start mirroring the traffic to the destination VM.

Procedure

1. Log in to Prism Central.
2. From the Application Switcher Function on page 45, select the **Infrastructure** application and from the navigation bar, select **Network & Security** > **Traffic Mirroring**.
   The **Traffic Mirroring** page opens displaying the **List** tab. This tab provides information about all the Traffic Mirroring sessions configured for the registered clusters.
3. Select the checkbox of the Traffic Mirroring session you want to enable.
4. From the **Actions** dropdown menu, select **Enable Session**.
   Prism Central displays the**Enable Session** window.
5. Click **Enable Session**.

Updating a Traffic Mirroring Session

Prism Central allows you to update a Traffic Mirroring session.

About this task

Update a Traffic Mirroring session to modify parameters such as name, description, cluster, host, source and destination types.

Procedure

1. Log in to Prism Central.
2. From the Application Switcher Function on page 45, select the **Infrastructure** application and from the navigation bar, select **Network & Security** > **Traffic Mirroring**.
   The **Traffic Mirroring** page opens displaying the **List** tab. This tab provides information about all the Traffic Mirroring sessions configured for the registered clusters.
3. Select the checkbox of the Traffic Mirroring session you want to update.
4. From the **Actions** dropdown menu, select **Update**.
   Prism Central displays the **Update Mirror Session** window, which includes the same fields as the **Create Mirror Session** window. For information about creating a Traffic Mirroring Session, see Creating a Traffic Mirroring Session on page 368.
5. Modify the Traffic Mirroring session based on your requirements and click **Update Session**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2845

Deleting a Traffic Mirroring Session

Prism Central allows you to delete a Traffic Mirroring session.

About this task

You can delete a Traffic mirroring session to permanently remove from the Traffic Mirroring session page list.

Procedure

1. Log in to Prism Central.
2. From the Application Switcher Function on page 45, select the **Infrastructure** application and from the navigation bar, select **Network & Security** > **Traffic Mirroring**.
   The **Traffic Mirroring** page opens displaying the **List** tab. This tab provides information about all the Traffic Mirroring sessions configured for the registered clusters.
3. Select the checkbox of the Traffic Mirroring session you want to delete.
4. From the **Actions** dropdown menu, select **Delete**.
   Prism Central displays the **Delete Session** window.
5. Click **Delete Session**.

Traffic Mirroring Session Alerts

Prism Central generates the Traffic Mirroring session alerts for the following inconsistent state scenarios:

> **Note:** For more information about the Alerts generated in Prism Central, see Prism Central Alerts and Events Reference Guide.

Table 86: Traffic Mirror Session Alerts List

Alert Title	Possible Cause
Inconsistent SPAN Session State Detected	This alert occurs when a VM NIC is removed from the destination VM.
Inconsistent SPAN Session State Detected	This alert occurs when a destination VM is migrated to another host.
Inconsistent SPAN Session State Detected	This alert occurs when a destination VM is powered off.

Role-Based Access Control in Traffic Mirroring

Prism Central supports role-based access control (RBAC) that allows you to configure and provide customized access to the users based on their assigned roles for the Traffic Mirroring entity. For more information on configuring RBAC, see Controlling User Access (RBAC).

From the Prism Central roles dashboard, you can define and assign the following roles to users or user groups:

- Predefined built-in roles (system roles)
- Custom roles

Any user with the following predefined built-in roles can configure the Traffic Mirroring functionality:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2846

- Network Infra Admin
- Prism Admin

For more information on predefined built-in and custom roles, see Built-in Role Management and Custom Role Management in the *Security Guide*.

Traffic Mirroring Permissions

The following table lists all of the permissions that you can add to a custom role and assign that custom role to the user to perform various Traffic Mirroring tasks.

Table 87: Traffic Mirroring Permissions

Traffic Mirroring Permissions
Create Traffic Mirror
Delete Traffic Mirror
Update Traffic Mirror
View Traffic Mirror
View Traffic Mirror Stats
View Cluster
View Cluster Networking Capabilities
View Host
View Uplink Bond
View VM

Floating IPs

You can access the floating IP addresses you have created and configured, from the **Floating IPs** page.

For information on floating IP addresses and their role in flow virtual networking, see the *SNAT and Floating IP Address* section in the Essential Concepts topic of the *Flow Virtual Networking Guide*.

> **Note:** Floating IP addresses are not reachable (Pings fail) unless you associate them to primary or secondary IP addresses of VMs. For more information, see Assigning Secondary IP Addresses to Floating IPs in the *Flow Virtual Networking Guide*.

For information on the limitation on using floating IP on a guest VM with load balancing configuration, see Network Load Balancer.

Floating IPs Summary View

The **Floating IPs** page displays the list of floating IP addresses across all the registered clusters.

To access the **Floating IPs** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Network & Security** > **Floating IPs** from the **Navigation Bar**.

   The **Floating IPs** page opens displaying the **List** tab. This tab provides a list of floating IPs you have created and configured, and the operations you can perform on the IPs.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2847

> **Note:** For information on the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

The following table describes the fields that appear in the **Floating IPs** page.

> **Note:** The fields vary based on the **View by** option. A dash (-) is displayed in a field when a value is not available or applicable. For more information, see the View by on page 56 information.

Table 88: Floating IPs – Field Description

Parameter	Description	Values
Floating IP Address	Displays the floating IP address assigned.	(IP address)
External Subnet	Displays the name of the external subnet that the IP address is assigned to.	(Name of the assigned subnet)
Association Status	Displays the status of association between the IP address and the external subnet and VPC.	Associated
VPC	Displays the name of the VPC associated with the IP address.	(Name of the associated VPC)
VM Name	Displays the name of the VM associated with the IP address.	(Name of the assigned VM)
Private IP	Displays the private IP address assigned to the same VM. This private IP address is assigned from the internal private subnet that the network controller creates when you crate a network gateway.	(IP address)

You can perform the following actions for the floating IP addresses from the **Floating IPs** page:

- Request a floating IP address by clicking **Request Floating IP**. For more information, see Requesting Floating IPs in the *Flow Virtual Networking Guide*.
- Update or delete an existing floating IP address using the **Actions** dropdown menu. The **Actions** dropdown appears when one or more addresses are selected.
  - **Update**: Assign or change the assignment of the floating IP address. You can assign the floating IP address to a IP address such as a private IP address in a VPC or the primary IP address of a VM or a secondary IP address created on a VM.
  - **Delete**: Delete the floating IP address. The deleted IP address returns to the IP address pool as unused. Before you delete a floating IP address, ensure that it is not assigned to a private IP address or a VM. Change the assignment to None if it is already assigned, using the **Update** option.
- View floating IP addresses based on pre-defined criteria or create a custom view. For more information on the **View by** option, see View By information.
- Filter the floating IP addresses list based on a variety of parameter values using **Filters** pane. For more information, see Filters Pane - Floating IPs Page.

Filters Pane - Floating IPs Page

You can filter the information in the **Floating IPs** page based on the following fields that are available in the **Filters** pane. For information on how to use the Filters pane, see the Filters Pane information.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2848

Table 89: Filter Pane Field Description - Floating IPs page

Field	Description	Values
Floating IP Address	Filters based on the floating IP address assigned. It returns a list of IP addresses that satisfy the string.	(Floating IP address)
External Subnet	Filters based on the external subnet that the IP address is assigned to.	(External Subnet)

Connectivity

You can access network gateways, VPN connections, subnet extensions, and BGP sessions from the **Connectivity** page.

To access the **Connectivity** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Connectivity** page opens displaying the **Gateways** tab. This tab provides a list of network Gateways you have created and configured, and the operations you can perform on the network Gateways.

- To view the VPN connections, click the **VPN Connections** tab.
- To view the subnets extended across the clusters, click the **Subnet Extensions** tab.
- To view the BGP sessions created for the clusters, click the **BGP Sessions** tab.

Gateways Summary View

The **Gateways** page displays a list of gateways created for the clusters managed by Prism Central.

To access the **Gateways** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways you have created and configured, and the operations you can perform on the network gateways.

> **Note:** For information on the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

The following table describes the fields that appear in the **Gateways** page.

Table 90: Field Descriptions for the Gateway Page

Parameter	Description	Values
Name	Displays the name of the gateway.	(Name of gateway)
Type	Displays the gateway type.	(Local or Remote)
Service	Displays the service that the gateway uses.	(VPN or VTEP)
Service IP	Displays the IP address used by the service.	(IP address)
Status	Displays the operational status of the gateway.	(Up or Down)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2849

Parameter	Description	Values
Attachment Type/Vendor	Displays the type of subnet associated with the gateway.	(VLAN or Overlay-VPC name)
Connections	Displays the number of service connections (such as VPN connections) configured and operational on the gateway.	(Number)

You can perform the following actions for a gateway from the **Gateways** page:

- Click the name of a gateway to open the gateway details page, which displays the detailed information about the gateway. For more information, see Gateway Details View on page 379.
- Create a local or remote gateway with VPN or VTEP service by clicking the **Create Gateway** dropdown menu. For more information, see Creating a Network Gateway in the *Flow Virtual Networking Guide*.
- Update or delete an existing gateway using the **Actions** dropdown menu. The **Actions** dropdown menu appears when one or more gateways are selected. For more information, see Updating a Network Gateway or Deleting a Network Gateway in the *Flow Virtual Networking Guide*.
- Filter the gateway list based on various parameter values using the **Filters** pane. For more information, see Filters Pane - Gateways Page.

Filters Pane on the Gateways Page

You can filter the information in the **Gateways** page based on the following fields that are available in the **Filters** pane. For information on how to use the Filters pane, see the Filters Pane information.

Table 91: Filter Pane Field Descriptions for the Gateways page

Field	Description	Values
Name	Filters based on the gateway name. It returns a list of gateways that satisfy the name condition/string.	(Gateway name string)
Service IP	Filters based on IP address used by the service.	(IP address)
Status	Filters based on the operational status of the gateway.	(Up or Down)

Gateway Details View

The **Summary** page of an individual gateway consists of a dashboard that provides the detailed information about the gateway.

To access the **Summary** page of an individual gateway:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways that you have created and configured.
3. Click a gateway to view the **Summary** page of the gateway.

> **Note:** For information on the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

The gateway **Summary** page has the following widgets:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2850

Table 92: Field Descriptions for the Gateway Widgets

Parameter	Description	Values
Properties widget		
Type	Displays the gateway type.	(Local or Remote)
Attachment Type	Displays the network entity like VLAN or VPC that the gateway is attached to.	(VLAN or VPC)
VPC or Subnet (VLAN)	Displays the name of the attached VPC or VLAN subnet.	(Name of VLAN or VPC)
Vendor (Applicable only if you select remote gateway)	Displays the name of the vendor of the gateway appliance at the remote site.	(Name of Vendor)
Floating or Private IP Address	Displays the Floating (for VPC) or Private (for VLAN) IP address assigned to the gateway.	(IP Address)
External IP (Applicable only if you select remote gateway)	Displays the IP address assigned to the remote gateway.	(IP Address that you assigned to the remote gateway.)
Status	Displays the operational status of the gateway.	(Up or Down)
Gateway Version	Displays the version of the Nutanix gateway appliance deployed.	(Version)
Cluster	Displays the name of the cluster on which the gateway is created.	(Cluster name)
Gateway VM	Displays the name of the VM on which the gateway is created.	(Name of VM - actionable link. Click the name-link to open the VM details page of the gateway VM.)
Service Configuration widget		
Service	Displays the service used by the gateway.	(VPN or VTEP or BGP)
VPN Service Configuration		
External Routing	Displays the type of routing associated with the gateway for external traffic routing.	(Static or eBGP with ASN)
Internal Routing	Displays the type of routing associated with the gateway for internal traffic routing.	(Static or eBGP with ASN)
VPN Connections	Displays the total number of VPN connections associated with the gateway.	(Number - actionable link. Click the link to open the VPN connection details page for the associated VPN connection.)
View VPN Connections	Click this link to open the VPN Connections tab.	-
VTEP Service Configuration		
VXLAN (UDP) Port	Displays the VXLAN (UDP) Port for the gateway.	(Number)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2851

Parameter	Description	Values
Subnet Extensions	Displays the total number of subnet extensions associated with the gateway.	(Number - actionable link. Click the link to open the subnet extensions details page for the associated subnet extension.)
View Subnet Extensions	Click this link to open the **Subnet Extensions** tab.	-
BGP Service Configuration		
ASN	Displays the ASN of the EBGP route.	(Number)
BGP Sessions	Displays the total number of BGP sessions associated with the gateway.	(Number - actionable link. Click the link to open the BGP sessions details page for the associated BGP session.)
Serviced VPC	Displays VPC service used by the gateway.	(Name of VPC)
View BGP Sessions	Click this link to open the **BGP Sessions** tab.	-

You can perform the following actions for a gateway from the **Summary** tab:

- Update an existing gateway by clicking **Update**. For more information, see Updating a Network Gateway in the *Flow Virtual Networking Guide*.
- Delete the gateway by clicking **Delete**. For more information, see Deleting a Network Gateway in the *Flow Virtual Networking Guide*.

VPN Connections Summary View

The **VPN Connections** page displays a list of VPN connections created for the clusters managed by Prism Central.

A VPN connection represents the VPN IPSec tunnel established between local gateway and remote gateway. When you create a VPN connection, you must select two gateways between which you want to create the VPN connection.

To access the **VPN Connections** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways.
3. Click the **VPN Connections** tab.

   The **VPN Connections** page opens displaying the list of VPN connections created for the clusters.

> **Note:** For information on the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

The following table describes the fields that appear in the **VPN Connections** page.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2852

Table 93: Field Descriptions for the VPN Connections Page

Parameter	Description	Values
Name	Displays the name of the connection.	(gateway name)
IPSec Status	Displays the connection status of IPSec tunnel.	(Connected or Not Connected)
EBGP Status	Displays the status of the EBGP gateway connection.	(Established or Not Established)
Local Gateway	Displays the name of the local gateway used for the connection.	(Name of local gateway)
Remote Gateway	Displays the name of the remote gateway used for the connection.	(Name of remote gateway)
Dynamic Routing Priority	Displays the dynamic routing priority assigned to the connection for throughput management. You can assign any value in the range of 100-1000. Nutanix Flow Virtual Networking assigns the first VPN connection the value 500 by default. Thereafter, subsequent VPN connections are assigned values decremented by 50. For example, the first connections is assigned 500, then the second connection is assigned 450, the third one 400 and so on.	(Number in the range of 100-1000. User assigned.)

You can perform the following actions for a VPN connection from the **VPN Connections** page:

- Click the name of a VPN connection to open the VPN connection details page, which displays the detailed information about the connection. For more information, see VPN Connection Details View on page 383.
- Create a VPN connection by clicking **Create VPN Connection**. For more information, see Creating a VPN Connection in the *Flow Virtual Networking Guide*.
- Update or delete an existing VPN connection using the **Actions** dropdown menu. The **Actions** dropdown appears when one or more VPN connections are selected. For more information, see Updating VPN Connection or Deleting a VPN Connection in the *Flow Virtual Networking Guide*.
- Filter the VPN connection list based on various parameter values using the **Filters** pane. For more information, see Filters Pane - VPN Connections Page.

Filters Pane on the VPN Connections Page

You can filter the information in the **VPN Connections** page based on the following fields that are available in the **Filters** pane. For information on how to use the Filters pane, see the Filters Pane information.

Table 94: Filter Pane Field Descriptions for the VPN Connections page

Field	Description	Values
Name	Filters based on the VPN connection name. It returns a list of VPN connections that satisfy the name condition/string.	(VPN connection name string)
EBGP Status	Filters based on the status of the EBGP gateway connection.	(Established or Not Established)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2853

Field	Description	Values
IPSEC Status	Filters based on the connection status of IPSec tunnel.	(Connected or Disconnected)

VPN Connection Details View

The VPN Connection details page provides detailed information about a VPN connection.

The details page has the **Summary**, **Throughput**, **IPSec Logging**, and **Routing Protocol Logging** tabs.

To access the details page of an individual VPN connection:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways you have created and configured.
3. Click the **VPN Connections** tab.

   The **VPN Connections** page opens displaying the list of VPN connections created for the clusters.
4. Click the name of a VPN connection to open the details page of the connection.

   The **Summary** tab opens displaying the detailed information about the VPN connection in widgets.

> **Note:** For information on the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

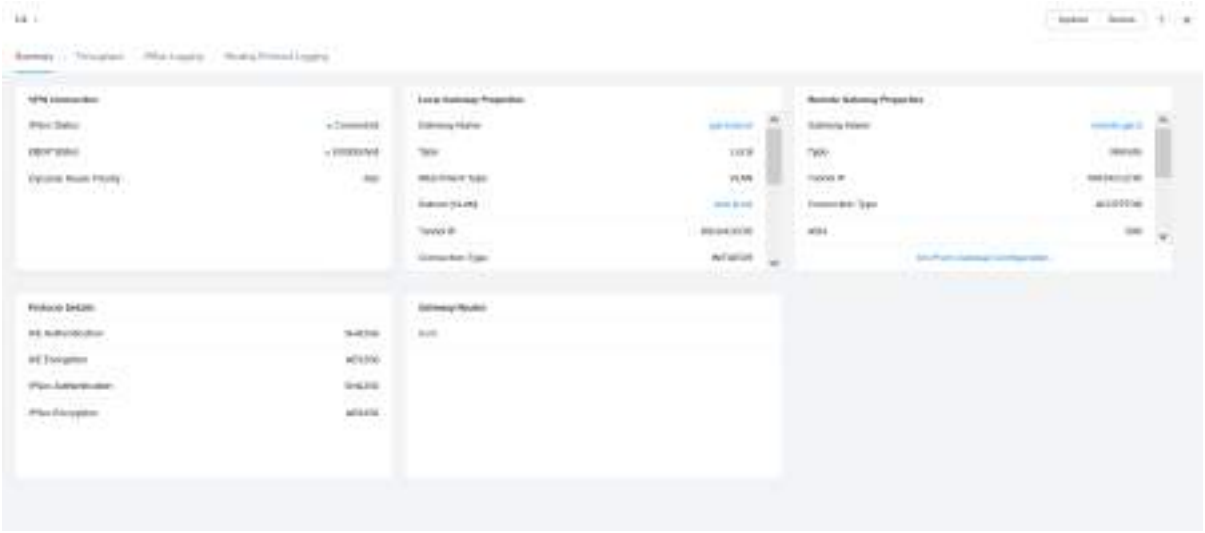


Figure 155: VPN Connection Details

Summary Tab

The **Summary** tab provides detailed information about a VPN connection in widgets.

The following table describes the fields that appear in the **Summary** tab.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2854

Table 95: Field Descriptions for the Summary Tab

Parameter	Description	Values
VPN Connection widget		
IPSec Status	Displays the connection status of IPSec tunnel.	(Connected or Not Connected)
EBGP Status	Displays the status of the EBGP gateway connection.	(Established or Not Established)
Dynamic Routing Priority	Displays the dynamic routing priority assigned to the connection for throughput management. You can assign any value in the range of 100-1000. Flow Virtual Networking assigns the first VPN connection the value 500 by default. Thereafter, subsequent VPN connections are assigned values decremented by 50. For example, the first connections is assigned 500, then the second connection is assigned 450, the third one 400 and so on.	(Number in the range of 100-1000. User assigned.)
Local Gateway Properties widget		
Gateway Name	Displays the name of the local gateway used for the connection.	(Name of local gateway)
Type	Displays the type of gateway.	(Local)
Attachment Type	Displays the network entity like VLAN or VPC that the gateway is attached to.	(VLAN or VPC)
VPC or Subnet (VLAN)	Displays the name of the attached VPC or VLAN subnet.	(Name of VLAN or VPC)
Tunnel IP	Displays the Tunnel IP address of the local gateway.	(IP Address)
Connection Type	Displays the connection type you selected while creating the VPN connection. The connection type may be Initiator or Acceptor of a VPN connection between the local and remote gateways. T	(Initiator or Acceptor)
External Routing	Displays the type of routing associated with the gateway for external traffic routing.	(Static or eBGP with ASN)
Internal Routing	Displays the type of routing associated with the gateway for internal traffic routing.	(Static or eBGP with ASN)
Floating or Private IP Address	Displays the Floating (for VPC) or Private (for VLAN) IP address assigned to the gateway.	(IP Address that you assigned to the local gateway with /30 prefix when you configured the VPN connection.)
Status	Displays the operational status of the gateway.	(Up or Down)
Cluster	Displays the name of the cluster on which the gateway is created.	(Cluster name)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2855

Parameter	Description	Values
Gateway VM	Displays the name of the VM on which the gateway is created.	(Name of VM - actionable link. Click the name-link to open the VM details page of the gateway VM.)
Remote Gateway Properties widget		
Gateway Name	Displays the name of the remote gateway used for the connection.	(Name of remote gateway)
Type	Displays the type of gateway.	(Remote)
Tunnel IP	Displays the Tunnel IP address of the remote gateway.	(IP Address)
Connection Type	Displays the connection type you selected while creating the VPN connection. The connection type may be Initiator or Acceptor of a VPN connection between the local and remote gateways. T	(Initiator or Acceptor)
External Routing	Displays the type of routing associated with the gateway for external traffic routing.	(Static or eBGP with ASN)
ASN	Displays the ASN of the EBGP route. This information is only displayed if you configured EBGP as the External Routing protocol.	(Number)
Vendor	Displays the name of the vendor of the gateway appliance at the remote site.	(Name of vendor of gateway appliance)
External IP	Displays the IP address assigned to remote the gateway.	(IP Address that you assigned to the remote gateway with /30 prefix when you configured the VPN connection.)
Status	Displays the operational status of the gateway.	-
Protocol Details widget		
Service	Displays the service used by the gateway.	(VPN or VTEP)
Gateway Routes widget	Displays the status of the routes used by the gateways.	(Sent)

You can perform the following actions from the **Summary** tab:

- View the detailed information of a VPN connection. For the list of available parameters, see the *VPN Connection Summary Tab* table above.
- Update an existing VPN connection by clicking **Update**. For more information, see Updating VPN Connection in the *Flow Virtual Networking Guide*.
- Delete an existing VPN connection by clicking **Delete**. For more information, see Deleting a VPN Connection in the *Flow Virtual Networking Guide*.

Throughput Tab

The **Throughput** tab provides a graphical representation of the throughput of the VPN connection.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2856

IPSec Logging

The **IPSec Logging** tab provides running logs for the IPSec tunnel of the VPN connection.

Routing Protocol Logging

The **Routing Protocol Logging** tab provides logs for the routing protocol used in the VPN connection.

Subnet Extensions Summary View

The **Subnet Extensions** page displays a list of subnet extensions created for the clusters managed by Prism Central.

To access the **Subnet Extensions** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways.
3. Click the **Subnet Extensions** tab.

   The **Subnet Extensions** page opens displaying the list of subnet extensions created for the clusters.

> **Note:** For information on the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

The following table describes the fields that appear in the **Subnet Extensions** page.

Table 96: Field Description for the Subnet Extensions Page

Parameter	Description	Values
Name	Displays the name of the subnet extension.	(Name of subnet extension)
Type	Displays the subnet extension type.	(**Across Availability Zones** or **To a Third Party Data Center**)
Extension Over	Displays the service that the subnet extension uses.	(VPN or VTEP)
Extension Uses	Displays the name of the local network gateway that the subnet extension uses.	(Name of local network gateway)
Local Subnet	Displays the name of the local subnet that the subnet extension uses.	(Name of local subnet)
Remote Site	Displays the name of the remote network gateway that the subnet extension uses.	(Name of remote network gateway)
Connection Status	Displays the status of the connection that is created by the subnet extension. **Note: Not Available** status indicates that Prism Central is unable to ascertain the status.	(Not Available, Connected, or Disconnected)
Interface Status	Displays the status of the interface that is used by the subnet extension.	(Connected or Down)

You can perform the following actions for a subnet extension from the **Subnet Extensions** page:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2857

- Click the name of a subnet extension to open the subnet extension details page, which displays the detailed information about the extension. For more information, see Subnet Extension Details View on page 387.
- Extend a subnet **Across Availability Zones** or **To a Third Party Data Center** by clicking the **Create Subnet Extension** dropdown menu. You can extend a subnet using **VPN** or **VTEP** service. For more information, see Layer 2 Virtual Network Extension in the *Flow Virtual Networking Guide*.
- Update or delete existing subnet extension using the **Actions** dropdown menu. The **Actions** dropdown appears when one or more subnet extensions are selected. For more information, see Updating an Extended Subnet or Removing an Extended Subnet in the *Flow Virtual Networking Guide*.
- Filter the subnet extension list based on various parameter values using the **Filters** pane. For more information, see Filters Pane - Subnet Extensions Page.

Filters Pane on the Subnet Extensions Page

You can filter the information in the **Subnet Extensions** page based on the following fields that are available in the **Filters** pane. For information on how to use the Filters pane, see the Filters Pane information.

Table 97: Filter Pane Field Descriptions for the Subnet Extensions page

Field	Description	Values
Name	Filters based on the subnet extension name. It returns a list of subnet extensions that satisfy the name condition/string.	(Subnet extension name string)
Connection Status	Filters based on the status of the connection that is created by the subnet extension.	(Connected or Disconnected)
Interface Status	Filters based on the status of the interface that is used by the subnet extension.	(Connected or Not Available)

Subnet Extension Details View

The Subnet Extension details page provides detailed information about a subnet extension.

The details page has the **Summary**, **Address Table**, and **Throughput** tabs.

To access the details page of an individual subnet extension:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways you have created and configured.

   > **Note:** For information on the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

3. Click the **Subnet Extensions** tab.

   The **Subnet Extensions** page opens displaying the list of subnet extensions created for the clusters.
4. Click a subnet extension to open the details page of the extension.

   The **Summary** tab opens displaying the detailed information about the extension in widgets.

Summary Tab

The **Summary** tab provides detailed information about the subnet extension in widgets.

The subnet extension **Summary** tab has the following widgets:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2858

Table 98: Subnet Extension Summary Tab Widgets

Parameter	Description	Values
Properties widget		
Type	Displays the subnet type.	(VLAN or Overlay)
VLAN ID	(For VLAN subnets only) Displays the VLAN ID of the VLAN subnet that is extended.	(VLAN ID number)
VPC	(For Overlay subnets only) Displays the name of the VPC subnet that is extended.	(Name of VPC)
Cluster	(For VLAN subnets only) Displays the cluster that the VLAN subnet belongs to.	(Name of cluster)
IP Address Prefix	Displays the network IP address with prefix, of the VLAN subnet that is extended.	(IP Address with prefix)
Virtual Switch	(For VLAN subnets only) Displays the virtual switch on which the VLAN subnet is configured.	(Virtual Switch name such as vs0 or vs1)
IP Address Pools widget		
Pool Range	Displays the range of IP addresses in the pool configured in the subnet that is extended.	(IP address range)
(Interactive Graphic Pie Chart)	Displays a dynamic pie chart that displays the statistic you hover on. Displays the following IP address statistics outside the pie chart, that you can hover on: • Total number of IP addresses available. • Used IP addresses in the subnets • Used IP addresses in the IP address pools • Free IP addresses in the subnets • Free IP addresses in the IP address pools	(IP Address statistics)
Subnet Extension widget		
Subnet Extension (properties) - Common		
Type	Displays the subnet extension type.	(**Across Availability Zones** or **To a Third Party Data Center**)
Interface Status	Displays the status of the interface that is used by the subnet extension.	(Connected or Down)
Connection Status	Displays the status of the connection that is created by the subnet extension. **Not Available** status indicates that Prism Central is unable to ascertain the status.	(Not Available, Connected, or Disconnected)
Local IP Address	Displays the IP address that you entered in the **Local IP Address** field while creating the subnet extension.	(IP Address)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2859

Parameter	Description	Values
Local Subnet	Displays the name of the local subnet that the subnet extension uses.	(Name of local subnet)
Subnet Extension (properties) - (Only for **Across Availability Zones** type)		
Local Availability Zone	(Only for **Across Availability Zones** type) Displays the name of the local AZ that is hosting the subnet that is extended.	(Name of the local Availability Zone)
Remote Availability Zone	(Only for **Across Availability Zones** type) Displays the name of the remote AZ that the subnet is extended to.	(Name of the remote Availability Zone)
Remote Subnet	(Only for **Across Availability Zones** type) Displays the name of the remote subnet that the subnet extension connects to.	(Name of remote subnet)
Remote IP Address	(Only for **Across Availability Zones** type) Displays the IP address that you entered in the **Remote IP Address** field while creating the subnet extension.	(IP Address)
Subnet Extension (properties) - (Only for **To a Third Party Data Center** type)		
Local Gateway	(Only for **To a Third Party Data Center** type) Displays the name of the local gateway used for the subnet extension.	(Name of local gateway)
Remote Gateway	(Only for **To a Third Party Data Center** type) Displays the name of the remote gateway used for the subnet extension.	(Name of remote gateway)

You can perform the following actions from the **Summary** tab:

- View the detailed information of a subnet extension. For the list of available parameters, see the *Subnet Extension Details - Summary Tab Fields* table above.
- Update an existing subnet extension by clicking **Update**. For more information, see Updating an Extended Subnet in the *Flow Virtual Networking Guide*.
- Delete an existing subnet extension by clicking **Delete**. For more information, see Removing an Extended Subnet in the *Flow Virtual Networking Guide*.

Address Table Tab

The **Address Table** tab provides MAC Address information only when the subnet extension uses VTEP service. The tab provides the following information:

- **MAC Address**: This provides the MAC addresses of devices connected to the remote VTEP endpoint in the subnet extension.
- **Remote VTEP Endpoint**: This provides the IP address of the remote VTEP endpoint in the subnet extension.

Throughput Tab

The **Throughput** tab provides a graphical representation of the throughput of the subnet extension.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2860

BGP Sessions Summary View

The **BGP Sessions** page displays a list of BGP sessions created for the clusters managed by Prism Central.

To access the **BGP Sessions** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways.

   > **Note:** For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

3. Click the **BGP Sessions** tab.

   The **BGP Sessions** page opens displaying the list of BGP sessions created for the clusters.

The following table describes the fields that appear in the **BGP Sessions** page.

Table 99: BGP Sessions – Field Description

Parameter	Description	Values
Name	Displays the name of the BGP session.	(Name of BGP session)
Serviced VPC	Displays the name of the VPC that the BGP session services.	(Name of VPC)
Local Gateway	Displays the name of the local BGP gateway that the BGP session uses.	(Name of local BGP gateway)
Remote Gateway	Displays the name of the remote BGP gateway that the BGP session uses.	(Name of remote BGP gateway)
Session Status	Displays the status of the eBGP session. • Displays **Established** if the session is **Up**. • Displays **Active** when the network controller is attempting to establish the session.	**Established** or **Active**

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2861

Parameter	Description	Values
Route Priority	Displays an integer number that denotes the route priority. When the route priority is assigned dynamically, then the network controller assigns integer numbers (usually between 600 and 800 starting with 700) in descending order with steps of 5. For example, the first session is assigned 700 as route priority and then when you create the second session, the controller assigns it a route priority of 695 and a third session is assigned 690. Greater the number, greater is the route priority. With dynamically assigned priority, the priority is assigned in the order of reducing priority to the order of BGP sessions created. The BGP session created first gets the highest priority 700, the second session get the second highest priority 695 and so on. You can manually assign a route priority as well by assigning any number between 300 and 900.	(Integer Number)

You can perform the following actions for a gateway from the **BGP Sessions** page:

- Click the name of a BGP session to open the details page, which displays the detailed information about the BGP session. For more information, see BGP Session Details View on page 391.
- Create a BGP session by clicking **Create BGP Session**. For more information, see Creating a BGP session in the *Flow Virtual Networking Guide*.
- Update or delete an existing BGP session using the **Actions** dropdown menu. The **Actions** dropdown menu appears when one or more BGP sessions are selected. For more information, see Updating a BGP session or Deleting a BGP session in the *Flow Virtual Networking Guide*.
- Filter the gateway list based on various parameter values using the **Filters** pane. For more information, see Filters Pane - BGP Sessions Page.

Filters Pane on the BGP Sessions Page

You can filter the information in the **BGP Sessions** page based on the following fields that are available in the **Filters** pane. For information on how to use the Filters pane, see the Filters Pane information.

Table 100: Filter Pane Field Description - BGP Sessions page

Field	Description	Values
Name	Filters based on the BGP session name. It returns a list of BGP sessions that satisfy the name condition/ string.	(BGP session name string)
Session Status	Filters based on the status of the eBGP session.	(Established or Down)

BGP Session Details View

The BGP Session details page provides detailed information about a BGP session.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2862

The details page has the **Summary**, **Routes**, and **BGP Logs** tabs.

To access the details page of an individual BGP session:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways you have created and configured.

   > **Note:** For information on the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

3. Click the **BGP Sessions** tab.

   The **BGP Sessions** page opens displaying the list of BGP sessions created for the clusters.
4. Click the name of a BGP session to open the details page of the session.

   The **Summary** tab opens displaying the detailed information about the BGP session in widgets.

Summary Tab

The **Summary** tab provides detailed information about the BGP session in widgets.

The BGP session **Summary** tab has the following widgets:

Table 101: BGP Session Summary Tab Widgets

Parameter	Description	Values
Properties widget		
Session Status	Displays the overall status of the BGP session.	(Up or Down)
eBGP Status	Displays the eBGP status of the BGP session.	**Established** or **Active**
Route Priority	Displays an integer number that denotes the route priority. For more information about Route Priority, see BGP Sessions Summary View on page 390.	(Integer Number)
Local Gateway widget		
Local Gateway	Displays the name of the local BGP gateway.	(Name)
eBGP ASN	Displays the Autonomous System Number (ASN) of the local BGP gateway used by the session. It would be an integer number in the 1-65534 range (per 32-bit ASN.1 standard). **Note:** Make sure that this ASN does not conflict with any of the other on-premises BGP ASNs.	(Number)
Remote Gateway widget		
Remote Gateway	Displays the name of the remote BGP gateway.	(Name)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2863

Parameter	Description	Values
eBGP ASN	Displays the ASN of the remote BGP gateway used by the session. It would be an integer number in the 1-65534 range (per 32-bit ASN.1 standard). **Note:** Make sure that this ASN does not conflict with any of the other on-premises BGP ASNs.	(Number)

You can perform the following actions from the **Summary** tab:

- View the detailed information of a BGP session. For the list of available parameters, see the *BGP Session Details - Summary Tab Fields* table above.
- Update an existing BGP session by clicking **Update**. For more information, see Updating a BGP session in the *Flow Virtual Networking Guide*.
- Delete an existing BGP session by clicking **Delete**. For more information, see Deleting a BGP session in the *Flow Virtual Networking Guide*.

Routes Tab

The **Routes** tab provides a list of the routes used by the BGP session with the corresponding **Next Hop** details. It has the following lists:

- **Advertised** (default): The **Routes** tab opens in the **Advertised** list. The **Advertised** list provides a list of the advertised routes with the corresponding **Next Hop** details.
- **Received**: This list provides list of the routes received from remote with the corresponding **Next Hop** details.

BGP Logs Tab

The **BGP Logs** tab provides detailed live logs for the BGP session. This information can be very useful in monitoring and debugging a BGP session.

Figure 156: BGP Session Details View - BGP Logs tab sample for a BGP session

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2864

Security Policies

Security policies are defined using Nutanix Flow that provides a policy-driven security framework to inspect traffic within the data center.

For information on how to create and apply security policies, see Flow Microsegmentation Guide.

For information on how to view security policies in Prism Central, see Security Policies Summary View on page 501 or Security Policy Details View on page 505.

Security Dashboard

The Security Dashboard provides dynamic summary of the security posture across all registered clusters. The Security Dashboard allows you to view the most critical security parameters like cluster-based issue summary, STIG policy compliance, security hardening, and identified vulnerabilities. For more information, see Security Dashboard in the *Nutanix Security Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2865

DATA PROTECTION AND RECOVERY ENTITIES

You can access dashboards for the following data protection types from the **Data Protection** entity of the **Infrastructure** application. For information about how to access the entity items available in **Data Protection** entity, see Application-specific Navigation Bar on page 66.

- Protection Summary on page 395
- Protection Policies on page 395
- Recovery Plans on page 395
- VM Recovery Points on page 395
- VG Recovery Points on page 395
- Consistency Groups on page 395

Protection Summary

Protection Summary provides a detailed information about the Nutanix Disaster Recovery entities in an AZ, and helps you to generate DR reports for the specified time. It also enables you to monitor the health of your DR deployments and the activities performed on the Nutanix Disaster Recovery entities. For more information about **Protection Summary**, see Nutanix Disaster Recovery Guide.

Protection Policies

A Protection policies is a configurable policy that takes recovery points of the protected entities (guest VMs, volume groups, and consistency groups) in equal time intervals, and replicates those recovery points to the recovery AZs. For more information about protection policies, see Nutanix Disaster Recovery Guide.

Recovery Plans

The Recovery plans are used in automated Disaster Recovery (DR) configurations to orchestrate the recovery of the protected entities to different Nutanix clusters at the same or different AZs. For more information about recovery plans, see Recovery Plans View information in *Nutanix Disaster Recovery Guide*.

VM Recovery Points

The protection policy associated with the VM creates the VM recovery points. For more information about VM recovery points, see Nutanix Disaster Recovery Guide.

VG Recovery Points

VG Recovery Points lists the recovery points of all the protected volume groups (generated over time) on the local cluster. For more information about VG recovery points, see Nutanix Disaster Recovery Guide.

Consistency Groups

A consistency group is a collection of the entities that are treated as a single group and backed up collectively in a recovery point. For information about Consistency Groups, see Consistency Groups information in *Nutanix Disaster Recovery Guide* .

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2866

HARDWARE ENTITIES

You can access dashboards for the following hardware components from the **Hardware** entity of the **Infrastructure** application. For information about how to access the entity items available in **Hardware** entity, see Application-specific Navigation Bar on page 66.

- Clusters (see Clusters Summary View on page 398)
- Hosts (see Hosts Summary View on page 419)
- Disks (see Disks Summary View on page 438)
- GPUs (see GPUs Summary View on page 444)

Cluster Management

In Prism Central, the clusters dashboard allows you to view summary information about all the registered clusters and access the detailed information about each cluster. For more information, see Clusters Summary View on page 398 and Cluster Details View on page 405.

The **Actions** menu appears when a cluster is selected. The following table provides the information about all the actions that you can perform to manage the clusters:

> **Note:** The available actions appear in bold; other actions are disabled. For disabled options, you can see a tool tip explaining the reason. The available actions depend on the current state of the selected clusters.

Table 102: Cluster Actions

Action	Description	Applicable to Multiple Clusters
Launch Prism Element	Launch Prism element for that cluster in a separate tab or window (depending on your browser settings). **Note:** When you access a cluster from Prism Central, you log in through your Prism Central user account, not a cluster user account. As a result, the cluster user configuration options are different (more limited) than when logging directly into the cluster. The options that appear in the Prism Element main menu user dropdown list are **REST API Explorer**, **About Nutanix**, **Support Portal**, **Help**, **Nutanix Next Community**, and **Sign Out**.	No
Upgrade Software	Upgrade the AOS version on the cluster. For more information, see Prism Central Deployment on page 12.	Yes
Rack Configuration	Configure the rack awareness feature. This option appears only for clusters that satisfy the conditions for rack awareness. For instructions on configuring rack awareness, see Rack Fault Tolerance in the *Prism Element Web Console Guide*.	No
Manage Categories	Configure and manage cluster categories.	No

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2867

Action	Description	Applicable to Multiple Clusters
Enable Efficiency Measurement	Enable efficiency measurement for the cluster.	Yes
Disable Efficiency Measurement	Disable efficiency measurement for the cluster.	Yes
Enable Anomaly Detection	Enable Anomaly Detection for the cluster.	Yes
Disable Anomaly Detection	Disable Anomaly Detection for the cluster.	Yes
Run Playbook	Run or create a new playbook for the cluster entity type.	Yes
Manage & Backup Keys	Download the encryption keys for the cluster. If the cluster goes down, you can access your data with the backup key.	No
Enable Data-at-Rest Encryption	Enable Data-at-Rest Encryption for the cluster.	Yes
Manage KMS Types	Manage the Key Management Solution (KMS) for the cluster.	No
Enable Data-in-transit Encryption	Enable Data-in-transit Encryption for the cluster.	Yes
Disable Data-in-transit Encryption	Disable Data-in-transit Encryption for the cluster.	Yes
Manage Rebuild Capacity	Manage Rebuild Capacity for a cluster having a minimum of three nodes. For more information about rebuild capacity, see Rebuild Capacity Reservation in Prism Element Web Console Guide.	No
Manage Recycle Bin	Manage Recycle Bin for the cluster. You can choose to retain the deleted VMs and volume groups for a specific retention time (1 to 7 days). This feature is supported for clusters running AOS 6.6.1 and later.	No
Manage Cluster Fault Tolerance	Modify the fault tolerance of the cluster based on your cluster configuration. For more information, see Managing Cluster Fault Tolerance on page 412. Cluster fault tolerance determines the readiness of the cluster to recover from an unexpected hardware failure. For more information, see Cluster Fault Tolerance in the *Prism Element Web Console Guide*.	No
Maintenance Resiliency	Modify the rebuild preference setting of the cluster. By default, the cluster rebuild preference is set as *Smart*. To modify the cluster rebuild preference to *Immediate*, clear the *Smart* checkbox. For more information on cluster rebuild preference, see Cluster Rebuild Preference in the *Prism Element Web Console Guide*.	No
Expand Cluster	Expand a cluster. For information on expanding a cluster, see Expanding a Cluster through Prism Central on page 428.	No

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2868

Action	Description	Applicable to Multiple Clusters
Destroy Cluster	Destroy a cluster. For information on destroying a cluster, see Destroying a Cluster on page 411.	Yes

Clusters Summary View

The **Summary** tab on the **Clusters** page provides a dashboard of all the registered clusters.

To access the summary view of all the clusters, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and go to **Hardware** > **Clusters** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The system displays the **List** tab by default with all the registered clusters in **Nutanix** environment.
3. Click the **Summary** tab. The system displays **Summary** page for all the clusters.

> **Note:** To access the summary view of all the non-nutanix clusters managed by *vCenter*, select **Non-Nutanix** from the dropdown menu in **Clusters** page.
>
> The **Summary**, **Alerts**, and **Events** tabs display the same information as for Nutanix-managed clusters. The **Metrics** tab displays CPU usage, memory usage, and VM operations. The **List** tab displays fields for name, host count, VM count, storage usage, and storage capacity. The **Profiles** tab allows you to view all the settings profiles created for the clusters.

Using playbooks, you can manage the clusters in **Non-Nutanix** environment. For more information about playbooks, see Task Automation - Playbooks in *Intelligent Operations Guide*.

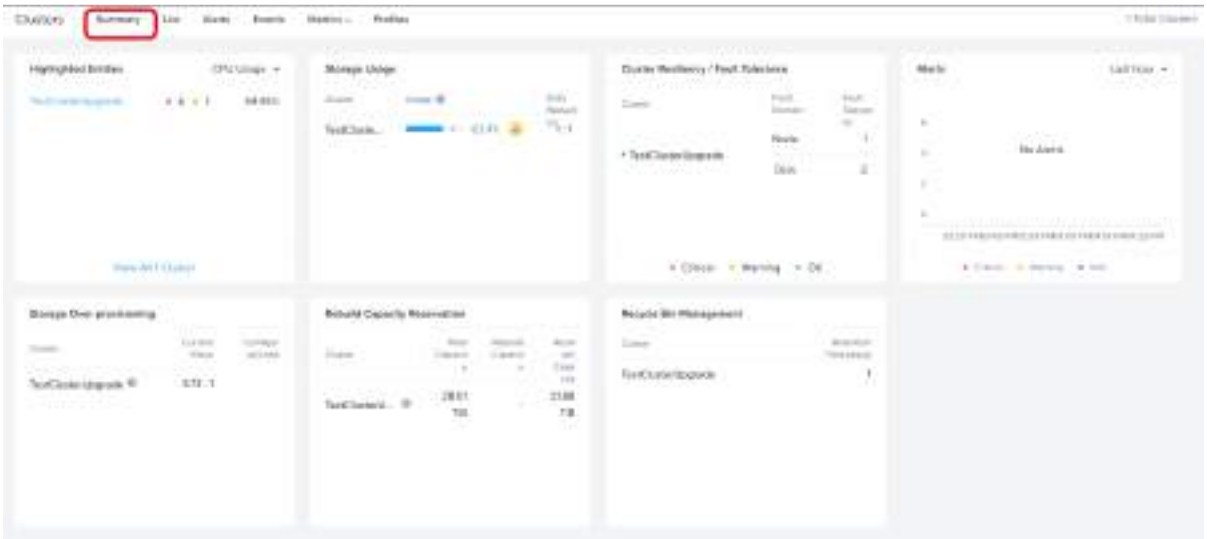


Figure 157: Summary Page - All Clusters

The **Summary** page for all clusters displays information about all the registered clusters and allows you to access detailed information about each cluster.

The **Clusters** page includes the following tabs on the left: **Summary**, **List**, **Alerts**, **Events**, **Metrics**, and **Profiles** with a display area below the selected tab.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2869

> **Note:** This section describes the information and options that appear in the **Summary** page for all clusters. For instructions on how to view and organize that information in various ways, see Prism Central GUI Organization on page 54.

The **Summary** tab for all the clusters displays the following widgets:

- **Highlighted Entities**: Displays a list of clusters with the highest usage of the parameter you select from the dropdown menu on the right of the widget. The options are **CPU Usage**, **IO Latency**, **IOPS**, and **Memory Usage**. Click the **View all XX Clusters** link at the bottom to display the **List** tab (following section).
- **Storage Usage**: Displays a list of clusters along with the percentage usage (with respect to total usable capacity of the cluster) and data reduction. Total usage is calculated as the sum of used capacity and free reserved capacity. Data reduction ratio displays the ratio of how much the data size is reduced by enabling compression, deduplication, and erasure coding. Placing the cursor anywhere on the horizontal axis displays a breakdown view of the storage capacity usage.
- **Cluster Resiliency / Fault Tolerance**: Displays a list of clusters along with the fault domain and the current state of the fault tolerance. Fault tolerance of a cluster can have any one of the following states:
  - **OK**: This state indicates that the fault tolerance domain is highly resilient to safely handle a node or a disk (in single or two node clusters) failure.
  - **Warning**: This state indicates that the fault tolerance level is almost reaching to 0. Warning state is displayed if the cluster is not fault tolerant at the configured domain, but is fault tolerant at a lower domain. For example, if you have configured rack as the configured domain and the cluster can no longer handle any rack failures due to some reason but can still handle node (lower domain) failures, then fault tolerance state is displayed as Warning.
  - **Critical**: This state indicates that the fault tolerance level is 0, and the fault tolerance domain cannot handle a node or a disk (in single or two node clusters) failure.
  - **Computing**: This state indicates that the new fault tolerance level is being calculated. This state is displayed soon after a node or disk failure, before rebuild is initiated.
- **Alerts**: Displays a list of cluster-related alerts that occurred during the specified interval. Select either **Last 24 hours** (default), **Last 1 Hours**, or **Last week** from the dropdown menu. When an alert appears, you can click on the graph, which then displays a list of those alerts. Clicking on an alert displays the details page for that alert.
- **Storage Over-provisioning**: Displays a list of the clusters along with the storage over-provisioning ratio (calculated based on the provisioned storage and the available raw storage). The current value and state of storage over-provisioning ratio is displayed according to the configured limits.
- **Rebuild Capacity Reservation**: Displays a list of clusters with their total capacity, rebuild capacity, and resilient capacity. For more information about rebuild capacity, see Rebuild Capacity Reservation section in Prism Element Web Console Guide.
- **Recycle Bin Management**: Displays a list of clusters with their retention time in days. For more information on Recycle Bin, see Recycle Bin in the *Prism Element Web Console Guide*.
- **Anomalies**: Displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified interval. Select either **Last 24 hours** (default), **Last 1 Hours**, or **Last week** from the dropdown menu. When an anomaly appears, you can click on the graph, which then displays a list of those anomalies. Clicking on an anomaly displays the event page for that anomaly.

Lists Tab

The **List** tab displays the list of clusters.

To access the **Lists** tab:

1. Log in to Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2870

2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Hardware** > **Clusters** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The system displays the **List** tab by default with clusters.

   > **Note:** You can use the **View by** and **Group by** options to create your own customized view and add the necessary columns to that view. For more information on how to **View by** and **Group by** options, see Prism Central GUI Organization on page 54.

The following table describes the fields that appear in the clusters **List** tab.

> **Note:** The fields vary based on the **View by** and **Group by** options. A dash (-) is displayed in a field when a value is not available or applicable. For more information about **View by** and **Group by** options, see Prism Central GUI Organization on page 54.

Table 103: Clusters List Fields

Parameter	Description	Values
View by **General** Fields		
Name	Displays the cluster name. Clicking on the name displays the details page for that cluster. For more information, see Cluster Details View on page 405.	(cluster name)
AOS Version	Displays the version number of AOS running on the cluster.	(version number)
Upgrade Status	Displays the current upgrade status. There are various stages from scheduled to succeeded (or failed).	Pending, Downloading, Queued, PreUpgrade, Upgrading, Succeeded, Failed, Cancelled, Scheduled
Hypervisors	Displays the hypervisor type running in the cluster. In the case of a mixed cluster such as one running ESXi or Hyper-V that also includes NX-6035C nodes running AHV, both hypervisor types are listed.	AHV, ESX, Hyper-V
Host Count	Displays the number of hosts (nodes) in the cluster.	(number of nodes)
VM Count	Displays the total number of VMs in the cluster (in any state).	(number of VMs)
Cluster Runway	Displays the predicted runway (time period) before the cluster requires additional resources. For more information, see the *Capacity Tab* section in Cluster Details View on page 405.	(number of days)
Inefficient VMs	Displays the number of inefficient VMs in the cluster. For more information, see Behavioral Learning Tools in *Intelligent Operations Guide*.	(number)
View by **Performance** Fields		

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2871

Parameter	Description	Values
Name	Displays the cluster name.	(cluster name)
CPU Usage	Displays the percentage of CPU capacity in the cluster currently being used.	0 -100%
Memory Usage	Displays the percentage of memory capacity in the cluster currently being used.	0 -100%
IOPS	Displays total (both read and write) I/O operations per second (IOPS) for this cluster.	(number)
IO Bandwidth	Displays total I/O bandwidth used per second in this cluster.	xxx [MBps|KBps]
IO Latency	Displays the average I/O latency in this cluster.	xxx [ms]
View by **Capacity** Fields		
Name	Displays the cluster name.	(cluster name)
Cluster Runway	Displays the predicted runway (time period) before the cluster requires additional resources. For more information, see the *Capacity Tab* section in Cluster Details View on page 405.	(number of days)
CPU Runway	Displays the predicted CPU runway (time period) before the cluster requires additional resources.	(number of days)
Memory Runway	Displays the predicted memory runway (time period) before the cluster requires additional resources.	(number of days)
Storage Runway	Displays the predicted storage memory runway (time period) before the cluster requires additional resources.	(number of days)
View by **Encryption** Fields		
Name	Displays the cluster name.	(cluster name)
Data-at-Rest Encryption	Displays the cluster encryption type.	Not Encrypted, Software, Hardware, Software and Hardware
KMS Type	Displays the key management system (KMS) type.	Not Set, Native (Local), Native (Remote), External
Data-in-Transit Encryption	Displays the cluster encryption type.	Not Encrypted, Software, Hardware, Software and Hardware
Host Count	Displays the number of hosts (nodes) in the cluster.	(number of nodes)

You can perform the following actions for the clusters in the **Lists** tab:

- Create a cluster. For information about how to create a cluster, see Creating a Cluster on page 409.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2872

- Access the detailed information about an individual cluster. For more information, see Cluster Details View on page 405.
- Filter the clusters list based on available parameter values using **Filters** pane. For more information about **Filters** pane, see the following section *Filters Pane - Clusters Page*.
- Export the table that contains the list of clusters and their information to a file in a CSV format. For more information about **Export** option, see Export on page 59.
- Group the clusters based on pre-defined criteria. For information about how to group the clusters, see Group by on page 56.
- View clusters based on pre-defined criteria or create a custom view. For information about available views and how to create a custom view, see View by on page 56.
- Assign a label to the filtered criteria. For information about how to define a label, see Label on page 59.
- Perform the cluster-specific actions on a single or multiple clusters using the **Actions** dropdown menu. For more information, see Cluster Management on page 396.

Filters Pane - Clusters Page

The following table describes the fields available in the **Filters** pane:

Table 104: Filters Pane

Parameter	Description	Values
Labels	Filters on label name. Select one or more labels from the dropdown list. (If there are no labels currently, a message about how to create labels is displayed.)	(label names)
Name	Filters on the cluster name. Select a condition from the dropdown list (**Contains**, **Doesn't contain**, **Starts with**, **Ends with**, or **Equal to**) and enter a string in the field. It will return a list of clusters that satisfy the name condition/string.	(cluster name string)
AOS Version	Filters on AOS version. Select one or more versions to return a list of clusters running those version(s). The number of clusters currently running each version is displayed on the right of the line.	(Acropolis version numbers across clusters currently)
Hypervisors	Filters on the hypervisor type. Select one or more hypervisors to return a list of clusters running those hypervisor(s). The number of clusters currently running each hypervisor is displayed on the right of the line.	AHV, ESXi, Hyper-V, XenServer
Health	Filters on the cluster health state (good, warning, or critical). Select one or more states to return a list of clusters in that state(s). The number of clusters currently in each state is displayed on the right of the line.	Critical, Warning, Good

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2873

Parameter	Description	Values
CPU Usage	Filters on the amount of total CPU being used. Check the box for the desired range or enter a percentage range in the **from <low> to <high> %** field. It will return a list of clusters utilizing total CPU in that range (0-100%).	([xx] to [yy]% range)
Memory Usage	Filters on the amount of total memory being used. Check the box for the desired range or enter a percentage range in the **from <low> to <high> %** field. It will return a list of clusters utilizing total memory in that range (0-100%).	([xx] to [yy]% range)
IOPS	Filters on the total (both read and write) IOPS. Check the box for the desired range or enter a range in the **from <low> to <high> iops** field. It will return a list of clusters with total IOPS in that range.	([xx] to [yy] range)
IO Bandwidth	Filters on the total I/O bandwidth used. Check the box for the desired range or enter a range in the **from <low> to <high> bps** field. It will return a list of clusters with total I/O bandwidth usage in that range.	([xx] to [yy] range)
IO Latency	Filters on the average I/O latency. Check the box for the desired range or enter a range in the **from <low> to <high> ms** field. It will return a list of clusters with average I/O latency in that range.	([xx] to [yy] range)
Upgrade Status	Filters on the current upgrade status. There are various stages from scheduled to succeeded (or failed).	Pending, Downloading, Queued, PreUpgrade, Upgrading, Succeeded, Failed, Cancelled, Scheduled
Categories	Filters on the category type. Search for the category name. For example, ADGroup:$Default	(category name string)
Data-at-rest Encryption Type	Filters on the encryption type. Check the box for the desired encryption type. It will return a list of clusters with the corresponding encryption type applied.	Not Encrypted, Software, Hardware, Dual
Data-at-rest Encryption Scope	Filters on the encryption scope. Check the box for the entities where encryption is applied on. It will return a list of clusters with the corresponding encryption scope applied.	Cluster, Entity
KMS Type	Filters on the key management system (KMS) type.	Not Set, Native (Local), Native (Remote), External
Data-in-Transit Encryption	Filters on the encryption type. Check the box for the desired encryption type. It will return a list of clusters with the corresponding encryption type applied.	Not Enabled, Enabled

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2874

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options that are available on the **Activity** > **Alerts** page, however it only displays the cluster-related alerts. For more information about alerts, see *Prism Central Alerts and Events Reference Guide*.

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options that are available on the **Activity** > **Events** page, however it only displays the cluster-related events. For more information about events, see *Prism Central Alerts and Events Reference Guide*.

Metrics Tab

The **Metrics** tab allows you to view usage metrics across the clusters. Click the **Metrics** tab to display dropdown menu of available metrics, and select the metric name to display the relevant performance information.

> **Note:** The **Metrics** dropdown menu is hypervisor-specific, and might vary based on the hypervisors used in the cluster.

Table 105: Metrics Tab Fields

Metric	Description
CPU Usage	Displays a CPU usage table listing current values and total clusters (number). The current values are split into percentile intervals (for example, less than 25%, 25-50, 50-75, more than 75%). Clicking on a percentile interval displays the Summary tab filtered to just those clusters. **Note:** The same format also applies to the other metrics in this table with either percentile or quantity intervals.
Memory Usage	Displays a memory percentage usage table.
IOPS	Displays total, read, and write IOPS tables.
IO Latency	Displays total, read, and write I/O latency rate tables.
IO Bandwidth	Displays total, read, and write I/O bandwidth rate tables.

Profiles Tab

The **Profiles** tab allows you to view all the settings profiles created for the clusters. Click the **Profiles** tab to display the list of available profiles, and select a profile to display the relevant information about clusters, their compliance status, and Settings.

You can perform the following actions from the **Profiles** tab:

- Create a Settings Profile
- Updating a Settings Profile
- Deleting a Settings Profile
- Assigning clusters to a Setting Profile
- Disassociating Clusters from a Settings Profile

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2875

Cluster Details View

Summary Tab

The **Summary** tab of an individual cluster consists of a dashboard that provides the detailed information about the cluster.

To access the **Summary** tab of an individual cluster:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and go to **Hardware** > **Clusters** from the **Navigation Bar**.

   For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66. The system displays the **List** tab by default with all the registered clusters in **Nutanix** environment. For information about how to access the list of clusters in **Non-Nutanix** environment (non-nutanix clusters managed by external *vCenter*), see Clusters Summary View on page 398.
3. Click the target <*cluster_name*> to view the **Summary** tab of an individual cluster.

   > **Note:** Replace <*cluster_name*> with the actual cluster name at your site.

The **Summary** tab of an individual cluster provides the following widgets:

- **Properties** - Displays summary information about the cluster. For information about the fields available in **Properties** widget, see Cluster Properties Widget on page 407.
- **Metrics** - Displays the cluster metrics such as CPU usage, Memory usage, IOPS, IO latency, and IO bandwidth.
- **Alert** - Displays a list of related alerts that occurred during the specified interval. Select either **Last week** (default),**Last 1 hour**, or **Last 24 hours** from the dropdown menu on the top right corner of the widget.
- **Anomalies** - Displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified interval. Select either **Last week** (default), **Last 1 hour**, or **Last 24 hours** from the dropdown menu on the top right corner of the widget. When an anomaly appears, you can click the graph to display a list of those anomalies. If you click an individual anomaly, the system displays the event page for that anomaly.
- **VM Efficiency** - Displays the number of VMs that are considered inefficient, broken down by category (over-provisioned, inactive, constrained, and bully). For more information, see Behavioral Learning Tools in *Intelligent Operations Guide*.
- **Tier-wise Usage**: Displays a pie chart divided into the percentage of storage space used by each disk tier in the cluster. Disk tiers can include SSD, HDD, and SSD-NVMe depending on the hardware model type.
- **Storage Over-provisioning** - Displays the storage over-provisioning ratio (calculated based on the provisioned storage and the available raw storage) in the cluster. You can configure a ratio limit to alert the administrator when the ratio changes excessively. If the ratio reaches 70% of the configured limit, the widget displays a warning alert in yellow color. The widget displays Critical alert in red color if the ratio exceeds 90%. Note that the time taken for the Storage Over-provisioning Ratio widget to reflect the changes made in the cluster varies according to the recent storage operations or activities performed.
- **Cluster Resiliency / Fault Tolerance Status** - Displays the current fault tolerance of the cluster. The information includes the type of cluster fault tolerance configured in the cluster, current failure domain (rack, block, disk, or node) and the level of fault tolerance (1 or 2). The widget indicates if any of the current fault domain changes from their configured state. If a data rebuild is triggered after a component failure, the widget also displays a rebuild progress indicator that enables you to track the estimated time until full resiliency has been restored to the cluster. For more information on the types of cluster fault tolerance see, Cluster Fault Tolerance in the *Prism Element Web Console Guide*.
- **Storage Summary** - Displays information about the physical storage space utilization (in GiB or TiB) and resilient capacity of the cluster. Placing the cursor anywhere on the horizontal axis displays a breakdown view

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2876

of the storage capacity usage. You can also configure a threshold warning for the resilient capacity utilization in the cluster by clicking the gear icon at the top right corner. For more information, see Configuring a Warning Threshold for Resilient Capacity.

The View Details link displays the resiliency status and storage information of all the individual nodes in the cluster.

The Storage Details page is divided into two sections: The right section displays a diagrammatic representation of the number of nodes present in the cluster along with the respective storage capacity used. You can view the warning threshold and resilient capacity of each of the nodes. The left section provides detailed storage information of the cluster as follows.

Table 106: Storage Information

Parameter	Description	Values
Failure Domain	Displays the entity (node, block, or rack) whose failure the cluster can tolerate while still running the guest VMs and responding to commands through the management console.	node, block, or rack
Total Capacity	Displays the total capacity of all the disks on all the hosts in the cluster.	xxx [GB|TB]
Resilient Capacity	Displays the total resilient capacity of the cluster. Resilient capacity is the storage capacity available in the cluster after accounting for the storage space needed to rebuild and restore in case of any component failure.	xxx [GB|TB]
Total Usage	Displays the sum of all the storage space used by the cluster. The total used capacity is calculated based on the following: • Used Capacity: The amount of used storage space in the cluster (by user data). • Snapshots: The total storage capacity in the cluster consumed by snapshots (sum of both local and remote. • Recycle Bin: The total storage capacity in the cluster consumed by the VMs deleted by the user. • Other: The total storage capacity occupied by VMs, VG disks, and images. • Free Reserved Capacity:The total capacity that can be used by selected storage containers.	xxx [GB|TB]
Available Capacity	Displays the available storage capacity on all the disks on all the hosts in the cluster.	xxx [GB|TB]

In addition to the above-mentioned widgets, some actions (only the applicable ones appear) also appear on the **Summary** tab. You can perform the cluster-specific actions on a single or multiple clusters using these actions. The first four actions are: **Launch Prism Element**, **Upgrade Software**, **Rack Configuration**, and **Manage Categories**. The rest of the actions appear in the **More** dropdown menu. For more information, see Cluster Management on page 396.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2877

Cluster Properties Widget

The following table describes the fields in the **Properties** widget. A dash (-) in a field indicates that there is not enough data to evaluate or a value is not assigned. The displayed fields vary by hypervisor.

Table 107: Cluster Properties Fields

Parameter	Description	Values
Health	Displays the cluster health state (good, warning, or critical).	Critical, Warning, Good
Storage Usage	Displays the amount of storage used in the cluster	xxx [GiB|TiB]
Storage Capacity	Displays the total amount of storage capacity in this cluster.	xxx [GiB|TiB]
Cluster Runway	Displays the predicted runway (time period) before the cluster requires additional resources (see the Capacity Tab section below).	(number of days)
VM Count	Displays the number of VMs in the cluster.	(number of VMs)
AOS Version	Displays the version number of AOS running on the cluster.	(version number)
Host Count	Displays the number of hosts (nodes) in the cluster.	(number of hosts)
Upgrade Status	Displays the status of the last (or current) upgrade attempt.	(status condition)
IP Address	Displays the virtual IP address for the cluster (if defined).	(IP address)
Hypervisors	Displays the hypervisor type running in the cluster. In case of a mixed cluster such as one running ESXi or Hyper-V that also includes NX-6035C nodes running AHV, both hypervisor types are listed.	AHV, ESX, or Hyper-V

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options as the Alerts dashboard, except it is filtered to display just alerts for this cluster. For more information, see Alerts Summary View (Prism Central) in *Prism Central Alerts and Events Reference Guide*.

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options as the Events dashboard, except it is filtered to display just events for this cluster. For more information, see Events Summary View (Prism Central) in *Prism Central Alerts and Events Reference Guide*.

Metrics Tab

The **Metrics** tab allows you to view usage metrics for the cluster. Click the **Metrics** tab and then the desired metric name (see following table) to display a graph for that metric below the tab. The graph is a rolling time interval performance or usage monitor. The baseline range appears as a blue band in the graph.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2878

Note: The baseline range and identified anomalies are based on sophisticated machine-learning capabilities. For more information, see Behavioral Learning Tools in the *Intelligent Operations Guide*. The machine-learning algorithm uses 21 days of data to monitor and predict performance. A graph or baseline band may not appear if less than 21 days of data is available.

- Place the cursor anywhere on the horizontal axis to display the value at that time.
- Select the duration (time interval) from the dropdown list on the right (last 1 hour, last 24 hours, last week, last 21 days).
- [I/O-based metrics] Check the appropriate box(es) to have the graph display total, read, or write usage (or any combination of the three).
- Click **Alert Settings** to configure an alert for this metric. For more information, see Creating Custom Alert Policies in *Prism Central Alerts and Events Reference Guide*.

The following table describes the available metrics. Some metrics are not available on all hypervisors.

Table 108: Metrics Tab Fields

Metric	Description
CPU Usage	Displays the percentage of CPU capacity currently being used by the cluster (0–100%).
Memory Usage	Displays the percentage of memory capacity currently being used by the cluster (0–100%).
IOPS	Displays separate graphs for total, write, and read I/O operations per second (IOPS) for the cluster.
I/O Latency	Displays separate graphs for total, write, and read average I/O latency (in milliseconds) for physical disk requests by the cluster.
I/O Bandwidth	Displays separate graphs for total, write, and read I/O bandwidth used per second (MBps or KBps) for physical disk requests by the cluster.

Storage Usage Tab

The **Storage Usage** tab displays the following graphs:

- The **Cluster-wide Usage Summary** graph displays a rolling time interval monitor of total storage usage across the cluster that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in-depth analysis, you can add the monitor to the analysis page by clicking the blue link in the upper right of the graph.
- The **Tier-wise Usage** graph displays a pie chart divided into the percentage of storage space used by each disk tier (SSD and DAS-SATA) across the cluster.

Hardware and Virtual Entities Tabs

Clicking these tabs displays a list of hardware and virtual entity types that exist in this cluster. Clicking a hardware entry such as **Hosts** or a virtual entity such as **Containers** displays the information you would see on the **List** tab summary page for that the specified hardware or virtual entity except filtered to just those in this cluster. See Hardware Entities on page 396 and Compute Entities on page 103 for more information.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2879

Capacity Tab

The **Capacity** tab displays current and historical usage information and provides resource planning tools. The capacity planning feature requires a Prism Pro license. For more information, see Capacity Planning in the *Intelligent Operations Guide*.

Security Dashboard Tab

The Security Dashboard provides dynamic summary of the security posture across all registered clusters. The Security Dashboard allows you to view the most critical security parameters like cluster-based issue summary, STIG policy compliance, security hardening, and identified vulnerabilities. For more information, see Security Dashboard in the *Nutanix Security Guide*.

Entity Relationship Widget

The entity relationship widget shows the relationship between related entities like clusters, hosts, and VMs instances. The widget allows quick access between the related entities. You can directly navigate to a target cluster, host, or VM instance through the respective dropdown menus.

Example: Viewing Cluster Instances

Click the **Cluster** dropdown menu to view the list of cluster instances. Alternatively, you search a cluster name.

Figure 158: Clusters

Note:

- The **Recent** label indicates the last accessed entity instances. The widget displays a maximum of three recently accessed entity instances.
- The filtered list of VMs display only the powered-on VM instances.
- If the VMs are not filtered on a host instance, all VMs on the selected cluster are displayed.

Creating a Cluster

Before you begin

Ensure that you meet the following prerequisites:

- All hosts are running AOS 6.7 or later versions.
- All hosts are reimaged with the same set of AOS and hypervisor versions. For information about reimaging the hosts using Foundation Central, see Run Foundation Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2880

- All hosts are reachable.
- All hosts are in the same subnet.

About this task

To create a cluster through Prism Central, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Hardware** > **Clusters**.
   The system displays the **List** tab with all the registered clusters in your **Nutanix** environment.
3. Click **Create Cluster**.
4. Review the **Create Cluster Prerequisites**, and click **Next**.
5. Enter the following details in the **Create Cluster** wizard:
   a. In the **Select Host** section, enter the CVM IP of the hosts that you want to use for cluster creation, separated by a comma or a space and click **Discover Hosts**.
      The list of discovered hosts, along with their details, is displayed at the bottom of the wizard.
   b. In the **Configure** section, enter the following details:
      - **Cluster Name**: Name for the cluster.
      - **Cluster external IP**: [Optional] External IP address for the cluster.
      - **Cluster Fault Tolerance**: [Optional] Fault tolerance for the cluster. The default value is **1N/1D**.
        Consider the following when you select the fault tolerance for your cluster:
        - A one-node cluster supports 1N/1D mirroring inside single node.
        - A two-node cluster supports 1N/1D mirroring inside each node and 1N/1D across clusters.
        - Clusters with more than three nodes do not support any mirroring inside nodes.
        - You can choose 1N&1D if the cluster has a minimum of three nodes only. You can choose 2N/2D if the cluster has a minimum of five nodes only.

        For more information on the types of cluster fault tolerance see, Cluster Fault Tolerance in the *Prism Element Web Console Guide*.
      - **DNS Server(s) IP**: [Optional] IP address of DNS server, separated by a comma or a space if you are entering multiple IP addresses.
      - **NTP Server(s) IP**: [Optional] IP address of NTP server, separated by a comma or a space if you are entering multiple IP addresses.
      - **Container Name**: [Optional] Name of the container that you want to be associated with the cluster.
      - **Cluster Fault Tolerance Domain**: [Optional] Select the fault tolerance domain for the cluster. The default value is **Disk** for a single node cluster, and **Node** for multiple-nodes cluster. You can choose **Disk**, **Block**, or **Rack** as the fault tolerance domain.
      - **Enable Backplane Segmentation**: [Optional] Enable backplane segmentation. Backplane segmentation separates the CVM-to-CVM traffic from other kinds of traffic. This is applicable only if you have at least three hosts. If you enable backplane segmentation, you need to enter a few mandatory

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2881

parameters such as subnet, netmask, and ports. For more information on backplane segmentation, see Segmented and Unsegmented Networks.

c. Click **Next**.

In the **Review** section, the pre-checks are run to validate that the hosts meet all the requirements mentioned under the Prerequisites. If the pre-checks are successful, the configuration details of the cluster are displayed for review.

d. Click **Create Cluster**.

Cluster creation operation might take some time. Under **Recent Tasks**, you can verify that a cluster create task was initiated.

What to do next

You can register the newly created cluster with Prism Central. For more information, see Registering or Unregistering a Cluster with Prism Central on page 61.

Destroying a Cluster

Before you begin

Ensure the following prerequisites:

- The minimum supported versions for destroying a cluster through Prism Central are version 6.8 for Prism Element (with recommended AHV version) and version pc.2024.1 for Prism Central.
- You need to reclaim your license before destroying a cluster.

About this task

> **Caution:** Destroying a cluster is irreversible. Upon successful completion of this operation, the cluster is unregistered, and all the nodes go back to the available node pool. All cluster settings, user VMs, and data policies are permanently deleted, and all Prism Central configurations for categories and policies applied to the cluster are lost. Nutanix recommends performing all the preparatory actions before destroying a cluster.

To destroy a cluster through Prism Central, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Hardware** > **Clusters** .
   The system displays the **List** tab with all the registered clusters in your **Nutanix** environment.
3. Select the cluster to destroy and click **Actions** > **Destroy Cluster**.

> **Note:** You cannot destroy a cluster that is hosting a Prism Central Instance.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2882

4. Review the **Destroy Cluster Prerequisites** and click **Next**.

   The pre-checks are run to validate that the cluster meets all the requirements mentioned under the Prerequisites. The result of the pre-checks and the cluster details are displayed for review.

Figure 159: Destroy Cluster

5. Under **Destroy Cluster?**, type DESTROY to confirm the destroy cluster operation.

   Note that this is a case-sensitive input, and you need to enter the word in upper-case.

6. Click **Destroy Cluster**.

   Destroy Cluster operation might take some time. Under **Recent Tasks**, you can verify that a cluster destroy task has been initiated.

Managing Cluster Fault Tolerance

You can modify the fault tolerance of the cluster based on your cluster configuration.

About this task

- You can modify the fault tolerance of a cluster from 1N/1D to 2N/2D. Before you do this, ensure that the cluster has a minimum of five nodes.
- You cannot modify the fault tolerance of a cluster from 1N/1D to 1N&1D. The 1N&1D cluster fault tolerance must be configured when you create the cluster.
- You cannot modify the fault tolerance of a cluster with 1N&1D fault tolerance.
- You cannot reduce the cluster fault tolerance. For example, you cannot reduce the cluster fault tolerance from 2N/2D to 1N/1D. If you attempt to reduce cluster fault tolerance, Prism Central displays an error.
- Increasing the cluster fault tolerance might require at least 30 percent of your disk space.
- For more information on the types of cluster fault tolerance, see Cluster Fault Tolerance in the *Prism Element Web Console Guide*.

To modify the fault tolerance of a cluster through Prism Central, perform the following steps:

Procedure

1. Log in to Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2883

2. Select the **Infrastructure** application from Application Switcher Function, and go to **Hardware** > **Clusters**.
   The system displays the **List** tab with all the registered clusters in your **Nutanix** environment.
3. Select the checkbox associated with the cluster and click **Actions** > **Manage Cluster Fault tolerance**.
   The system displays the **Manage Cluster Fault Tolerance** dialog box.
4. From the **Change Cluster Fault Tolerance** dropdown menu, select **2N/2D**.
   The system increases the fault tolerance to 2N/2D and displays **Configured CFT : 2N/2D** in the **Cluster Resiliency / Fault Tolerance Status** widget in the **Summary** tab on the **Clusters** page of Prism Central.

Settings Profile for Clusters

Prism Central version pc.2024.3 onwards, you can create a cluster profile with system settings that you can apply to multiple clusters with a single click. When you apply a profile to a cluster, the settings in the profile are applied to the corresponding settings on the cluster.

The following system settings can be configured through the settings profile:

- NTP server
- Name server
- SNMP
- SMTP server
- Syslog server
- File system allowlists
- Pulse

For more information on cluster system settings, see System Management in the *Prism Element Web Console Guide*.

Viewing Cluster Profiles

Using the Prism Central web console, you can view the list of settings profile for clusters.

About this task

Summary tab on the Profiles page provides a dashboard of all the settings profiles created for the clusters.

To access the summary view of all the clusters, follow these steps:

Procedure

1. Log in to the Prism Central web console.
2. From the Application Switcher, select the **Infrastructure** application, and navigate to**Hardware** > **Clusters**.
   The system displays the **List** tab with all the registered clusters in your Nutanix environment.
3. Select the **Profiles** tab.
   The system displays a list of all the profiles along with the number of assigned clusters, drifting clusters (clusters where local settings override the profile settings), number of system settings in the profile, and the date and time when the profile was last modified.
4. Click the name of a profile to view the details.
   The system displays the profile details under three tabs: **Summary**, **Compliance**, and **Settings**. The **Summary** tab displays basic details about the Profile. The **Compliance** tab displays details such as compliance

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2884

status, number of drifting cluster settings, actions to be taken for the drifting settings. The **Settings** tab displays all the settings included in the profile, listed under respective categories.

Creating a Cluster Settings Profile

Using the Prism Central web console, you can create a settings profile for clusters.

Before you begin

Ensure that all hosts are running AOS 7.0 or later versions.

About this task

To create a settings profile for clusters, follow these steps:

Procedure

1. Log in to the Prism Central web console.
2. From the Application Switcher, select the **Infrastructure** application, and navigate to**Hardware** > **Clusters**. The system displays the **List** tab with all the registered clusters in your Nutanix environment.
3. Click the **Profiles** tab.
4. Select **Create Profile**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2885

5. In the **Create Settings Profile** window, enter the following details under the Setup Profile section:

   - **Profile Name**: Enter a name for the settings profile. Alphabets, numbers, dots, hyphens, and underscores are allowed.
   - **Profile Description**: Enter a description for the settings profile.
   - **Configuration Type**: Do one of the following:

     - **Configure new settings values**: To configure new settings for the profile, follow these steps:

       1. Click **Add Settings** to add the settings and configure values for each setting added to the profile.
       2. In the **Add Settings** window, click the blue plus **(+)** icon to select the settings or a group of settings to configure as part of this profile from **Available Settings**on the left. The selected settings or group of settings move to the right side under **Settings in Profile**.

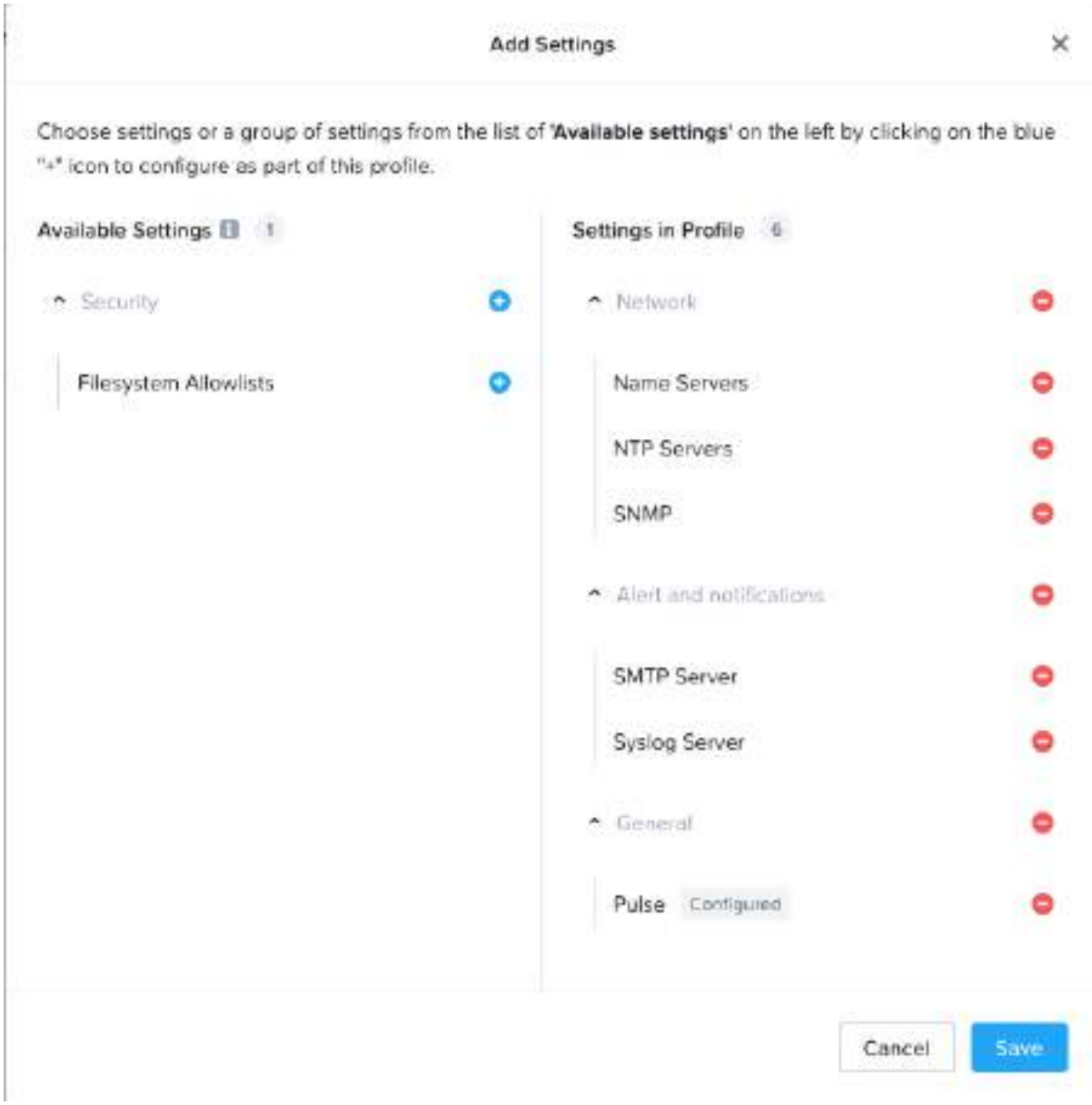


Figure 160: Create Profile - Configure New Settings

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2886

3. Click **Save**. Under the **Configure Settings** section, you can see all the selected settings listed along with their setting type, configuration status, and applicable actions.

- **Import Settings Values from Existing Cluster**: To import settings, follow these steps:

  1. Select a cluster from which the settings are to be imported.
  2. Click **Next**.

     Under the **Configure Settings** section, all the settings in the selected cluster are replicated to the new profile.
  3. The configuration for SNMP and SMTP Server requires authentication, you must enter the authentication information to complete the configuration.

6. [Optional] Click **Configure** to configure a setting, and **Remove** to remove a setting from the profile.
   Pulse is configured by default, you can either edit the setting or remove it.

7. [Optional] Select **Allow Override** to allow a cluster admin to change the settings for an individual cluster through Prism Element web console.
   In this case, the changes made by the cluster admin are not considered as drifted settings.

8. Click **Create Profile**.
   The system displays the newly created profile under the **Profiles** tab.

Updating a Settings Profile

Using the Prism Central web console, you can update a settings profile for clusters.

About this task

To update a settings profile for clusters, follow these steps:

Procedure

1. Log in to the Prism Central web console.

2. From the Application Switcher, select the **Infrastructure** application, and navigate to**Hardware** > **Clusters**.
   The system displays the **List** tab with all the registered clusters in your Nutanix environment.

3. Select the **Profiles** tab.
   The system displays a list of all the profiles.

4. From the **Actions** drop-down menu, select the settings profile, then select **Update**.

5. In the **Update Settings Profile** window, modify one or more of the following:

   - Profile name and description
   - Setting configurations
   - List of clusters assigned to the profile

6. Click **Save**.

Deleting a Settings Profile

Using the Prism Central web console, you can delete a settings profile for clusters.

Before you begin

You must disassociate all the clusters from a profile before you delete the profile.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2887

About this task

To delete a settings profile for clusters, follow these steps:

Procedure

1. Log in to the Prism Central web console.
2. From the Application Switcher, select the **Infrastructure** application, and navigate to**Hardware** > **Clusters**.
   The system displays the **List** tab with all the registered clusters in your Nutanix environment.
3. Select the **Profiles** tab.
   The system displays a list of all the profiles.
4. From the **Actions** drop-down menu, select the settings profile, then select **Delete**.
   The **Delete** action is enabled only for the profiles that do not have any associated clusters.

Assigning Clusters to a Settings Profile

Using the Prism Central web console, you can assign a settings profile to one or more clusters. A cluster can be assigned only one profile at a time.

About this task

To assign a settings profile to one or more clusters, follow these steps:

Procedure

1. Log in to the Prism Central web console.
2. From the Application Switcher, select the **Infrastructure** application, and navigate to**Hardware** > **Clusters**.
   The system displays the **List** tab with all the registered clusters in your Nutanix environment.
3. Select the **Profiles** tab.
   The system displays a list of all the profiles.
4. From the **Actions** drop-down menu, select the settings profile, then select **Assign Clusters**.
5. In the **Assign Settings Profile** page, click **Select Clusters**.
6. In the **Select Clusters** page, select the clusters where the profiles setting is to be applied.
7. Click **Save**.
   A pre-check script verifies if the version of all the selected clusters are compatible with the settings included in the settings profile. After a successful verification, the clusters are assigned to the profile.

Disassociating Clusters from a Settings Profile

Before you can assign a profile to a cluster that already has another profile assigned to it, you must first disassociate the cluster from the earlier profile, then you can assign the new profile to the cluster.

About this task

To disassociate a cluster from a settings profile, follow these steps:

Procedure

1. Log in to the Prism Central web console.
2. From the Application Switcher, select the **Infrastructure** application, and navigate to**Hardware** > **Clusters**.
   The system displays the **List** tab with all the registered clusters in your Nutanix environment.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2888

3. Select the **Profiles** tab.
   The system displays a list of all the profiles.
4. Select a settings profile.
5. From the list of associated clusters, select the clusters to disassociate and click **Disassociate Clusters**.

Reapplying Profile to a Cluster

If a settings profile is assigned to a cluster and the same settings are later modified on cluster level, the modified settings are displayed as drifted, and the cluster is displayed as non-compliant. Using the Prism Central web console, you can overwrite these drifted settings by reapplying the profile.

About this task

To reapply a settings profile on a cluster, follow these steps:

Procedure

1. Log in to the Prism Central web console.
2. From the Application Switcher, select the **Infrastructure** application, and navigate to**Hardware** > **Clusters**.
   The system displays the **List** tab with all the registered clusters in your Nutanix environment.
3. Select the **Profiles** tab.
   The system displays a list of all the profiles.
4. Select a settings profile.
5. From the list of associated clusters, select the clusters to reapply the profile and click **Reapply**.
   After you reapply a profile to a cluster, the drifted settings are overwritten, and the cluster becomes compliant with the settings profile.

Host Management

In Prism Central, the hosts dashboard allows you to view summary information about hosts across registered clusters and access detailed information about each host. For more information, see Hosts Summary View on page 419 and Host Details View on page 423.

You can perform the following actions to manage hosts in Prism Central:

- Assign a category to the host. For more information, see Assigning a Category on page 460.
- Run playbook to perform operations on host. For more information, see Task Automation - Playbooks in *Intelligent Operations Guide*.
- Rename an AHV host. For more information, see Renaming an AHV Host on page 428.
- Expand a cluster. For more information, see Expanding a Cluster through Prism Central on page 428.
- Remove a node from the cluster. For more information, see Removing a Node through Prism Central on page 435.
- Put the host in maintenance mode. For more information, see Putting a Host into Maintenance Mode Using Prism Central on page 436.
- Remove the host from maintenance mode. For more information, see Exiting a Host from Maintenance Mode Using Prism Central on page 437.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2889

Hosts Summary View

The **Summary** tab on the **Hosts** page provides a dashboard of the hosts across all the registered clusters.

To access the summary view of all the hosts, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Hardware** > **Hosts** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The system displays the **List** tab by default with all the hosts across registered clusters in **Nutanix** environment. For information about how to access the list of hosts in **Non-Nutanix** environment (non-nutanix hosts managed by external *vCenter*), see Host Details View on page 423.
3. Click the **Summary** tab. The system displays **Summary** page for all the hosts.

   > **Note:** To access the summary view of all the hosts managed by *vCenter*, select **Non-Nutanix** environment from the dropdown menu in **Hosts** page.
   >
   > The **Summary**, **Alerts**, and **Events** tabs display the same information as for Nutanix-managed clusters. The **Metrics** tab displays a subset of the full list (5 of the 7 metrics). The **List** tab displays fields for name, host IP, VM count, memory capacity, and cluster name.

   Using playbooks, you can manage the hosts in **Non-Nutanix** environment. For more information about playbooks, see Task Automation - Playbooks in *Intelligent Operations Guide*.

Clicking the **Summary** tab displays the following three widgets:

- **Suggested**: Displays a list of the hosts with the highest usage of the parameter you select from the dropdown menu on the right of the widget. The options are **CPU Usage**, **Memory Usage**, **IO Latency**, and **IOPS**. Click the **View all XX Hosts** link at the bottom to display the **List** tab (following section).
- **Alert**: Displays a list of host-related alerts that occurred during the specified interval. Select either **Last 24 hours** (default) or **Last week** from the dropdown menu.
- **Anomalies**: Displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified interval. Select either **Last 24 hours** (default) or **Last week** from the dropdown menu. When an anomaly appears, you can click on the graph, which then displays a list of those anomalies. Clicking on an anomaly displays the event page for that anomaly.

List Tab

Clicking the **List** tab, which appears by default when you first open the page, displays a list of the hosts across the registered clusters. The following table describes the fields that appear in the hosts list. The fields vary based on the **Focus** menu selection, which is either **General** or **Performance**. A dash (-) is displayed in a field when a value is not available or applicable.

Table 109: Hosts List Fields

Parameter	Description	Values
General Focus Fields		
Name	Displays the name of the host. Clicking on the name displays the details page for that host. For more information, see Host Details View on page 423.	(host name)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2890

Parameter	Description	Values
Host IP	Displays the IP address assigned to the hypervisor running on the host.	(IP address)
CVM IP	Displays the IP address assigned to the Controller VM.	(IP address)
Hypervisor	Displays the hypervisor type running on the host.	AHV, ESX, or Hyper-V
Memory Capacity	Displays the memory capacity of the host.	xxx [MB|GB]
Cluster	Displays the name of the cluster in which the host resides.	(cluster name)
Performance Focus Fields		
Name	Displays the name of the host.	(host name)
CPU Usage	Displays the percentage of CPU capacity currently being used by this host.	0 - 100%
Memory Usage	Displays the percentage of memory capacity currently being used by this host.	0 -100%
IOPS	Displays I/O operations per second (IOPS) for this host.	[0 - unlimited]
Disk IO Bandwidth	Displays I/O bandwidth used per second for this host.	xxx [MBps|KBps]
IO Latency	Displays the average I/O latency (in milliseconds) for this host.	xxx [ms]
Cluster	Displays the name of the cluster in which the host resides.	(cluster name)

You can filter the hosts list based on a variety of parameter values. The following table describes the filter options available when you open the Hosts view **Filter** pane. To apply a filter, select a parameter and check the box of the desired value (or multiple values) you want to use as a filter. You can apply filters across multiple parameters. Some parameter filters require additional context such as a constraint string or a range.

Table 110: Filters Pane - Hosts Page

Parameter	Description	Values
Name	Filters on the host name. Select a condition from the dropdown menu (**Contains**, **Doesn't contain**, **Starts with**, **Ends with**, or **Equal to**) and enter a string in the field. It will return a list of hosts that satisfy the name condition/string.	(host name string)
Cluster	Filters on the cluster name. Enter a string in the field. It will return a list of hosts that reside in the clusters which satisfy the name string.	(cluster name string)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2891

Parameter	Description	Values
Health	Filters on the host health state (good, warning, or critical). Select one or more states to return a list of hosts in that state(s). The number of hosts currently in each state is displayed on the right of the line.	Critical, Warning, Good
Categories	Filters on category names. Enter a category name in the field and then check the box. As you type a dropdown menu appear to help you select the correct category. A new field appears where you can add more categories to the filter. The number of hosts tagged to each selected category is displayed on the right of the line.	(category name)
Hypervisor	Filters on the hypervisor type. Select one or more hypervisors to return a list of clusters running those hypervisor(s). The number of clusters currently running each hypervisor is displayed on the right of the line.	AHV, ESXi, Hyper-V
Memory Capacity	Filters on the host memory capacity. Check the box for the desired range or enter an amount range in the *from <low> to <high> GiB* field. It will return a list of hosts with memory capacity in that range.	([xx] to [yy] GiB range)
CPU Usage	Filters on the amount of CPU being used. Check the box for the desired range or enter a percentage range in the *from <low> to <high> %* field. It will return a list of hosts utilizing CPU in that range (0-100%).	([xx] to [yy]% range)
Memory Usage	Filters on the amount of total memory being used. Check the box for the desired range or enter a percentage range in the *from <low> to <high> %* field. It will return a list of clusters utilizing total memory in that range (0-100%).	([xx] to [yy]% range)
GPUs	Filters for GPU configuration information such as model name. Select a condition from the dropdown menu (**Contains**, **Doesn't contain**, **Starts with**, **Ends with**, or **Equal to**) and enter a string in the field. As you type a dropdown menu appears to help you select the correct configuration information. It will return a list of hosts that satisfy the GPU condition/string.	(configuration info)
IOPS	Filters on the IOPS. Check the box for the desired range or enter a range in the *from <low> to <high> iops* field. It will return a list of hosts with IOPS in that range.	([xx] to [yy] range)
IO Bandwidth	Filters on the I/O bandwidth used. Check the box for the desired range or enter a range in the *from <low> to <high> bps* field. It will return a list of hosts with I/O bandwidth usage in that range.	([xx] to [yy] range)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2892

Parameter	Description	Values
IO Latency	Filters on the average I/O latency. Check the box for the desired range or enter a range in the *from <low> to <high> ms* field. It will return a list of hosts with average I/O latency in that range.	([xx] to [yy] range)

You can perform the following actions for the hosts in the **List** tab:

- Access the detailed information about an individual host. For more information, see Host Details View on page 423.
- Filter the host list based on available parameter values using **Filters** pane. For more information about **Filters** pane, see Filters Pane - Hosts Page.
- Export the table that contains the list of hosts and their information to a file in a CSV format. For more information about **Export** option, see Export on page 59.
- Group the hosts based on pre-defined criteria. For information about how to group the clusters, see Group by on page 56.
- View hosts based on pre-defined criteria or create a custom view. For information about available views and how to create a custom view, see View by on page 56.
- Perform the host-specific actions on a single or multiple hosts using the **Actions** dropdown menu. For more information, see Host Management on page 418 .

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options as the Alerts dashboard, except it is filtered to display just host-related alerts across the registered clusters. For more information, see Alerts Summary View (Prism Central) in *Prism Central Alerts and Events Reference Guide*.

Audits Tab

The **Audits** tab displays a table of audits. This tab provides the same features and options as the Audits dashboard, except it is filtered to display just host-related events across the registered clusters. For more information, see Audits Summary View on page 449.

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options as the Events dashboard, except it is filtered to display just host-related events across the registered clusters. For more information, see Events Summary View (Prism Central) in *Prism Central Alerts and Events Reference Guide*.

Metrics Tab

The **Metrics** tab allows you to view usage metrics across the hosts. Clicking the **Metrics** tab displays a list of available metrics; click the metric name to display the relevant information to the right. The following table describes the available metrics. (Some metrics are not available on all hypervisors.)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2893

Table 111: Metrics Tab Fields

Metric	Description
CPU Usage	Displays a CPU usage table listing current values and total hosts (number). The current values are split into percentile intervals (for example, less than 25%, 25-50, 50-75, more than 75%). Clicking on a percentile interval displays the Summary tab filtered to just those hosts. **Note:** The same format also applies to the other metrics in this table with either percentile or quantity intervals.
Memory Swap	Displays memory swap-out and swap-in rate tables.
Memory Usage	Displays a memory percentage usage table.
IOPS	Displays total, read, and write IOPS tables.
IO Latency	Displays total, read, and write I/O latency rate tables.
IO Bandwidth	Displays total, read, and write I/O bandwidth rate tables.
Network Packets Dropped	Displays the number of network packets that have been received and then dropped.

Host Details View

Summary Tab

The **Summary** tab of an individual host consists of a dashboard that provides the detailed information about the host.

To access the **Summary** tab of an individual host:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Hardware** > **Hosts** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   By default, the system displays the **List** tab with all the hosts.
3. Click the target <*host_name*> to view the **Summary** tab of an individual host.

   Note: Replace <*host_name*> with the actual host name at your site.

The **Summary** tab of an individual host provides the following widgets and actions:

- **Properties**: Displays summary information about the host. For more information, see the Host Properties on page 424 table.
- **Alert**: Displays a list of related alerts that occurred during the specified interval. Select either **Last week** (default),**Last 1 hour**, or **Last 24 hours** from the dropdown menu on the top right corner of the widget.
- **Metrics**: Displays the metrics information: **CPU Usage**, **Memory Usage**, **IOPS**, **IO Latency**, and **IO Bandwidth**.
- **Anomalies**: Displays a graph of memory, I/O, CPU, networking, disk, or other anomalies that occurred during the specified interval. Select either **Last week** (default), **Last 1 hour**, or **Last 24 hours** from the dropdown menu on the top right corner of the widget. When an anomaly appears, you can click the graph to display a list of those anomalies. If you click an individual anomaly, the system displays the event page for that anomaly.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2894

- **Rename**: Renames an AHV host. For more information, see Renaming an AHV Host on page 428.
- **Manage Categories**: Manages categories for the host. For more information, see Category Management on page 456.
- **Run Playbook**: Runs a playbook. For more information, see Running a Playbook (Manual Trigger) in *Intelligent Operations Guide*.

The host name and the following set of tabs appear on the left: **Summary**, **Alerts**, **Events**, **Metrics**, **Usage**, **Hardware**, and **Virtual Entities**. Click a tab to display that information on the right. Click the **Back to Hosts** link to return to the summary view.

Host Properties

The following table describes the fields in the **Properties** widget. A dash (-) in a field indicates there is not enough data to evaluate or a value is not assigned. The displayed fields vary by hypervisor.

Table 112: Host Properties Fields

Parameter	Description	Values
Memory Capacity	Displays the total memory capacity for this host.	xxx [MB|GB]
Disk Capacity	Displays the total amount of disk capacity on this host.	xxx [GB|TB]
Cluster	Displays the name of the cluster in which the host resides. Clicking the name displays the details page for that cluster . For more information, see Cluster Details View on page 405.	(cluster name)
Host IP	Displays the host IP address.	(IP address)
Hypervisor	Displays the hypervisor name.	(hypervisor name)
VM Count	Displays the number of VMs running on this host.	(number)
Block Model	Displays the block model number.	(model series number)
Serial Number	Displays the block serial number.	(block serial number)
CPU Capacity	Displays the total CPU capacity for this host.	xxx [GHz]
CVM IP	Displays the IP address assigned to the Controller VM.	(IP address)
IPMI Address	Displays the IP address of the Intelligent Platform Management Interface (IPMI) port. An IPMI port is used for the hypervisor host console.	(IP address)
Node Serial	Displays the node serial number. The node serial is a unique number passed through from the manufacturer. (The form can vary because it is determined by each manufacturer.)	(manufacturer serial number)
Oplog Disk %	Displays the percentage of the operations log (oplog) capacity currently being used. The oplog resides on the metadata disk.	[0 - 100%]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2895

Parameter	Description	Values
Oplog Disk Size	Displays the current size of the operations log. (The Oplog maintains a record of write requests in the cluster.) A portion of the metadata disk is reserved for the Oplog, and you can change the size through the nCLI.	xxx [GB]
Monitor Enabled	Displays whether the host is high availability (HA) protected. A **Yes** value means HA is active for this host. A **No** value means VMs on this host are not protected (will not be restarted on another host) if the host fails. Normally, this value should always be **Yes**. A **No** value is likely a sign of a problem situation that should be investigated.	[Yes|No]
Disks	Displays the number of disks in each storage tier in the host. Tier types vary depending on the Nutanix model type.	DAS-SATA: (number), SSD-SATA: (number), SSD-PCIe: (number)
GPUs	Displays the number and type of GPUs in the host. For example, if the host contains four Tesla M10 GPUs, this field displays "Tesla M10 (4)".	(GPU type and number)
Datastore(s)	Displays the names of any datastores.	(names)

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options as the Alerts dashboard, except it is filtered to display just alerts for this host. For more information, see Alerts Summary View (Prism Central) in *Prism Central Alerts and Events Reference Guide*.

Audits Tab

The **Audits** tab displays a table of audits. This tab provides the same features and options as the Audits dashboard, except it is filtered to display just host-related events across the registered clusters. For more information, see Audits Summary View on page 449.

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options as the Events dashboard, except it is filtered to display just events for this host. For more information, see Events Summary View (Prism Central) in *Prism Central Alerts and Events Reference Guide*.

Metrics Tab

The **Metrics** tab allows you to view usage metrics for the host. Click the **Metrics** tab and then the desired metric name (see following table) to display a graph for that metric on the right. The graph is a rolling time interval performance or usage monitor. The baseline range appears as a blue band in the graph.

> **Note:** The baseline range and identified anomalies are based on sophisticated machine-learning capabilities. For more information, see Behavioral Learning Tools in *Intelligent Operations Guide*. The machine-learning algorithm uses 21 days of data to monitor and predict performance. A graph or baseline band may not appear if less than 21 days of data is available.

- Place the cursor anywhere on the horizontal axis to display the value at that time.
- Select the duration (time interval) from the dropdown list on the right (last 1 hour, last 24 hours, last week, last 21 days).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2896

- [I/O-based metrics] Check the appropriate box(es) to have the graph display total, read, or write usage (or any combination of the three).
- Click **Alert Settings** to configure an alert for this metric. For more information, see Creating Custom Alert Policies in *Prism Central Alerts and Events Reference Guide*.

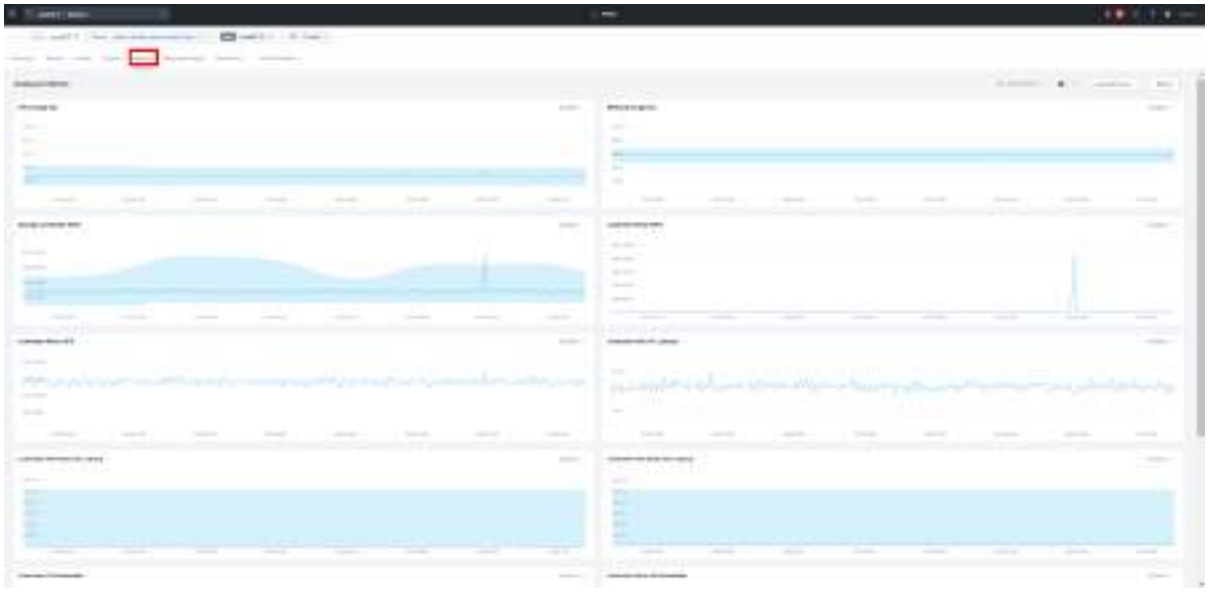


Figure 161: Host Metrics Tab

The following table describes the available metrics. Some metrics are not available on all hypervisors.

Table 113: Metrics Tab Fields

Metric	Description
CPU Usage	Displays the percentage of CPU capacity currently being used by the host (0 - 100%).
Memory Usage	Displays the percentage of memory capacity currently being used by the host (0 - 100%).
Controller IOPS	Displays graph for total I/O operations per second (IOPS) for the host.
Controller Read IOPS	Displays graph for read I/O operations per second (IOPS) for the host.
Controller Write IOPS	Displays graph for write I/O operations per second (IOPS) for the host.
Controller AVG I/O Latency	Displays graph for average I/O latency (in milliseconds) for physical disk requests by the host.
Controller AVG Read I/O Latency	Displays graph for average read I/O latency (in milliseconds) for physical disk requests by the host.
Controller AVG Write I/O Latency	Displays graph for average write I/O latency (in milliseconds) for physical disk requests by the host.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2897

Metric	Description
Controller I/O Bandwidth	Displays graph for I/O bandwidth used per second (MBps or KBps) for physical disk requests by the host.
Controller I/O Read Bandwidth	Displays graph for read I/O bandwidth used per second (MBps or KBps) for physical disk requests by the host.
Controller I/O Write Bandwidth	Displays graph for write I/O bandwidth used per second (MBps or KBps) for physical disk requests by the host.

Storage Usage Tab

The **Storage Usage** tab displays the following graphs:

- The **Usage Summary** graph displays a rolling time interval monitor of host storage usage that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in depth analysis, you can add the monitor to the analysis page by clicking the blue link in the upper right of the graph.
- The **Tier-wise Usage** graph displays a pie chart divided into the percentage of host storage space used by each disk tier (SSD and DAS-SATA).

Figure 162: Host Usage Tab

Hardware and Virtual Entities Tabs

Clicking these tabs displays a list of hardware and virtual entity types that exist on this host. Clicking a hardware entry such as **Disks** or a virtual entity such as **VMs** displays the information you would see on the **List** tab summary page for that the specified hardware or virtual entity except filtered to just those on this host. For more information, see Hardware Entities on page 396 and Compute Entities on page 103 topics.

Entity Relationship Widget

The entity relationship widget shows the relationship between related entities like clusters, hosts, and VMs instances. The widget provides quick access between the related entities. You can directly navigate to a target cluster, host, or VM instance through the respective dropdown menus.

Example: Viewing Hosts on a Cluster

Click the **Host** dropdown menu to view the list of host instances on the selected cluster. Alternatively, you can search the host instance name belonging to the target cluster.

Note:

- The **Recent** label indicates the last accessed entity instances. The widget displays a maximum of three recently accessed entity instances.
- The filtered list of VMs display only the powered-on VM instances.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2898

- If the VMs are not filtered on a host instance, all VMs on the selected cluster are displayed.

Renaming an AHV Host

You can rename an AHV host from Prism Central.

About this task

The minimum supported versions to rename an AHV host from Prism Central are AOS 6.6 for the registered Prism Element (with recommended AHV version) and 2022.9 for Prism Central. For information on the recommended AHV version based on the AOS release and hardware model, see Compatibility and Interoperability Matrix.

To rename an AHV host from Prism Central, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Hardware** > **Hosts** .
   The system displays the **List** tab by default with all the hosts across registered clusters.
3. Select the target host checkbox, and choose **Rename** from the **Actions** dropdown menu.
   The system displays the **Rename Host** window.
4. Enter a new name for the host in the **New Host Name** field, and click **Save**.

   You must adhere to the following rules for the host name:

   - Allowed characters are: uppercase letters (A-Z), lowercase letters (a-z), decimal digits (0-9), dots (.), and hyphens (-).
   - The host name must start and end with a number or letter.
   - A minimum of one character and a maximum of 63 characters are allowed.
   - Successive dots are not allowed. Each dot-separated string must follow the first two rules.

   Note: Once the AHV host rename task is complete, it might take a few minutes for the changes to propagate from the host to Prism Central.

Expanding a Cluster through Prism Central

A cluster is a collection of nodes. You can expand a cluster by adding new nodes to the cluster after connecting them to the network on the same subnet as the cluster. The cluster expansion process compares the AOS version on the existing and new nodes and performs any upgrades necessary for all the nodes to run the same AOS version.

Before you begin

Ensure that the following prerequisites are met before you add a node to the cluster:

- Review the relevant sections in Prerequisites for adding a node before attempting to add a node to the cluster. The process for adding a node varies depending on several factors. This section covers specific considerations based on your AOS, hypervisor, encryption, and hardware configuration.
- Check the Health of the cluster. If any health checks are failing, resolve them before adding any nodes. As a final check, run NCC to ensure that the cluster is healthy.
- Allow any current expand cluster operations to complete.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2899

- All nodes are in the correct metadata state by checking the Hardware dashboard. If any nodes show Metadata store disabled on the node or Node is removed from metadata store, enable the metadata store by clicking **Enable Metadata Store**.
- Follow the SSDs' requirements for Hybrid HCI Node and All-Flash HCI Node specified in HCI Node Field Requirements in the *Acropolis Advanced Administration Guide*.

About this task

You can add new nodes to a cluster using Prism Central or Prism Element web console. For information about expanding a cluster through Prism Element web console, see Expanding a Cluster in the *Prism Element Web Console Guide*.

The minimum supported versions to add new hosts using Prism Central web console is Prism Central version 2023.3. From Prism Central version pc.2024.3 onwards, you can expand a cluster without registering the same with Prism Central.

To add one or more nodes to an existing cluster through Prism Central, do the following:

Procedure

1. Log in to Prism Central.
2. From the Application Switcher Function on page 45, select the **Infrastructure** application, and navigate through **Navigation Bar** to **Hardware** > **Clusters**.

   For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The system displays the **List** tab with all the registered clusters in your **Nutanix** environment.
3. Select the cluster that you want to expand, and click **Expand Cluster**.

   The system searches for hosts in the entire network and all the discovered hosts are listed in the **Expand Cluster** page.
4. (Optional) Click **Discover Hosts Manually** to discover any hosts that are not listed after automatic host discovery, and enter the hostname or CVM IP.

   > **Note:** ESXi or AHV compute-only nodes and hosts with deactivated IPv6 support are not discovered automatically. You must initiate manual host discovery for such hosts.
5. In the **Select Host** page, select the hosts that you want to add to the cluster, and click **Next**.
6. In the **Choose Host Type** page, select **Host Type** from the dropdown menu for each of the hosts you have selected, and then click **Next**.

   You can select any one of the following host types:

   - **HCI**: Standard host in the cluster.
   - **Storage**: Host optimized for storage usage. This type of host allows seamless expansion of storage capacity of your cluster.
   - **Compute**: Host optimized for computing purposes (CPU and memory).
7. In the **Configure Host** page, enter or update the host details such as hostname, CVM IPv4, CVM IPv6, hypervisor IPv4, hypervisor IPv6, IPMI IPv4, IPMI IPv6. Click **Next**.

   Host name is required for the Hyper-V clusters, while it is optional for AHV and ESXi clusters.
8. (Optional) In the **Networking** page, select the **Active Uplink**and **Backup Uplink** for each host and click **Next**. To configure the switches, expand the row containing each host.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2900

9. In the **Software Check** page, review the AOS and hypervisor versions and their compatibility status.

   The new hosts must run the same AOS and hypervisor versions as the cluster. If the host's AOS version is lower than the cluster's AOS version, an upgrade is performed.

   If there is a version mismatch between the new host and ESXi or Hyper-V cluster, you are prompted to upload the ISO in the ~/software_downloads/hypervisor_installer directory in any one CVM of the cluster using wget command. If the ~/software_downloads/hypervisor_installer directory does not exist on the CVM, you must create the directory and then upload the ISO file. After you upload the ISO file, enter the ISO file name in the text box under **hypervisor Compatibility** and click **Validate**. The system checks for the file and displays a message.

10. Click **Next**.

11. Review the model and serial information displayed for all the selected hosts, and click **Expand Cluster**.

12. (Optional) You can click **Run Prechecks** before clicking **Expand Cluster** to know any issues that you must fix before proceeding with the Expand Cluster operation.

    Under Recent tasks list, you can verify that the **Expand Cluster** operation has started. The operation might take some time if it involves the re-imaging or a software upgrade at the node.

Prerequisites for expanding a Cluster through Prism Central

The process for expanding a cluster varies depending on the AOS version, hypervisor host type, data-at-rest encryption status, and certain hardware configuration factors.

AOS Considerations

The following apply to any cluster:

- Ensure that the total number of nodes per cluster does not exceed the Cluster Maximums defined in Maximum System Values in *Prism Element Web Console Guide*. Note that the maximum number of nodes per cluster differ per the hypervisor type and in case it is a pure hypervisor cluster (cluster with only one type of hypervisor) or mixed hypervisor cluster (cluster with more than one type of hypervisor).
- The expand cluster process does not support compute-only node preparation.
- The expand cluster discovery step (finding nodes to add) requires that IPv6 multicast packets are allowed through the physical switch. Therefore, the expand cluster process does not work when IPv6 is disabled in your network. If IPv6 is not enabled currently, do one of the following:
  - Enable IPv6 in your network and retry the expand cluster operation.
  - If enabling IPv6 is not an option, the expand cluster procedure allows you to enter the IP addresses of nodes to add manually and run discovery using IPv4. This requires that you have the IP addresses before starting the expand cluster operation.
- If the Controller VM memory on a new node is less than the current nodes in the cluster, the expand cluster process increases the memory on the new node to the same base value as the current nodes. The new Controller VM is upgraded to a maximum of 32 GB.

  The Controller VM is upgraded to a maximum of 28 GB for ESXi nodes with 64 GB or less of total physical memory. With total physical memory greater than 64 GB, the existing Controller VM memory is increased by 4 GB.
- A new node is reimaged automatically before being added under certain conditions. The following table describes those conditions.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2901

Table 114: Node Imaging Criteria

Configuration	Description
Same AOS and hypervisor versions	The node is added to the cluster without reimaging it.
Same hypervisor version but different AOS version	The node is automatically reimaged before it is added. However, if the AOS version on the node is higher than the version on the cluster, you can upgrade the cluster to the higher version. If you do not upgrade the base cluster to match the node AOS version, the node is reimaged automatically to match the lower AOS version of the cluster. For more information about how to upgrade your cluster, see the Life Cycle Manager Guide.
Same AOS version but different hypervisor version	The node is automatically reimaged before it is added.

Note: If you are expanding a cluster (now) on which the network is segmented only by traffic type (management and backplane), see Network Segmentation During Cluster Expansion in the *Security Guide*.

AHV Considerations

The following apply to clusters running AHV:

- If the Controller VMs in the cluster reside in a VLAN configured network, the discovery process still finds any factory-prepared nodes regardless of their current VLAN status (configured or not configured).
- Network configuration has the following restrictions and requirements:
  - You cannot migrate management from br0 to other bridges.
  - You can only have the Controller VM management interface (eth0) and hypervisor management interface deployed on the br0 bridge.

ESXi Considerations

The following apply to clusters running ESXi:

- Before adding a host running ESXi 7.0U2 and later versions, with Trusted Platform Module (TPM) 2.0 enabled, to a cluster, Nutanix recommends that you backup the recovery key created when encrypting the host with TPM. For information on how to generate and backup the recovery key, see *KB 81661* in the *VMware documentation*. Ensure that you use this recovery key to restore the host configuration encrypted by TPM 2.0 if it fails to start after adding the host to your cluster. For information on how to restore an encrypted host, see *KB 81446* in the *VMware documentation*. If you don't have the recovery key, and if the host fails to start, contact Nutanix Support.
- If the ESXi root user password was changed from the default, the expand cluster operation might fail. In this case, reset the ESXi root user password to the default, and then retry the expand cluster procedure. For default cluster credentials, see KB 1661.
- While expanding a Nutanix cluster running NSX enabled ESXi hosts, add the newly imaged node to the Nutanix cluster where the host and CVM management network are configured with a standard vSwitch, and then add the node in NSX manager. Otherwise, the cluster expansion operation fails with the following error. For information on expanding a cluster, see Expanding a Cluster in *Prism Element Web Console Guide*.

  ```
  Failed to get VLAN tag of node <MAC Address of the node>
  ```

- If network segmentation is not enabled, expand cluster supports mixed (ESXi + storage-only) node clusters. However, when network segmentation is enabled, you cannot use expand cluster for a mixed cluster.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2902

- Network configuration has the following restrictions and requirements:
  - You cannot configure the network when either a target node or the base cluster has LACP enabled. Prepare LACP nodes offline using a Foundation VM.
  - You cannot migrate management from vSwitch0 to another standard vSwitch.
  - Management interfaces must either be on a VSS or a DVS; a mixed setup is not supported.
  - If on VSS, the Controller VM management interface (eth0) and the hypervisor management interface must be deployed on vSwitch0 and connected to port group VM Network and Management Network, respectively.
  - If on DVS, all Controller VM management interfaces and all host management interfaces must be connected to the same distributed virtual switch and same port group. (However, the Controller VM interfaces can be connected to a different DVS port group than the host management interfaces.)
  - Segmented network interfaces (backplane, volume, DR) must be on same vSwitch type (VSS or DVS) as the management.
  - If network segmentation is enabled on the base cluster and the backplane is deployed on a separate vSwitch than management, you can create vSwitches (VSS or DVS) and prepare the required Controller VM interfaces. (Manual switch configuration is required for expand now but is integrated into the expand later work flow.)
  - If the base cluster is on DVS and you are doing an expand later, you can migrate the target nodes from the default vSwitch0 to that DVS.
- If the Controller VMs in the cluster reside in a VLAN configured network, you must first configure the new nodes in the same VLAN before attempting to add them. Otherwise, the discovery process does not find these nodes. For more information about VLAN configuration instructions, see Discovering Nodes in a VLAN-Segmented Network in the *Field Installation Guide*.
- To expand a cluster (now) configured with DVS for Controller VM external communication, ensure that you do the following:
  - Expand DVS with the new node.
  - Make sure both the host and the CVM are configured with DVS.
  - Make sure that host to CVM and CVM to CVM communications are working.
  - Follow the cluster expansion procedure.
- After adding the new nodes, note the following:
  - The common Nutanix datastores are mounted on the new nodes by default after cluster expansion.
  - The target storage containers must be set to mount on the new hosts. You can check the mount status from the **Storage** dashboard. For more information, see Storage Table View in *Prism Element Web Console Guide*. Click the **Storage Container** tab, select the target storage container, click the **Update** button, and verify that **Mount on all ESXi Hosts** (or the new hosts are checked in **Mount/Unmount on the following ESXi Hosts**) is selected in the **NFS DATASTORE** field.
  - If an added node has an older processor class than the existing nodes in the cluster, cluster downtime is required to enable EVC (enhanced vMotion compatibility) with the lower feature set as the baseline. For an indication of the processor class of a node, see the **Block Serial** field in the **Hardware** dashboard. For more information, see Hardware Diagram View or Hardware Table View in *Prism Element Web Console Guide*. For more information on enabling EVC, see vSphere EVC Settings in the *vSphere Administration Guide for Acropolis*.

    Caution: If you mix processor classes without enabling EVC, vMotion/live migration of VMs is not supported between processor classes. If you add the host with the newer processor class to vCenter Server before enabling

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2903

EVC, cluster downtime is required to enable EVC later because all VMs (including the Controller VM) must be shut down.

- Add the new nodes to the appropriate vCenter Server cluster. If an added node has a newer processor class (for example, Haswell) than the existing nodes in the cluster (Ivy Bridge or Sandy Bridge), enable EVC with the lower feature set as the baseline before adding the node to vCenter.
- If you are adding multiple nodes to an existing EVC-enabled vCenter cluster, which requires powering off the Controller VM for each node to complete the addition, add just one node at a time and wait for data resiliency to return to *OK* before adding the next node to vCenter.

  Caution: Adding multiple nodes to vCenter simultaneously can cause a cluster outage when all the Controller VMs are powered off at the same time.

- If you are adding a node to a cluster where HA is enabled with APD and VMCP is enabled, you must enable APD and APD timeout on the new host.
- If you are adding new nodes to vCenter EVC configured cluster, ensure the following requirements.
  - Enabling EVC requires ESXi version 6.0 or above.
  - All ESXi nodes should be on same version and build.

Hyper-V Considerations

The following apply to clusters running Hyper-V:

- Network preparation is not supported. To bypass this step and prepare the nodes otherwise, click the **Skip Networking** button when you get to the **Networking** tab. In addition, imaging to AHV or ESXi is not possible if the node or base cluster is Hyper-V.
- If the Controller VMs in the cluster reside in a VLAN configured network, you must first configure the new nodes in the same VLAN before attempting to add them. Otherwise, the discovery process does not find these nodes. For more information about VLAN configuration instructions, see Discovering Nodes in a VLAN-Segmented Network in the *Field Installation Guide*.
- After adding the new nodes, if you manage your Hyper-V cluster by using Microsoft System Center VM Manager (SCVMM), do not use the Prism Element web console or Microsoft Failover Cluster Manager to add the new node to the failover cluster. Instead, use SCVMM to add the node to the Hyper-V cluster and then perform the following steps in the SCVMM user interface.
  1. Open the SCVMM user interface.
  2. Refresh the cluster in SCVMM. The new node is displayed under the failover cluster in the **Pending** state.
  3. Right-click the node and select **Add to host cluster**.
  4. Choose a run-as account that has the local administrator permissions on the new node.
  5. Click **OK**. The SCVMM agent is installed on the node and file shares are registered to the new node.
  6. Update the networking and other settings of the node to match your standard configuration.

For Microsoft Windows Server 2012 R2 deployments, after adding the node to the cluster in SCVMM, ensure that node disks are not added as clustered resources. Open the Failover Cluster Manager and click **Storage** > **Disks** to check.

Nutanix Clusters Considerations

The following apply to clusters hosted on a cloud platform:

- When expanding a cluster on AWS, the nodes are not added to the Cassandra ring (wait in a queue) until there are enough nodes to extend the ring. In addition, new nodes are added to the Cassandra ring only when they are do not break domain awareness. (Other services remain unaffected.)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2904

Hardware Considerations

Note the following when it applies to the nodes you are adding:

- Ensure that you use the minimum version of Foundation required by your hardware platform. To determine whether Foundation needs an upgrade for a hardware platform, see the respective system specifications guide. If the nodes you want to include in the cluster are of different models, determine which of their minimum Foundation versions is the most recent version, and then upgrade Foundation on all the nodes to that version.
- When adding partially populated all-SSD nodes to an existing cluster, the minimum number of partially populated all-SSD nodes added must be equal to the maximum RF in the cluster.
- If you are adding a node with a different processor class to the cluster, ensure that there are no running VMs on the node and the host has the following configuration:
  - ESXi: Verify that EVC is enabled on the cluster.
  - Hyper-V: If you want to move the VMs between the nodes, ensure that you have selected the **Migrate to a physical computer with a different processor version** option for each VM by browsing to **Settings** > **Processor** > **Compatibility** in the **Action** pane of the Hyper-V Manager.

    Note: Do not shut down more than one Controller VM at the same time.
- If you expand a cluster by adding a node with older generation hardware to a cluster that was initially created with later generation hardware, power cycle (do not reboot) any guest VMs before migrating them to the added older generation node or before upgrading the cluster.

  Guest VMs are migrated during hypervisor and firmware upgrades (but not AOS upgrades).

  For example, if you are adding a node with G4 Haswell CPUs to a cluster that also has newer G5 nodes with Broadwell CPUs, you must power cycle guest VMs hosted on the G5 nodes before you can migrate the VMs to the node with G4 CPUs. Power cycling the guest VMs enables them to discover a CPU set compatible with older G4 processors.

  In rare cases, certain CPU features might be deprecated in the new generation of CPUs. For example, Intel introduced MPX in Skylake class of CPUs and deprecated it with Ice Lake. In such cases, introduction of Ice Lake (newer) CPUs to an all-Skylake cluster can cause problems with existing VMs that are running with MPX. Such VMs must be power cycled.

  Power cycle guest VMs from the Prism Element web console VM dashboard. Do not perform a Guest Reboot; a VM power cycle is required in this case.
- If you physically add a node to a block (for example, a single node shipped from Nutanix is placed into an empty slot in an existing chassis), log on to the Controller VM for that node, and update the following parameters in the /etc/nutanix/factory_config.json file:
  - rackable_unit_serial: Set it to the same value as the other Controller VMs in the same block.
  - node_position: Set it to the physical location of the node in the block (A, B, C, D).

  After changing the configuration file, restart Genesis with the `genesis restart` command.

Limitations for Expanding a Cluster through Prism Central

Consider the following limitations before you expand a cluster through Prism central.

- Encryption and Rack Awareness functionalities are not yet supported for expanding a cluster through Prism Central.
- Expand cluster functionality does not have an option to upload the hypervisor image through Prism Central web console. If there is a version mismatch between the new host and ESXi or Hyper-V cluster, you are prompted to

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2905

upload the ISO in the ~/software_downloads/hypervisor_installer directory in any one CVM of the cluster using wget command, and enter the file details in the Prism Central web console.

Removing a Node through Prism Central

You can remove a node from a cluster using Prism Central.

Before you begin

Review Prerequisites for Removing a Node through Prism Central on page 435 before attempting to remove a node from a cluster.

About this task

From Prism Central version pc.2024.3 onwards, you can remove a node without registering the hosting cluster with Prism Central. The minimum supported version to remove a host using Prism Central web console is pc.2023.3.

To remove a host from a cluster using Prism Central web console, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Hardware** > **Hosts** .
   The system displays the **List** tab by default with all the hosts across registered clusters.
3. Select the target host checkbox, and choose **Remove Host** from the **Actions** dropdown menu.
   The system displays the **Remove Host** window. As a result of successful execution of remove host operation, the host gets detached from the cluster and the VMs on the selected host are migrated to other hosts. Some VMs might be automatically powered off due to lack of resources.
4. In the **Remove host** window, click **Run Precheck** to run the prechecks for remove host operation. The system checks several points including the space availability for VMs of the node to be removed, fault tolerance, upgrade status on the node. If any of the prechecks fail, fix the issue and then click **Remove** to remove the host.
   You can verify the progress of the remove host operation under recent tasks list.

   Caution: Do not shut down the CVM or put the CVM into maintenance mode while the node removal is in progress.

Prerequisites for Removing a Node through Prism Central

Consider the following set of prerequisites before you remove a node from a cluster:

- For information about reclaiming or rebalancing your cluster licenses after node removal, see the License Manager Guide.
- Removing a node (host) takes some time because data on that node must be migrated to other nodes before it can be removed from the cluster. You can monitor progress through the dashboard messages. Removing a node implicitly removes all the disks in that node.
- (Hyper-V only) Initiating a removal of a node running Hyper-V fails if the node is running as a part of a Hyper-V failover cluster and the following message appears.

  ```
  Node node id is a part of a Hyper-V failover cluster failover cluster name. Please
   drain all the roles, remove the node from the failover cluster and then mark the
   node for removal.
  ```

  If this message is displayed in either nCLI or in web interface, as a cluster administrator, you must use the management tools provided by Microsoft such as *Failover Cluster Manager* to drain all the highly-available

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2906

roles off the node. Then remove the node from the failover cluster followed by removing the node from the AOS cluster.

- (ESXi only) Before removing the node, ensure that there are no guest VMs running on the respective ESXi host. Note that CVM should be running on the node to initiate the node removal.
- (ESXi only) Temporarily disable DRS on the cluster before the node removal. The DRS must be re-enabled after the node is removed. Update the HA configuration to exclude the node you want to remove.
- (ESXi only) As a cluster administrator, you must use the management tools provided by VMware to first migrate all the guest VMs off the node/host, then remove the node from the AOS cluster of ESXi hosts. After that disconnect and remove the node (host) from the vCenter server.

  Caution: Ensure that you migrate the guest VMs before removing a host or node. Verify that the target cluster has enough available compute capacity before actually migrating the VMs. Removing a node or host without first migrating the guest VMs may result in loss of service.

  1. Migrate the guest VMs that need to be migrated.
  2. Click **Remove Host** from Prism.
  3. After successful removal from the AOS cluster, put the host in maintenance mode.

     Caution: When you put the host in maintenance mode, the maintenance mode process powers down or migrates all the VMs that are running on the host.

     For more information, see Node Maintenance in the *vSphere Administration Guide for Acropolis*.
  4. Remove the host from the vCenter server.

Limitations for Removing a Node through Prism Central

Consider the following limitations before you remove a node from a cluster.

- For a cluster with 1N/1D fault tolerance, the minimum number of nodes to support node removal is four. You cannot remove a node from a cluster that has less than four nodes.
- For a cluster with 2N/2D fault tolerance, the minimum number of nodes to support node removal is five. You cannot remove a node from a cluster with 2N/2D fault tolerance if it has less than five nodes.
- You can remove only one node at a time.

Putting a Host into Maintenance Mode Using Prism Central

This section describes how to put the host into maintenance mode using Prism Central.

Before you begin

Ensure that the following prerequisites are met before you put a host in maintenance mode:

- All the hosts are running, and no host in the cluster is in maintenance mode or undergoing existing maintenance mode operation.
- The cluster comprises at least two hosts.
- The selected host uses the AHV or ESXi hypervisor only.
- The **Data Resiliency** status of the cluster is **OK.** For more information, see Clusters Summary View on page 398.

About this task

You can put only one host of the cluster in maintenance mode from Prism Central at a time.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2907

> **Note:** If you put the ESXi host in maintenance mode using vCenter, Prism Central does not show the host maintenance mode status.

As the host enters the maintenance mode, the following high-level tasks are performed internally:

- The AHV host initiates the maintenance mode process.
- The HA VMs are live migrated.
- The system prompts the user to confirm the shut down action for pinned VMs and for VMs with replication factor 1.
- The AHV host completes the maintenance mode process.

  > **Note:** At this stage, the AHV host is not shut down.

- The CVM enters the maintenance mode.
- The CVM shuts down.

Procedure

To put the node into maintenance mode, follow these steps:

1. Log on to Prism Central.
2. From the Application Switcher Function, select the **Infrastructure** application, and navigate through the **Navigation Bar** to **Hardware** > **Hosts**.

   For information about the **Navigation Bar**, see Application-specific Navigation Bar.

   The system displays the **List** tab with all the hosts across registered clusters.
3. Select the target host checkbox and from the **Actions** dropdown menu, choose **Enter Maintenance Mode**.
   The system displays the **Host Maintenance** window and performs the checks to identify if there are any non-migratable VMs on the host.

   > **Note:** For the ESXi cluster, the system prompts you to enter the vCenter credentials before it performs any check to identify the non-migratable VMs in the cluster. After you enter the vCenter credentials, the system prompts you to perform the following actions based on the VM condition:
   >
   > - Non-migratable VMs: The system prompts you to shut down the non-migratable VMs. Select the **Power off VMs that cannot migrate (x unmigratable VMs)** checkbox.
   > - No non-migratable VMs: The system prompts you to confirm the enter maintenance mode action.
   >
   >   > **Note:** Click **View these x VMs** to display the list of non-migratable VMs. x indicates the number of non-migratable VMs
   >
   > For more information on the conditions that impact VM live migration, see VM Live Migration Restrictions in the *AHV Administration Guide*.

4. Click **Enter Maintenance Mode.**
   The system puts the host in maintenance mode. You can check the status of the **Enter Maintenance Mode** operation from the **Tasks** page. For more information, see Tasks View on page 452.

Exiting a Host from Maintenance Mode Using Prism Central

This section describes how to exit the host from maintenance mode using Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2908

About this task

You can exit maintenance mode from Prism Central only if you have put the host in maintenance mode from Prism Central or Prism Element.

> **Note:**
>
> - If you put the host in maintenance mode using aCLI (for AHV host) or using vCenter (for ESXi host), you cannot exit the maintenance mode from Prism Central.
> - If you put the ESXi host in maintenance mode using vCenter, Prism Central does not show the host maintenance mode status.

As the host exits the maintenance mode, the following high-level tasks are performed internally:

- The CVM is powered on.
- The CVM is taken out of maintenance mode.
- The host is taken out of maintenance mode.

> **Note:** The AHV host is shut down while Putting a Host into Maintenance Mode Using Prism Central on page 436 and you must start the AHV host. For information on how to start the AHV host, see Starting a Node in a Cluster (AHV) in *AHV Administration Guide*.
>
> After the host exits the maintenance mode, the VMs with replication factor 1 continue to be powered on and the VMs migrate to restore the host locality.

Procedure

To exit the node from maintenance mode, follow these steps:

1. Log on to Prism Central.
2. From the Application Switcher Function, select the **Infrastructure** application, and navigate through the **Navigation Bar** to **Hardware** > **Hosts**.

   For information about the **Navigation Bar**, see Application-specific Navigation Bar.

   The system displays the **List** tab with all the hosts across registered clusters.
3. Select the target host checkbox and from the **Actions** dropdown menu, choose **Exit Maintenance Mode**.
   The system displays the **Host Maintenance** window and prompts you to confirm the exit maintenance mode action.
4. Click **Exit Maintenance Mode.**
   The system exits the host from maintenance mode. You can check the status of the **Exit Maintenance Mode** operation from the **Tasks** page. For more information, see Tasks View on page 452.

Disks Summary View

Summary View of All Disks

The **Summary** tab on the **Disks** page provides a dashboard of the disks across all the registered clusters.

To access the **Summary** view of all the disks:

1. Log in to Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2909

2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Hardware** > **Disks** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
3. Click the **Summary** tab. The system displays **Summary** page for all the disks.

Clicking the **Summary** tab displays the following three widgets:

- **Highlighted Entities**: Displays a list of the disks with the highest usage of the parameter you select from the dropdown menu on the right of the widget. The options are **IO Bandwidth**, **IOPS**, **IO Latency**, and **Disk Usage**. Click the **View all XX Disks** link at the bottom to display the **List** tab (following section).
- **Alert**: Displays a list of disk-related alerts that occurred during the specified interval. Select either **Last 24 hours** (default) or **Last week** from the dropdown menu.
- **Anomalies**: Displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified interval. Select either **Last 24 hours** (default) or **Last week** from the dropdown menu. When an anomaly appears, you can click on the graph, which then displays a list of those anomalies. Clicking on an anomaly displays the event page for that anomaly.

Detailed View of an Individual Disk

For information about how to access the detailed view of an individual host, see Disk Details View on page 442.

List Tab

Clicking the **List** tab, which appears by default when you first open the page, displays a list of the disks across the registered clusters. The following table describes the fields that appear in the disks list. The fields vary based on the **Focus** menu selection, which is either **General** or **Performance**. A dash (-) is displayed in a field when a value is not available or applicable.

Table 115: Disks List Fields

Parameter	Description	Values
General Focus Fields		
Serial Number	Displays the disk serial number.	(serial number)
Host	Displays the name of the host in which this disk resides.	(host name)
Tier	Displays the disk type (tier name). Nutanix models can contain disk tiers for PCIe solid state disks (SSD-PCIe), SATA solid state disks (SSD-SATA), and direct attach SATA hard disk drives (DAS-SATA) depending on the model type.	[SSD-PCIe | SSD-SATA | DAS-SATA]
Mode	Displays the operating state of the disk.	online, offline
Disk Usage	Displays the percentage of disk space used and total capacity of this disk.	[0 - 100%] of xxx [GB| TB]
Cluster	Displays the name of the cluster in which the host resides.	(cluster name)
Performance Focus Fields		
Serial Number	Displays the disk serial number.	(serial number)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2910

Parameter	Description	Values
Disk Usage	Displays the percentage of disk space used and total capacity of this disk.	[0 - 100%] of xxx [GB|TB]
Disk Capacity	Displays the total physical space on the drive.	xxx [GB|TB]
IOPS	Displays I/O operations per second (IOPS) for this disk.	[0 - unlimited]
IO Bandwidth	Displays I/O bandwidth used per second for this disk.	xxx [MBps|KBps]
IO Latency	Displays the average I/O latency (in milliseconds) for this disk.	xxx [ms]
Cluster	Displays the name of the cluster in which the disk resides.	(cluster name)

You can filter the disks list based on a variety of parameter values. The following table describes the filter options available when you open the **Filter** pane. To apply a filter, select a parameter and check the box of the desired value (or multiple values) you want to use as a filter. You can apply filters across multiple parameters. Some parameter filters require additional context such as a constraint string or a range.

Table 116: Filter Pane Fields

Parameter	Description	Values
Serial Number	Filters on the disk serial number. Select a condition from the dropdown list (**Contains**, **Doesn't contain**, **Starts with**, **Ends with**, or **Equal to**) and enter a string in the field. It will return a list of disks that satisfy the serial number condition/string.	(serial number string)
Host	Filters on the host name. Enter a string in the field. It will return a list of disks in the hosts that satisfy the host name condition/string.	(host name string)
Cluster	Filters on the cluster name. Enter a string in the field. It will return a list of disks in the clusters that satisfy the cluster name condition/string.	(cluster name string)
Mode	Filters on whether the disk is online or offline. Check the box for one or both of these modes. The number of disks currently in each state is displayed on the right of the line.	Online, Offline
Tier	Filters on whether the disk is in the solid state (SSD-SATA) or hard disk (DAS-SATA) tier. Check the box for one or both of these modes. The number of disks currently in each tier is displayed on the right of the line.	DAS-SATA, SSD-SATA
Health	Filters on the disk health state (good, warning, or critical). Select one or more states to return a list of disks in that state(s). The number of disks currently in each state is displayed on the right of the line.	Critical, Warning, Good

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2911

Parameter	Description	Values
Disk Usage	Filters on the used capacity. Enter a percentage range in the "**from <low> to <high> %**" field. It will return a list of disks with used capacity in that range (0-100%).	([xx] to [yy]% range)
Disk Capacity	Filters on the total capacity. Enter an amount range in the "**from <low> to <high> GiB**" field. It will return a list of disks with total capacity in that range.	([xx] to [yy] GiB range)
IOPS	Filters on the IOPS. Enter a range in the "**from <low> to <high> iops**" field. It will return a list of disks with IOPS in that range.	([xx] to [yy] range)
IO Bandwidth	Filters on the I/O bandwidth used. Enter a range in the "**from <low> to <high> bps**" field. It will return a list of disks with I/O bandwidth usage in that range.	([xx] to [yy] range)
IO Latency	Filters on the average I/O latency. Enter a range in the "**from <low> to <high> ms**" field. It will return a list of disks with average I/O latency in that range.	([xx] to [yy] range)

You can group the disks list in the following ways:

- The **Color** dropdown menu allows you to color code the disk entries by tier type, mode, or health state. (You can only choose one.) A legend appears at the bottom to indicate what each color means in that grouping.
- The **Group** dropdown menu allows you to group the disk entries by host, tier type, mode, cluster, or health state. (You can only choose one.)
- [Tiles and Circles views only] The **Sort** dropdown menu allows you to group the disk entries by the information parameters (fields), which vary depending on whether you selected the **General** or **Performance** focus. (You can only choose one parameter.)

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options as the Alerts dashboard, except it is filtered to display just disk-related alerts across the registered clusters. For more information, see Alerts Summary View (Prism Central) in *Prism Central Alerts and Events Reference Guide*.

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options as the Events dashboard, except it is filtered to display just disk-related events across the registered clusters. For more information, see Events Summary View (Prism Central) in *Prism Central Alerts and Events Reference Guide*.

Metrics Tab

The **Metrics** tab allows you to view usage metrics across the hosts. Clicking the **Metrics** tab displays a list of available metrics; click the metric name to display the relevant information to the right. The following table describes the available metrics.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2912

Table 117: Metrics Tab Fields

Metric	Description
IOPS	Displays total, read, and write IOPS tables listing current values and total disks (number). The current values are split into intervals (for example, less than 20, 20-40, 40-60, more than 60). Clicking on an interval displays the Summary tab filtered to just those disk. **Note:** The same format also applies to the other metrics in this table.
IO Latency	Displays total, read, and write I/O latency rate tables.
IO Bandwidth	Displays total, read, and write I/O bandwidth rate tables.

Disk Details View

Summary Tab

The **Summary** tab of an individual disk consists of a dashboard that provides the detailed information about the disk.

To access the **Summary** tab of an individual disk:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Hardware** > **Disks** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   By default, the system displays the **List** tab with all the disks.
3. Click the target <*disk_name*> to view the **Summary** tab of an individual disk.

   Note: Replace <*disk_name*> with the actual host name at your site.

Summary Tab

The **Summary** tab of an individual disk provides the following widgets:

- A **Properties** widget that displays summary information about the disk. For more information, see the Table 118: Disk Properties Fields on page 442 table.
- An **Alert** widget that displays a list of related alerts that occurred during the specified interval. Select either **Last 24 hours** (default) or **Last week** from the dropdown menu.
- An **Anomalies** widget that displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified interval. Select either **Last 24 hours** (default) or **Last week** from the dropdown menu. When an anomaly appears, you can click on the graph, which then displays a list of those anomalies. Clicking on an anomaly displays the event page for that anomaly.

The following table describes the fields in the **Properties** widget. A dash (-) in a field indicates there is not enough data to evaluate or a value is not assigned. The displayed fields vary by hypervisor.

Table 118: Disk Properties Fields

Parameter	Description	Values
Disk Usage	Displays the amount of used space on the drive.	xxx [GB|TB]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2913

Parameter	Description	Values
Cluster	Displays the name of the cluster in which the disk resides.	(cluster name)
Host	Displays the name of the host in which the disk resides.	(host name)
Host IP	Displays the IP address of the host.	(IP address)
Tier	Displays the disk type (tier name). Nutanix models can contain disk tiers for PCIe solid state disks (SSD-PCIe), SATA solid state disks (SSD-SATA), and direct attach SATA hard disk drives (DAS-SATA) depending on the model type.	[SSD-PCIe | SSD-SATA | DAS-SATA]
Mode	Displays whether the disk is currently online or offline.	[online|offline]
Disk Capacity	Displays the total physical space on the drive.	xxx [GB|TB]
Status	Displays the operating status of the disk. Possible states include the following: • **Normal**. Disk is operating normally. • **Data migration initiated**. Data is being migrated to other disks. • **Marked for removal, data migration is in progress**. Data is being migrated in preparation to remove disk. • **Detachable**. Disk is not being used and can be removed.	Normal; Data migration initiated; Marked for removal, data migration is in progress; Detachable
Self Encryption Drive	Displays whether this is a self-encrypted drive.	Not Present, Present

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options as the Alerts dashboard, except it is filtered to display just alerts for this disk. For more information, see Alerts Summary View (Prism Central) in *Prism Central Alerts and Events Reference Guide*.

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options as the Events dashboard, except it is filtered to display just events for this disk. For more information, see Events Summary View (Prism Central) in *Prism Central Alerts and Events Reference Guide*

Metrics Tab

The **Metrics** tab allows you to view usage metrics for the disk. Click the **Metrics** tab and then the desired metric name (**IOPS**, **IO latency**, and **IO Bandwidth**) to display a graph for that metric on the right. The graph is a rolling time interval performance or usage monitor. The baseline range (based on the machine-learning algorithm) appears as a blue band in the graph.

> **Note:** The machine-learning algorithm uses 21 days of data to monitor and predict performance. A graph or baseline band may not appear if less than 21 days of data is available.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2914

- Check the appropriate box(es) to have the graph display total, read, or write usage (or any combination of the three).
- Place the cursor anywhere on the horizontal axis to display the value at that time.
- Select the duration (time interval) from the dropdown list on the right (last 1 hour, last 24 hours, last week, last 21 days).
- Click **Alert Settings** to configure an alert for this metric. For more information, see Creating Custom Alert Policies in *Prism Central Alerts and Events Reference Guide*.

Storage Usage Tab

The **Usage** tab displays the following graph:

- The **Usage Summary** graph displays a rolling time interval monitor of disk storage usage that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in depth analysis, you can add the monitor to the analysis page by clicking the blue link in the upper right of the graph.

GPUs Summary View

Summary View of All GPUs

The **Summary** tab on the **GPUs** page provides a dashboard of the GPUs across all the registered clusters.

To access the **Summary** view of all the GPUs:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Hardware** > **GPUs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
3. Click the **Summary** tab.

   The system displays **Summary** page for all the GPUs.

The following table describes the fields that appear in the GPUs list. A dash (-) is displayed in a field when a value is not available or applicable.

Table 119: GPU List Fields

Parameter	Description	Values
Type	Displays the GPU model type.	Tesla M10, Tesla M60, Tesla M60 compute
Cluster	Displays the name of the cluster in which the GPU resides.	(cluster name)
Mode	Displays the mode in which the GPU is operating.	None, vGPU, passthrough
Allocation	Indicates the number of VMs allocated to the GPU.	"No VM allocated", "*x* of *y* VMs allocated"

You can filter the GPUs list based on several parameter values. The following table describes the filter options available when you open the GPUs view **Filter** pane. To apply a filter, select a parameter and check the box of the

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2915

desired value (or multiple values) you want to use as a filter. You can apply filters across multiple parameters. Some parameter filters require additional context such as a constraint string or a range.

Table 120: Filter Pane Fields

Parameter	Description	Values
Type	Filters on the GPU model type. Select a condition from the dropdown menu (**Contains**, **Doesn't contain**, **Starts with**, **Ends with**, or **Equal to**) and enter a string in the field. It returns a list of GPUs that satisfy the type condition/string.	Tesla M10, Tesla M60, Tesla M60 compute
Host	Filters on the host name. Enter a string in the field. It returns a list of GPUs in the selected hosts.	(host name string)
Cluster	Filters on the cluster name. Enter a string in the field. It returns a list of GPUs in the selected clusters.	(cluster name string)
Mode	Filters on the GPU operation mode. Check the box for one or more of these modes. The number of GPUs currently in each mode is displayed on the right of the line.	None, vGPU, Passthrough

You can group the GPUs list in the following ways:

- The **Group** dropdown menu allows you to group the GPU entries by cluster, host, or mode. (you can only choose one.)
- The **Sort** dropdown menu allows you to group the GPU entries by type, cluster, mode, or allocation. (you can only choose one parameter.)

Clicking the **Summary** tab displays the following three widgets:

- **Highlighted Entities**: Displays a list of the disks with the highest usage of the parameter you select from the dropdown menu on the right of the widget. The options are **IO Bandwidth**, **IOPS**, **IO Latency**, and **Disk Usage**. Click the **View all XX Disks** link at the bottom to display the **List** tab (following section).
- **Alert**: Displays a list of disk-related alerts that occurred during the specified interval. Select either **Last 24 hours** (default) or **Last week** from the dropdown menu.
- **Anomalies**: Displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified interval. Select either **Last 24 hours** (default) or **Last week** from the dropdown menu. When an anomaly appears, you can click on the graph, which then displays a list of those anomalies. Clicking on an anomaly displays the event page for that anomaly.

Detailed View of an Individual GPU

For information about how to access the detailed view of an individual host, see GPU Details View on page 445.

GPU Details View

Summary Tab

The **Summary** tab of a GPU consists of a dashboard that provides the detailed information about the GPU.

To access the **Summary** tab of an individual GPU:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2916

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Hardware** > **GPUs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   By default, the system displays the **List** tab with GPUs across all the registered clusters.
3. Click the target <*GPU_name*> to view the **Summary** tab of an individual GPU.

   Note: Replace <*GPU_name*> with the actual GPU name at your site.

Clicking the **Summary** tab displays the following:

- A section on the left that displays summary information about the GPU. For more information, see the Table 121: GPU Summary Fields on page 446 table.
- A section of the right that displays GPU performance metrics. The graphs are rolling time interval performance monitors that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. This section includes the following graphs:
  - **GPU Usage**: Displays the percentage of GPU capacity being used.
  - **GPU Framebuffer Usage**: Displays the percentage of GPU framebuffer (RAM) capacity being used.
- **Action** on the upper right (which appears regardless of which tab is selected):
  - Click the Help icon to open a help page in a separate tab or window.
  - Click the X icon to close the details page.

The following table describes the GPU summary information fields. A dash (-) is displayed in a field when a value is not available or applicable.

Table 121: GPU Summary Fields

Parameter	Description	Values
GPU Type	Displays the GPU type for this entry.	Tesla M10, Tesla M60, Tesla M60 compute
Cluster Name	Displays the name of the cluster in which the GPU resides.	(cluster name)
Host	Displays the name of the host in which the GPU resides.	(host name)
Mode	Displays the GPU operational mode. If it is vGPU, an additional field appears that displays the vGPU profile used.	None, vGPU, Passthrough
Allocation	Displays the number of VMs allocated to this GPU. This field does not appear if no VMs are allocated.	"*x* of *y* VMs allocated"
Framebuffer (RAM) Per GPU	Displays the framebuffer (RAM) size per GPU.	xx GiB
ID	Displays the GPU ID number.	(ID number)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2917

VMs Tab

Clicking the **VMs** tab displays a table of VMs allocated (attached) to the GPU. The table includes the following fields:

- **Name**: Displays the VM name. Click the name to display the details page for that VM. For more information, see VM Details View on page 117.
- **GPU Usage**: Displays the percentage of GPU capacity used by this VM.
- **GPU Framebuffer Usage**: Displays the percentage of GPU framebuffer (RAM) capacity used by this VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2918

ACTIVITY ENTITIES – ALERT AND EVENT MONITORING

For information about Alerts and Events in Prism Central, see Prism Central Alerts and Events Reference Guide.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2919

ACTIVITY ENTITIES – TASKS AND AUDITS

You can access dashboards for the following activity monitors from the **Activity** entity of the **Infrastructure** application. For information about how to access the entity items available in **Activity** entity, see Application-specific Navigation Bar on page 66.

- Audits (see Audits Summary View on page 449)
- Tasks (see Tasks View on page 452)

Audits Summary View

The **Audits** summary view provides a dashboard of the actions performed across the registered clusters.

> **Note:**
>
> - The retention period for audit entries is four weeks by default.
> - Audit information appears only for those registered clusters running AOS 5.10 or later.
> - Audit logs with default values are generated when updates to VMs are initiated, either by Prism Central **Self Service** users or by using Nutanix v3 API calls for the first time.
> - For all Prism Central related events, see Prism Central Logs in *Prism Central Alerts and Events Reference Guide*. Additionally, you can refer to the Audit Log Events in *Prism Central Alerts and Events Reference Guide* for the complete list of captured audit events.

To access the **Audits** summary view, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Activity** > **Audits** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The system displays the **Audits** dashboard.

The following table describes the fields that appear in the audits list. A dash (-) is displayed in a field when a value is not available or applicable.

Table 122: Recovery Plans Fields

Parameter	Description	Values
Action Description	Describes the action taken such as "deleted VM `vm-name`" or "added disk `disk-name`"	(action description)
User Name	Displays the name of the user who requested the action.	(user name)
Entity Affected	Displays the entity name. Click the name to go to the details page for that entity.	(entity name)
Entity Type	Displays the entity type such as VM or host.	(entity type)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2920

Parameter	Description	Values
Operation Type	Displays the type of operation that took place. The possible operation types depend on the entity type and can include create, update, delete, and power state change.	(operation type)
Request Time	Displays the time the user requested the action.	(time and date)
Cluster	Displays the name of the cluster in which the action took place. Click the cluster name to display the details page for that cluster.	(cluster name)

To filter the list, click **Modify Filters** (upper right). This displays a pane for selecting filter values. The following table describes the filter options available. You can apply multiple filters together. For example, if you want to filter by a particular VM name, you can filter by *entity type = VM* and then use the *name contains* filter.

Table 123: Filter Pane Fields

Field	Description	Values
User IP	Enter a user IP address and then click **Add** to filter for actions requested by that user. You can add multiple user IP addresses.	(IP address)
Cluster	Enter a cluster name in the field to filter for actions in the cluster.	(cluster name)
Entity Type	Check the boxes of one or more entities to filter for actions on those entity types.	VM, Storage Container, Catalog Item, Image, Cluster, Host, Disk, GPU, Security Policy, NGT Policy, Project, Role, User, Category, Availability Zone, Protection Policy, Recovery Plan, Recoverable Entity, Report
Operation Type	Check the boxes of one or more operations to filter on those operations.	Create, Update, Delete, Power State Change
Request Time	Check an interval box to filter for actions that were requested during that time period. For the custom interval option (**from** *xxx* **to** *xxx*), click in each field and select a date from the pop-up calendar.	Last 1 hour, Last 24 hours, Last week, From *xxx* to *xxx*
Cluster	Enter a cluster name in the field to filter for actions in the cluster. **Note:** Entering *Prism Central* in the cluster filter criteria does not populate any result.	(cluster name)
User IP	Enter a user IP address and then click the **Add** to filter for actions requested by that user. You can add multiple user IP addresses.	(IP address)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2921

Audit Details View

The details page of an individual action provides the detailed information about the action.

To access the details page of an action:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Activity** > **Audits** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
3. Click the target <*action_name*> to view the details page of an individual action.

> **Note:** Replace <*action_name*> with the actual action description at your site.

The details page includes the following:

- The action description (upper left). You can switch from one action details page to another by selecting from the dropdown list.
- A section on the left that displays summary information about the action (see following table).
- A section on the right that displays a table of information specific to that action. The table shows the attributes that were changed during the action and the current value that is set for the attribute. The attributes vary depending on the specifics of the action (see following examples).

The following table describes the action summary information fields. A dash (-) is displayed in a field when a value is not available or applicable.

Table 124: Action Summary Fields

Parameter	Description	Values
Action Description	Displays the action description.	(description)
User Name	Displays the name of the user who requested the action.	(user name)
Target Entity	Displays the name of the entity that was the action target. Click the entity name to display the details for that entity.	(entity name)
Affected Entities	Displays the names of the entities that were affected by the action. Click an entity name to displays the details page for that entity.	(one or more entity names)
Operation Type	Displays the type of operation that took place. The possible operation types depend on the entity type and can include create, update, delete, and power state change.	(operation type)
Request Time	Displays the time the user requested the action.	(time and date)
User IP	Displays the IP address of the user.	(IP address)
Cluster	Displays the name of the cluster in which the action took place. Click the cluster name to display the details page for that cluster.	(cluster name)
Status	Displays the status of the action.	Succeeded, Failed

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2922

Tasks View

The **Tasks** page provides a dashboard that displays information about all tasks across the registered clusters. You can view a task if you have the view permission for any one of the clusters affected by the task.

> **Note:** Prism Central version pc.2024.3 introduces an enhanced **Tasks** dashboard. You can access this enhanced dashboard only if all the connected Prism Element clusters are upgraded to version 7.0.

To access the **Tasks** dashboard:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Activity** > **Tasks** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
3. The system displays the **Tasks** dashboard.

An icon appears in the main menu when there are current tasks (running or completed within the last 48 hours). The icon appears blue when a task runs normally, yellow when it generates a warning, or red when it fails. Clicking the icon displays a dropdown menu of current tasks.

You can see the tasks dashboard by doing one of the following:

- Clicking the **View All Tasks** link at the bottom of the current tasks dropdown menu.
- Clicking the **View All Tasks** link in the Tasks widget in the main dashboard.
- Selecting **Activity** > **Tasks** from the **Navigation Bar**.

The following table describes the fields on the tasks page. Each task appears on the list for a minimum of one hour after completion. The duration for which a task stays on the list varies based on several factors. However, tasks may be removed from the list sooner when new tasks are added, especially during periods of high activity. In some instances, a task may remain visible for longer than two weeks if it is the last task associated with a specific component.

Table 125: Tasks List Fields

Parameter	Description	Values
Task	Specifies which type of operation the task is performing. The number of child tasks are also displayed in this column, if applicable.	(name of operation such as garbage collection of logs)
Entity Affected	Lists the entity name or entity UUID. If this is a live link, click it to either see more details or go to the entity details page. If multiple entities are affected, only upto five entities are displayed under this column.	(name or description)
Cluster	Specifies the cluster name(s) on which the task is running. A dash (-) appears when the task applies to Prism Central rather than one of the registered clusters.	(cluster names)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2923

Parameter	Description	Values
Status	Indicates the status of the task: • Canceled: The task has been canceled by a user. • Canceling: The task cancellation has been initiated by a user, but cancellation is yet to be completed. • Failed: The task has failed. • Queued: The task has been queued by the system. • Running: The task is running. The progress percentage is displayed for the running tasks. • Succeeded: The task has succeeded. • Suspended: The task has been suspended by the system.	Cancelled, Canceling, Failed, Queued, Running, Succeeded, Suspended
Initiator	Indicates the user who initiated the task.	(user name)
Start Time	Displays when the task began.	[date],[time]
Duration	Displays how long the task has been running or took to complete.	xx [seconds| minutes| hours| days]

When you select a task, a side panel appears at the right side, displaying the details of the task, such as:

- Overall status of the task
- Names of all the entities affected (a maximum of 300 entities can be displayed in the side pane)
- Cluster
- Initiator (user who initiated the task)
- Duration of the task
- Details of the child tasks
- Brief description of the sub-steps included in the selected task (if applicable)
- Errors or warnings related to the task (if applicable)

You can do the following in the Tasks dashboard:

- Filter the list by entering a criteria in the filter field at the top of the page.
- Save your favorite filters.
- Filter the list by clicking **Modify Filters**. This displays a filter pane on the right of the screen. For more information, see Filters Pane - Tasks Page.
- Click the X icon to close the filter pane.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2924

- Export the entire task list or a filtered list in CSV format by clicking **Export**.

Filters Pane - Tasks Page

The following table describes the fields available in the **Filters** pane:

Table 126: Filter Pane Fields

Parameter	Description	Values
TASK	Filters based on task name. Select a condition from the dropdown menu (**Contains**, **Equal to**, **Not Equal to**, **Doesn't contain**, **Starts with**, **Ends with**), and enter a string in the field.	(task name)
ENTITIES AFFECTED	Filters based on the entities affected. Select a condition from the dropdown menu (**Contains**, **Equal to**, **Not Equal to**, **Doesn't contain**, **Starts with**, **Ends with**), and enter a string in the field.	(entities name string)
INITIATOR	Filters based on the initiator of the task. Select a condition from the dropdown menu (**Contains**, **Equal to**, **Not Equal to**, **Doesn't contain**, **Starts with**, **Ends with**), and enter a string in the field.	(initiator string)
CLUSTER	Filters based on the cluster name. Select a cluster name from the dropdown list to filter the result.	(cluster name)
STATUS	Filters based on the status of the task. Select one of more status from the list to filter the result.	(Canceled, Canceling, Failed, Queued, Running, Suspended, or Succeeded)
TIME RANGE	Filters based on the time range. Select date and time for **Start** and **End** fields.	(date and time)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2925

OPERATIONS ENTITIES

Starting from Prism Central version 2023.3, NCM Intelligent Operations (formerly AIOps) now has a new user interface. The following Operations Entities have been moved from Prism Central Infrastructure app to the new user interface created for NCM Intelligent Operations:

- Analysis
- App Discovery
- Monitoring Configurations
- Operations Policies
- Planning
- Playbooks
- Reports
- Settings and Configurations

The documentation for the above-mentioned entities has been moved to the newly created *Intelligent Operations Guide*. For more information, see Intelligent Operations Guide.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2926

ADMINISTRATION ENTITIES

You can manage the following entity items from the **Administration** entity of the **Infrastructure** application:

- Users, Roles, and Projects. For more information about how to manage users, roles, and projects in Prism Central, see Prism Central Admin Center Guide.
- LCM. For information about LCM, see LCM Documentation.
- Availability Zones. For information about Availability Zones in Prism Central, see Availability Zones on page 456.
- Categories. For information about how to manage Categories in Prism Central, see Category Management on page 456.

For information about how to access the entities items available in **Administration** entity, see Application-specific Navigation Bar on page 66.

Availability Zones

Nutanix Disaster Recovery works with sets of physically isolated locations called availability zones (AZs). For information about Availability Zones in Prism Central, see Nutanix Disaster Recovery Guide .

Category Management

A category is a grouping of entities into a key-value pair. Typically, new entities are assigned to a category based on some criteria. Policies can then be tied to those entities that are assigned (grouped by) a specific category value.

For example, you might have a Department category that includes values such as engineering, finance, and HR. In this case, you could create one backup policy that applies to engineering and HR and a separate (more stringent) backup policy that applies to just finance. Categories allow you to implement a variety of policies across entity groups, and Prism Central allows you to view any established relationships quickly.

The following hypothetical example illustrates the relationship of four policies (Backupbasic, Engenvironment, Hourly alerts, and Daily backup) tied to three departments (Eng, Fin, and HR) that apply to 30+ VMs in each department.

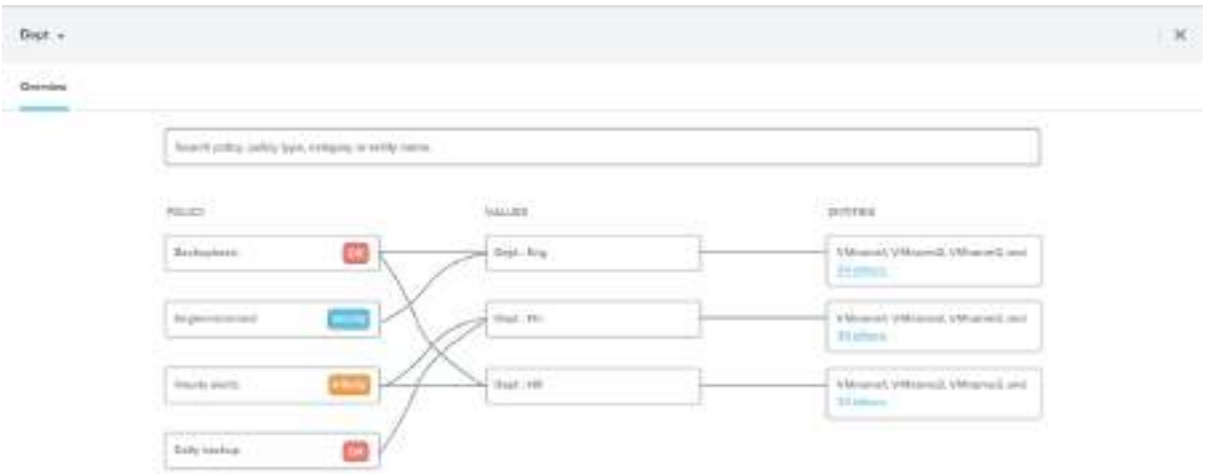


Figure 163: Dept Details View (example)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2927

Important:

The **Storage: $Default** category is used to assign the default storage policy to an entity such as a VM or a VG. You cannot associate any other storage policy with this category. Nutanix recommends that you do not associate any other policy with the **Storage: $Default** category or make any other changes to this category.

For more information on the default storage policy, see Default Storage Policy on page 509.

Categories Summary View

The **Categories** summary view provides a dashboard of the existing categories.

To access the **Categories** dashboard:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Administration** > **Categories** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
3. The system displays the **Categories** dashboard.

> **Note:** To view the categories, you must log in as a user with all the category permissions.

The following table describes the fields that appear in the categories list. A dash (-) is displayed in a field when a value is not available or applicable.

Table 127: Categories List Fields

Parameter	Description	Values
Name	Displays the name of the category.	(category name)
Value	Displays the values defined for the category. Click **Show more** (right of line) to see a line for each value. (Click**Show fewer** to collapse the list.) You may see an icon with a "showing X of Y" message to indicate there are additional values; click the icon to display the full list.	(value names)
Associated Entities	Lists the number of entities assigned to this category. **Note:** For a non-admin user, Prism Central displays the list of associated entities only when you expand the row. Prism Central does not display the cumulative list of associated entities for a non-admin user.	(number)
Associated Policies	Lists the number of policies assigned to this category.	(number)

You can filter the category list based on several parameter values. The following table describes the options available when you click **Modify Filters**, which displays the Categories view **Filters** pane. To apply a filter, select a parameter and check the box of the desired value (or multiple values) you want to use as a filter. You can apply filters across multiple parameters.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2928

Table 128: Filter Pane Fields

Parameter	Description	Values
Name	Filters on the category name. Select a condition from the dropdown list and enter a string in the field. It will return a list of categories that satisfy the name condition/string. **Note:** In this and the Value field, the condition menu options are **Contains**, **Does not contain**, **Starts with**, **Ends with**, and **Equal to**.	(name string)
Entities	Filters on the entity type. Check the box for one or more entity types.	VM, Host, App, Blueprint, Cluster, Image, Marketplace Item, Reports, Subnet
Policies	Filters on the policy type. Check the box for one or more entity types.	Security Policy, Affinity Policy, Image Placement Policy, NGT Policy, Protection Policy, QoS Policy

Click **New Category** to create a category. For more information, see Creating a Category on page 459.

Perform the following category-specific actions on a category using the **Actions** dropdown menu. The **Actions** dropdown appears when one or more categories are selected.

- **Update**: Click this action to modify an existing category. For more information, see Modifying a Category on page 460.
- **Delete**: Click this action to modify an existing category.

Category Details View

The details page of an individual category provides the detailed information about the category.

To access the details page of a category:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Administration** > **Categories** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
3. Click the target <*category_name*> to view the details page of an individual category.

   Note: Replace <*category_name*> with the actual category name at your site.

A category details page includes the following:

- Category name (upper left). You can switch from one category to another by selecting a different category name from the dropdown list in the upper left of the screen.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2929

- Action buttons (upper right).
  - Click **Update** to update the category definition. For more information, see Modifying a Category on page 460.
  - Click **Delete** to delete the category.

    The actions are grayed out if not allowed. For example, you cannot delete system categories.
  - Click the Help icon to open a help page in a separate tab or window.
  - Click the X icon to close the details page.
- **Policies** (left), **Values** (middle), and **Entities** (right) columns that list the values defined for the category plus the policies and entities associated with that category. The list does not include the policies that are associated with multiple categories. Placing the cursor over a policy, value, or entity displays lines that graphically indicate the association among the three parameters.

Creating a Category

About this task

To create a category, do the following:

Procedure

1. Log in to Prism Central.
2. Select **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Administration** > **Categories** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
3. Go to the categories dashboard and click **New Category**.
   The **Create Category** page appears.
4. Do the following in the indicated fields:
   a. **Name**: Enter a name for the new category.

      Note: The **Name** and **Values** fields are case sensitive.

   b. **Purpose** (optional): Enter a description of the category purpose.

   c. **Values**: Enter a category value. To add a second (and subsequent) value, click the plus sign (+) to the right. This opens another line; enter the next value in the new field.

      Repeat this step for all the values you want to include in the category. For example, if the category name is Departments, values might include Engineering, HR, Sales, Marketing, and so on.

      Duplicate values are discarded. Character case is considered when determining duplicates. For example, multiple instances of the value `Sales` are considered duplicates and all instances but one are dropped; the values `Sales` and `sales` are considered unique and are accepted.

   d. Click **Save**.

      This creates the category and closes the page. The new category now appears in the category list.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2930

Modifying a Category

About this task

You can update or delete a custom (user-defined) category. System (built-in) categories cannot be modified or deleted.

> **Note:** You cannot delete a category if it is used in an existing policy. All associations with existing policies must be removed before a category can be deleted.

To update or delete an existing category, do the following:

Procedure

1. Log in to Prism Central.
2. Select **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Administration** > **Categories** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
3. Go to the categories dashboard and select the desired category from the list.
4. Do one of the following:
   - » To modify that category, select **Update** from the **Actions** dropdown menu. The **Update Category** page appears, which includes the same fields as the **Create Category** page. For more information, see Creating a Category on page 459. Update the field values as desired and then click the **Save** button.
   - » To delete that category, select **Delete** from the **Actions** dropdown menu. You are prompted to verify the delete (click the **OK** button). The category is then deleted and removed from the list.

Assigning a Category

About this task

You can assign a category value to an entity of the following types: cluster, VM, host, volume group, catalog, image, report, subnet, blueprint, app, and marketplace item. To assign a category value to one or more entities, do the following:

Procedure

1. Log in to Prism Central.
2. Select **Infrastructure** application from Application Switcher Function on page 45, and navigate to the dashboard of the entity that you want to assign a category to.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2931

3. Select all the entities that you want to tag with the same category value.

   - Cluster: Go to the **List** tab in the clusters dashboard and select the checkboxes for the target clusters. For more information, see Clusters Summary View on page 398.
   - VM: Go to the **List** tab in the VMs dashboard and select the target VMs. For more information, see VMs Summary View on page 104.
   - Host: Go to the **List** tab in the hosts dashboard and select the target hosts. For more information, see Hosts Summary View on page 419.
   - Volume group: Go to the **List** tab in the volume groups dashboard and select the target volume groups. For more information, see Volume Groups Summary View on page 302.
   - Catalog: Go to the catalog items dashboard and select the target catalog items. For more information, see Catalog Items Summary View on page 266.
   - Image: Go to the **List** tab in the images dashboard and select the target images. For more information, see Images Summary View on page 243.
   - Report: Go to the reports dashboard and select the target reports. For more information, see Reports Summary View in *Intelligent Operations Guide*)
   - Subnet: Go to the subnets dashboard and select the target subnets. For more information, see Subnet Details View on page 344.
   - Blueprint, App, or Marketplace item: For information, see Marketplace Manager section of the *NCM Self-Service Administration and Operations Guide*.

4. Select **Manage Categories** from the **Actions** dropdown menu.
   This displays the **Manage [Cluster|VM|Image|Subnet] Categories** page.

Figure 164: Manage VM Categories Page

5. In the **Manage [Cluster|VM|Image|Subnet] Categories** page, do the following:

   a. Enter a category name in the **Set Categories** field, select the target value from the list, and then click the plus sign (+) to the right of the field to assign that category value to the selected entities.

      The **Set Categories** field acts like a search field; it provides a list of matching categories as you enter a string. Select the desired category value when you see it in the list. Any policies associated with the selected category value appear in the **Associated Polices** section to the right.

   b. Repeat the first step to assign a value for a second category.

      You can repeat this step for as many categories as desired. To illustrate, in the figure above the VMs are assigned two values, *AV* from the *Cluster* category and *Default* from the *Quarantine* category. In this example

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2932

Cluster:AV has no policies associated with it currently, but *Quarantine:Default* is associated with the Quarantine security policy.

> **Note:** Categories support multi-cardinality, which means you can assign multiple category values to the same entity. In this case you can assign multiple values to the same VM.

c. Click **Save** to save the category assignment.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2933

POLICIES IN INFRASTRUCTURE

This section describes the policies framework in Prism Central.

Policies are used to define the systematic configuration guidelines for the following requirements:

- Controlled management of **VMs**, **Images**, **Storage**, and **Network & Security** entities. For more information, see the following sections:
  - VM Policy Management on page 463 for VM-related policies.
  - Image Policy Management on page 487 for image-related policies.
  - Storage Policy Management on page 506 for storage-related policies.
  - Security Policy Management on page 501 for policies related to network security framework setup.
- System services customization. For more information, see Operations Policy Management in *Intelligent Operations Guide*.
- Disaster Recovery setup. For information about how to create the protection policies in Disaster Recovery setup, see Nutanix Disaster Recovery Guide.

VM Policy Management

In Prism Central, you can create and manage the following types of policies for the VMs:

- VM-Host Affinity Policies (see VM-Host Affinity Policies Defined in Prism Central on page 463)
- VM-VM Anti-Affinity Policies (see VM-VM Anti-Affinity Policies Defined in Prism Central on page 474)
- NGT Policies (see NGT Policies on page 484)

VM-Host Affinity Policies Defined in Prism Central

In Prism Central, you can define the category-based VM-Host affinity policies, where a set of VMs can be affined (correlated) to run only on a particular set of hosts. Category-based affinity policy enables you to easily manage affinities for a large number of VMs. In case of any changes to the affined hosts, you only need to update the category of the host, and it updates the affinity policy for all the affected VMs.

This policy checks and hard enforces where a VM can be hosted when you start or migrate the VM. If there are no resources available on any of the affined hosts, the VM is not started.

> **Note:**
>
> If you create a VM-Host affinity policy for a VM that is configured for asynchronous replication, you must create similar categories and corresponding policies on the remote site as well. If you define similar categories and policies on the remote site, the system applies the affinity policies when the VMs are migrated to the remote site.

For information on how the category-based VM-Host affinity policies are handled during disaster recovery, see Affinity Policies Handling - PC Based DR Solution with Physically Isolated Locations.

VM-Host Affinity Policies Summary View

The VM-Host affinity policies summary view enables you to access a list of all the user-defined affinity policies across registered clusters.

To access the summary view of all VM-Host affinity policies:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2934

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information on the **Navigation Bar**, see Application-specific Navigation Bar.

   The system displays the **List** tab by default.
3. Select **VM-Host Affinity Policies** in the **Policies** tab dropdown menu.

   The system displays a summary view of VM-Host affinity policies across all registered clusters.

Figure 165: Summary View - All Affinity Policies

Table 129: VM-Host Affinity Policies Page Field Description

Parameter	Description	Values
Name	Displays the VM-Host affinity policy name.	(name)
VMs	Displays the count of VMs associated with the selected VM-Host affinity policy.	(number of VMs)
Hosts	Displays the count of hosts associated with the selected VM-Host affinity policy.	(number of hosts)
VM Compliance Status	Displays the compliance status of the VMs associated with this policy. If the policy is being applied and the compliance status is not yet known, the status is displayed as Pending. If a VM is part of multiple VM-Host affinity policies, the oldest policy is applied on the VM. For rest of the policies, the VM is displayed as non-compliant.	(number of VMs Compliant/Non Compliant/Pending)
Modified By	Displays the name of the user who modified the selected VM-Host affinity policy last time.	(user)
Last Modified	Displays the date and time when the selected VM-Host affinity policy is modified last time.	(date & time)

You can perform the following actions for the affinity policies in the **VM-Host Affinity Policies** summary view:

- Access the detailed information about an individual VM-Host affinity policy. For more information, see VM-Host Affinity Policies Details View on page 465.
- Create a VM-Host affinity policy. For more information, see Creating a VM-Host Affinity Policy on page 471.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2935

- Use the **Actions** dropdown menu to update, delete, or re-enforce VM-Host affinity policy. For more information, see Managing VM-Host Affinity Policies on page 472.

VM-Host Affinity Policies Details View

The VM-Host affinity policy details view allows you access the detailed information about an individual VM-Host affinity policy. It includes four tabs: **Summary**, **Categories**, **Entities** and **Audit**.

To access the details view of an individual VM-Host affinity policy, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information on the **Navigation Bar**, see Application-specific Navigation Bar.

   The system displays the **List** tab by default.
3. Select **VM-Host Affinity Policies** in the **Policies** tab.

   The system displays a summary view of VM-Host affinity policies across all registered clusters.
4. Click the target <*Affinity_Policy_Name*> to view the **Summary** tab of an individual VM-Host affinity policy.

> **Note:** Replace <*VM-Host_Affinity_Policy_Name*> with the actual VM-Host affinity policy name at your site.

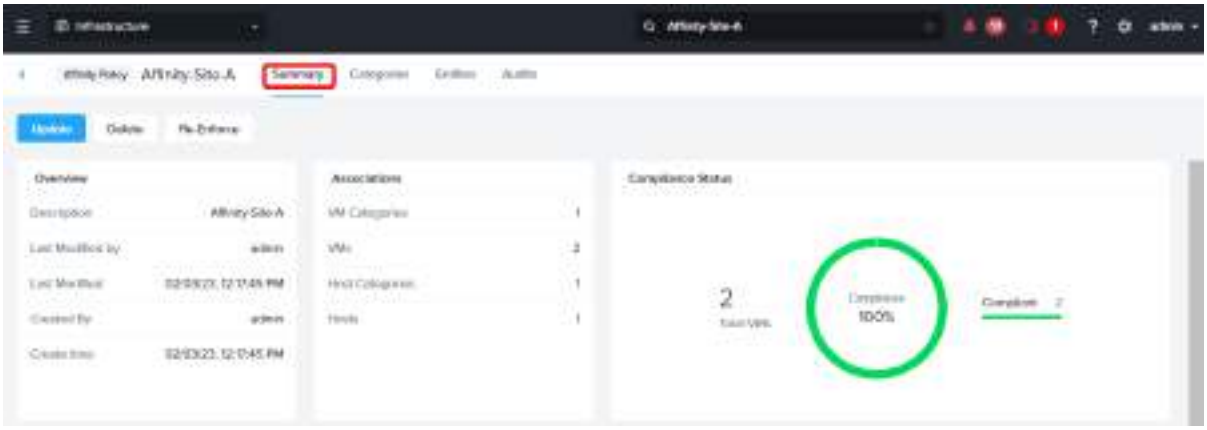


Figure 166: VM-Host Affinity Policies Details view

The **Summary** tab of an individual VM-Host affinity policy provides the following widgets:

- **Overview** - Displays an overview information about the VM-Host affinity policy.
- **Associations**- Displays the associated VM and Host entities and their categories.
- **Compliance Status** - Displays the compliance status of the VMs associated with this policy. If the policy is being applied and the compliance status is not yet known, the status is displayed as Pending. If a VM is part of multiple VM-Host affinity policies, the oldest policy is applied on the VM. For rest of the policies, the VM is displayed as non-compliant.

For information on the fields available in the widgets, see VM-Host Affinity Policy Widgets Field Details on page 465.

<*Action*> available above the widgets. Click the appropriate <*Action*> to run that administrative action on the VM-Host affinity policy. For more information on how to perform any <*Action*>, see Managing VM-Host Affinity Policies on page 472.

VM-Host Affinity Policy Widgets Field Details

The following table describes the fields in the **Overview**, **Associations**, and **Compliance Status** widgets.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2936

Table 130: VM-Host Affinity Policy Widgets Field Description

Field	Description	Values
Overview widget		
Description	Displays the VM-Host affinity policy description specified while creating the VM-Host affinity policy.	(description)
Last Modified By	Displays the name of the user who modified the VM-Host affinity policy last time.	(user)
Last Modified	Displays the date and time when the policy is modified last time.	(date & time)
Created By	Displays the name of the user who created the VM-Host affinity policy	(user)
Create time	Displays the date and time when the VM-Host affinity policy is created.	(date & time)
Associations widget		
VM Categories	Displays the count of VM categories mapped to the selected VM-Host affinity policy.	(number of VM categories)
VMs	Displays the count of VMs associated with the selected VM-Host affinity policy.	(number of VMs)
Host Categories	Displays the count of host categories mapped to the selected VM-Host affinity policy.	(number of host categories)
Hosts	Displays the count of hosts associated with the selected VM-Host affinity policy.	(number of hosts)
Compliance Status widget		
Total VMs	Displays the total number of VMs in the selected VM-Host affinity policy.	(total number of VMs)
Compliance	Displays the compliance status in percentage.	(percentage of complaint VMs)
Compliant, In Progress, or Non compliant	Displays the number of VMs that are compliant and non-compliant with the VM-Host affinity policy. If the compliance check is in progress, the system displays the compliance status as *In progress*.	Compliant, In Progress, or Non compliant

Categories Tab

The **Categories** tab displays the VMs and hosts categories information.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2937

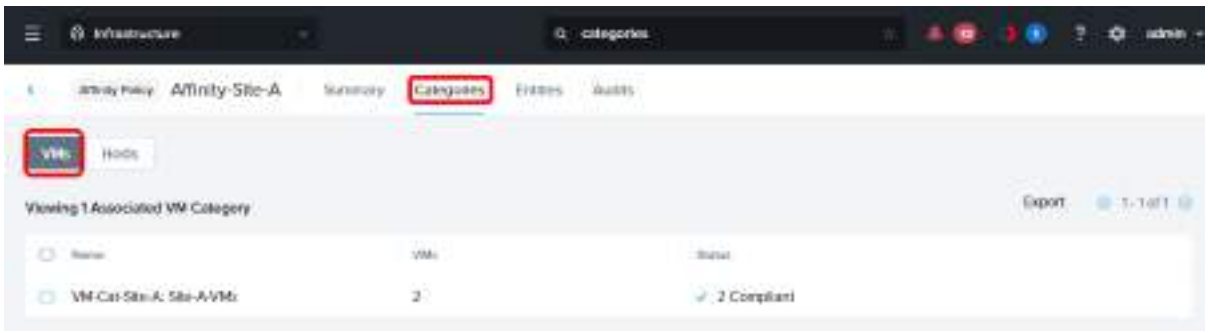


Figure 167: VM-Host Affinity Policies Categories (VMs)

Figure 168: VM-Host Affinity Policies Categories (Hosts)

The following table describes the information displayed in the **Categories** tab

Table 131: Categories Tab Field Description

Field	Description	Values
VMs tab		
Name	Displays the VM category name and its value.	(VM Category Name: Value)
VMs	Displays the count of VMs associated with the selected VM-Host affinity policy.	(number of VMs)
Status	Displays the compliance status.	(number of VMs Compliant|Non-compliant|Pending
Host tab		
Name	Displays the host category name and its value.	(host category Name: Value)
Hosts	Displays the count of hosts associated with the selected VM-Host affinity policy.	(number of hosts)

You can export the table that contains the list of VM categories and host categories and their information to a file in a CSV format. For more information about **Export** option, see Export on page 59.

Entities Tab

The **Entities** tab displays the VMs and hosts entity-related information.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2938

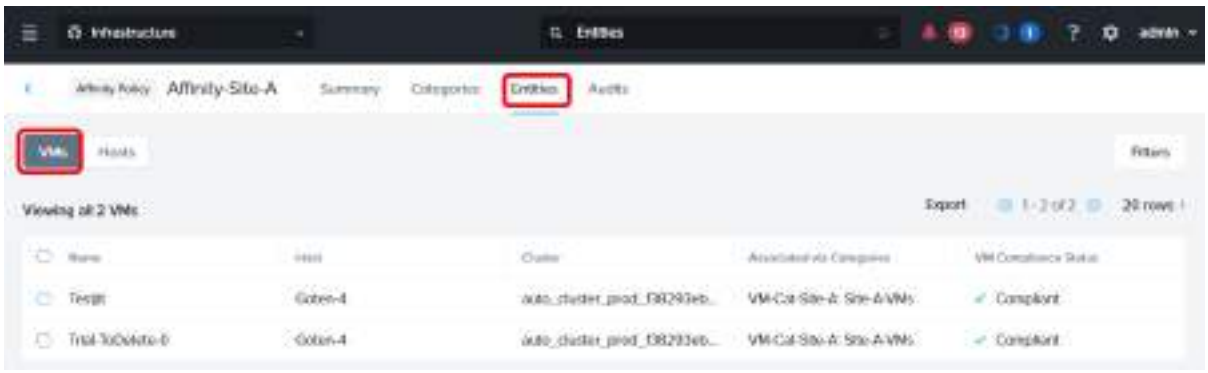


Figure 169: VM-Host Affinity Policies Entities (VMs)

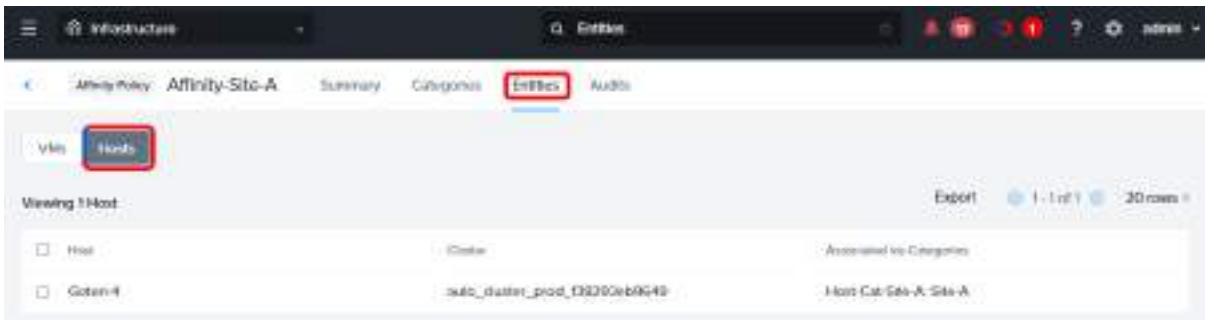


Figure 170: Affinity Policies Entities (Hosts)

The following table describes the information displayed in the **Entities** tab

Table 132: Entities Tab Field Description

Field	Description	Values
VMs tab		
Name	Displays the VM name associated with the selected VM-Host affinity policy.	(VM name)
Host	Displays the host name associated with the selected VM-Host affinity policy.	(host name)
Cluster	Displays the name of the cluster (on which the host resides) associated with the selected VM-Host affinity policy.	(cluster name)
Associated via Categories	Displays the VM category name and its value.	(VM category name: Value)
Compliance Status	Displays the VM compliance status with the selected VM-Host affinity policy.	Compliant|Non-compliant|Pending
Host tab		
Host	Displays the name of the host associated with the selected VM-Host affinity policy.	(host name

Field	Description	Values
Cluster	Displays the name of the cluster (on which the host resides) associated with the selected VM-Host affinity policy.	(cluster name)
Associated via Categories	Displays the host Category name and its value.	(host category name: Value)

You can export the table that contains the list of VM entities and host entities related information to a file in a CSV format. For more information about **Export** option, see Export on page 59.

Audits Tab

The **Audits** tab displays the user action-related information for the VM-Host affinity policies.

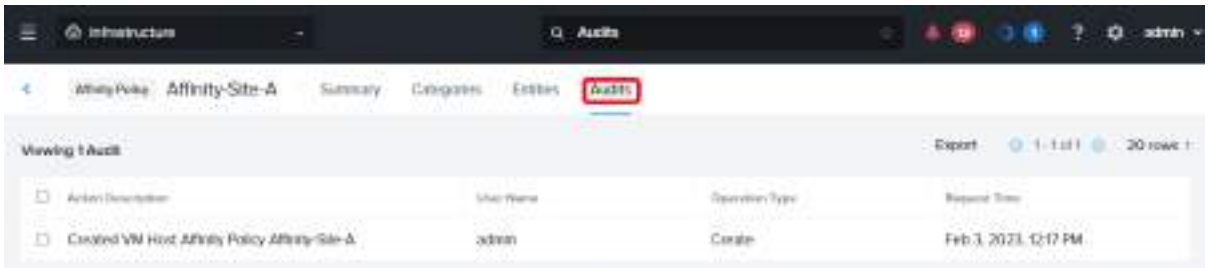


Figure 171: Affinity Policies Audits

The following table describes the information displayed in the **Audits** tab

Table 133: Audits Tab -Field Description

Field	Description	Values
Action Description	Displays the user-action for VM-Host affinity policies.	(action description)
User Name	Displays the name of the user who performed the action.	(host name)
Operation Type	Displays the type of operation performed by the user for VM-Host affinity policies. For example, Create	(cluster name)
Request Time	Displays the date and time of the user action.	(date and time)

You can export the table that contains the list of user actions related information to a file in a CSV format. For more information about **Export** option, see Export on page 59.

Limitations of VM-Host Affinity Policies

VM-Host affinity policies created in Prism Central have the following limitations:

- The minimum supported versions for VM-Host affinity policies are version 6.1 for Prism Element and version 2022.1 for Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2940

- Host category attach or detach takes around five minutes to get reflected in the applicable VM-Host affinity policies.

  When you assign a category to a host and map the host category to the VM-Host affinity policy, you can observe that the host count gets updated immediately in the Entities tab. However, the system takes approximately 5 minutes to update the host count in VM-Host Affinity Policies Summary View on page 463.

  The delay in host count update is due to the usage of different APIs to derive the host count in Entities tab and VM-Host Affinity Policies Summary View on page 463.

  For information about how to create a category, see Creating a Category.

  For information on how to assign a category to host, see Associating Hosts with Categories on page 471

  For information on how to create the VM-Host affinity policy and map the host category to the VM-Host affinity policy, see Creating a VM-Host Affinity Policy on page 471.

VM-Host Affinity Policy Configuration Workflow

About this task

To set up VM-Host affinity policy, perform the following steps:

Procedure

1. Create categories for the following entities:

   a. VMs

   b. Hosts

   For information on how to create a category, see Creating a Category.

2. Apply the VM categories to the VMs and host categories to the hosts.

   For information on how to associate a category to the VMs, see Associating VMs with Categories. For information on associating categories with hosts, see Associating hosts with Categories.

3. Create the VM-Host affinity policy. For more information, see Creating an Affinity Policy.

Associating VMs with Categories

About this task

To associate categories to VMs, perform the following steps:

Procedure

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
   The system displays the **List** tab by default.

3. Select the target VMs checkboxes that you want to associate with a category, and choose **Manage Categories** from the **Actions** dropdown menu.
   The system displays the **Manage VM Categories** window.

4. Type the name of the category in **Set Categories** field.
   The system displays the list of matching categories based on the typed entry.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2941

5. Use the Add icon and Remove icon to add and remove the required categories.

> **Note:** If the VM category you selected is already part of any affinity policy, the system displays the associated affinity policy details.

6. Click **Save**.

Associating Hosts with Categories

About this task

To associate categories with hosts, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Hardware** > **Hosts** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
   The system displays the **List** tab by default.
3. Select the target host checkboxes that you want to associate with a category, and choose **Manage Categories** from the **Actions** dropdown menu.
   The system displays the **Manage Host Categories** window.
4. Type the name of the category in **Set Categories** field.
   The system displays the list of matching categories based on the typed entry.
5. Use the Add icon and Remove icon to add and remove the required categories.
6. Click **Save**.

Creating a VM-Host Affinity Policy

About this task

This section describes how to create a VM-Host affinity policy in Prism Central.

Before you begin

Ensure that the following prerequisites are met before you create the VM-Host affinity policy:

- VM and Host categories are created. For information on how to create a category, see Creating a Category.
- VMs are associated with VM categories, and hosts with host categories. For more information, see Associating VMs with Categories on page 470 and Associating Hosts with Categories on page 471.

> **Note:**
>
> - The system also allows you to associate VMs with VM category and hosts with host category after creation of VM-Host affinity policy.
> - If you have configured any legacy affinity policy (non-category-based affinity policy) associated with the VMs, you must first remove those legacy affinity policies to allow the creation of category-based VM-Host affinity policies associated with the same VMs.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2942

Procedure

To create the VM-Host affinity policy, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
   The system displays the **List** tab by default.
3. Select **VM-Host Affinity Policies** in the **Policies** tab dropdown menu, and click **Create VM-Host Affinity Policy**.
   The system displays the **Create VM-Host Affinity Policy** window.
4. Specify the following information in the **Create VM-Host Affinity Policy** window:
   - **Name**: Enter the VM-Host affinity policy name.
   - (optional) **Description**: Enter the description for the VM-Host affinity policy.
   - **VM Categories**:Type the name of the VM category. The system displays the list of matching categories based on the typed entry. Use the Add icon and Remove icon to add and remove the required categories.
   - **Host Categories**:Type the name of the host category. The system displays the list of matching categories based on the typed entry. Use the Add icon and Remove icon to add and remove the required categories.
5. Click **Create**.

Managing VM-Host Affinity Policies

This section describes how to manage the existing VM-Host affinity policies in Prism Central.

About this task

You can perform the following actions to manage the existing VM-Host affinity policies in Prism Central:

- Update a VM-Host affinity policy.
- Delete a VM-Host affinity policy.
- Re-enforce a VM-Host affinity policy.

Procedure

To manage the VM-Host affinity policies, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
   The system displays the **List** tab by default.
3. Select **VM-Host Affinity Policies** in the **Policies** tab dropdown menu.
   The system displays the affinity policies created across registered clusters.
4. Select the target VM-Host affinity policy checkbox, and choose **Update** from the **Actions** dropdown menu.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2943

5. Update the fields in the **Update VM-Host Affinity Policy** window as per your requirement, and click **Save**. For information on the fields available in **Update VM-Host Affinity Policy** window, see Creating a VM-Host Affinity Policy on page 471.

   To delete the VM-Host affinity policy, select the target VM-Host affinity policy checkbox and choose **Delete** from the **Actions** dropdown menu. The system prompts you to confirm the delete action. Click **Delete** to confirm the delete affinity policy action.

   To re-enforce the VM-Host affinity policy, select the target VM-Host affinity policy checkbox and choose **Re-enforce** from the **Actions** dropdown menu. The system prompts you to confirm the action. Click **Re-enforce** to apply the updated VM-Host affinity policy.

Role Based Access Control for VM-Host Affinity Policies

This section describes the Role Based Access Control (RBAC) requirements and limitations for the VM-Host affinity policies. For information on RBAC, see Controlling User Access (RBAC) in *Security Guide*.

Role Based Access Control Requirements for VM-Host Affinity Policies

Before you allocate the VM-Host Affinity Policy Related Permissions on page 473, ensure that the following basic permissions are allocated to the admin user or a custom user to access the VM-Host affinity policies framework in Prism Central:

- View VM
- View category

VM-Host Affinity Policy Related Permissions

In addition to the basic permissions to view VM and categories as specified in Role Based Access Control Requirements for VM-Host Affinity Policies on page 473, you can also assign the following permissions to the admin or custom user to manage the VM-Host affinity policies in Prism Central:

Table 134: VM-Host Affinity Policy Related Permissions

Permission	Description
Create_VM_Host_Affinity_Policy	Admin or custom user can create the VM-Host affinity Policies.
View_VM_Host_Affinity_Policy	Admin or custom user can view the VM-Host affinity policies.
Update_VM_Host_Affinity_Policy	Admin or custom user can update the existing VM-Host affinity policies.
Reenforce_VM_Host_Affinity_Policy	Admin or custom user can re-enforce the existing VM-Host affinity policies.
Delete_VM_Host_Affinity_Policy	Admin or custom user can delete the VM-Host affinity policies.

These permissions also facilitate the admin or custom user to manage the legacy affinity policies (affinity policies that are defined in the Prism Element) from Prism Central.

Role-Based Access Control Limitations for VM-Host Affinity Policies

The following table describes the limitations that apply to RBAC for the VM-Host affinity policies:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2944

Table 135: RBAC Limitations for VM-Host Affinity Policies

Permission Assigned to the Admin or Custom user	Admin or Custom User Action	System Behavior	Limitation
Create_VM_Host_Affinity_Policy Update_VM_Host_Affinity_Policy	Admin or custom user creates or updates the VM-Host affinity policy.	The system applies the VM-Host affinity policy to all the VMs associated with the mapped VM categories.	The system does not check whether the admin or the custom user has permission to access the VMs or hosts mapped in the VM-Host affinity policy.
Update VM Categories	Admin or custom user updates a VM category (for example, attaches a VM to a VM category).	The system applies the VM-Host affinity policy to which the VM category is assigned.	The system does not check whether the admin or the custom user has permission to create or update the VM-Host affinity policy.
Update Host Categories	Admin or custom user updates a Host category (for example, attaches a host to a Host category).	The system applies the affinity policy to which the host category is assigned.	The system does not check whether the admin or the custom user has permission to create or update the VM-Host affinity policy.

VM-VM Anti-Affinity Policies Defined in Prism Central

This topic describes the VM-VM anti-affinity policies feature available in Prism Central.

In Prism Central, you can define category-based VM-VM anti-affinity policies that run a set of VMs on different hosts, preventing single host failure from impacting all the VMs. The category-based anti-affinity policy allows you easily to manage anti-affinities for a large number of VMs.

The VM-VM anti-affinity policy is soft enforced. The system does not block any operations, such as VM creation, VM updation, upgrades, host maintenance mode, or manual live migration of the VM, even if such operations result in a policy violation.

Disaster Recovery Considerations

If you create a VM-VM anti-affinity policy for a VM that is configured for replication, and you want those policies to be honored on the remote site, then you must create similar categories and corresponding policies on the remote site as well. When you define similar categories and policies on the remote site, the system applies the VM-VM anti-affinity policies to the VMs that you migrate to the remote site. For more information, see Management of VM-VM Anti-Affinity Policies for PC-Based Disaster Recovery Solution on page 483.

VM-VM Anti-Affinity Policies Summary View

Use VM-VM anti-affinity policies summary view to access a list of all user-defined VM-VM anti-affinity policies.

To access the summary view of all the VM-VM anti-affinity policies, follow these steps:

1. Log in to Prism Central.
2. From the Application Switcher Function, select **Infrastructure** application and from the navigation bar, select **Compute** > **VMs**.

   The system displays the **List** tab by default.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2945

3. From the **Policies** tab dropdown menu, select **VM-VM Anti-affinity Policies**.

   The system displays a summary view of VM-VM anti-affinity policies.

Table 136: VM-VM Anti-affinity Policies Page Field Description

Parameter	Description	Values
Name	Displays the VM-VM anti-affinity policy name.	(name)
Categories	Displays the count of categories associated with the selected VM-VM anti-affinity policy.	(number of categories)
VMs	Displays the count of VMs associated with the selected VM-VM anti-affinity policy.	(number of VMs)
VM Compliance Status	Displays the compliance status of the VMs associated with the VM-VM anti-affinity policy. If the policy is being applied and the compliance status is not yet known, the system displays the compliance status as **Pending**.	(number of VMs Compliant/Non-Compliant/Pending)
Modified By	Displays the name of the user who last modified the selected VM-VM anti-affinity policy.	(user)
Last Modified	Displays the date and time when the selected VM-VM anti-affinity policy is last modified.	(date & time)

You can perform the following actions for the VM-VM anti-affinity policies in the **VM-VM Anti-affinity Policies** summary view:

- Access the detailed information about an individual VM-VM anti-affinity policy. For more information, see VM-VM Anti-Affinity Policies Details View on page 475.
- Create a VM-VM anti-affinity policy. For more information, see Creating a VM-VM Anti-Affinity Policy on page 479.
- Update a VM-VM anti-affinity policy. For more information, see Updating a VM-VM Anti-Affinity Policy on page 480.
- Delete a VM-VM anti-affinity policy. For more information, see Deleting a VM-VM Anti-Affinity Policy on page 481.
- Remove a legacy VM group. For more information, see Removing a Legacy VM Group on page 481.

VM-VM Anti-Affinity Policies Details View

Use VM-VM anti-affinity policy details view to access detailed information about an individual VM-VM anti-affinity policy.

To access the details view of an individual VM-VM anti-affinity policy, follow these steps:

1. Log in to Prism Central.
2. From the Application Switcher Function, select **Infrastructure** application and from the navigation bar, select **Compute** > **VMs**.

   The system displays the **List** tab by default.
3. From the **Policies** tab dropdown menu, select **VM-VM Anti-affinity Policies**.

   The system displays a summary view of VM-VM anti-affinity policies across all registered clusters.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2946

4. Click the target *<VM-VM Anti-Affinity_Policy_Name>* to view the **Summary** tab of an individual VM-VM Anti-affinity policy.

> **Note:** Replace *<VM-VM Anti-Affinity_Policy_Name>* with the actual anti-affinity policy name at your site.

The **Summary** tab of an individual VM-VM anti-affinity policy provides the following widgets:

- **Overview**: Displays an overview information about the VM-VM anti-affinity policy.
- **Compliance Status**: Displays the compliance status of the VMs associated with this policy. If the policy is being applied and the compliance status is not yet known, the status is displayed as Pending. If a VM is part of multiple VM-VM anti-affinity policies, the oldest policy is applied on the VM. For rest of the policies, the VM is displayed as non-compliant.

For more information, see VM-VM Anti-Affinity Policy Widgets Field Details on page 476.

VM-VM Anti-Affinity Policy Widgets Field Details

The following table describes the fields in the **Overview** and **Compliance Status** widgets.

Table 137: VM-VM Anti Affinity Policy Widgets Field Description

Field	Description	Values
Overview widget		
Description	Displays the VM-VM anti-affinity policy description specified while creating the anti-affinity policy.	(description)
Last Modified By	Displays the name of the user who modified the VM-VM anti-affinity policy last time.	(user)
Last Modified	Displays the date and time when the VM-VM anti-affinity policy is modified last time.	(date & time)
Created By	Displays the name of the user who created the VM-VM anti-affinity policy.	(user)
Create Time	Displays the date and time when the VM-VM anti-affinity policy is created.	(date & time)
Categories	Displays the count of VM categories mapped to the selected VM-VM anti-affinity policy.	(number of VM categories)
Compliance Status widget		
Total VMs (Unique)	Displays the total number of VMs in the selected VM-VM anti-affinity policy.	(total number of VMs)
Compliance	Displays the compliance status in percentage .	(percentage of complaint VMs)
Compliant, In Progress, or Non compliant	Displays the number of VMs that are compliant and non-compliant with the VM-VM anti-affinity policy. If the compliance check is in progress, the system displays the compliance status as *In progress*.	Compliant, In Progress, or Non compliant

Clusters Tab

The **Clusters** tab displays the associated clusters information.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2947

The following table describes the information displayed in the **Clusters** tab:

Table 138: Clusters Tab Field Description

Field	Description	Values
Name	Displays the cluster name.	(cluster name)
VMs	Displays the count of VMs associated with the selected VM-VM anti-affinity policy.	(number of VMs)
VM Compliance Status	Displays the number of VMs that are compliant and non-compliant with the VM-VM anti-affinity policy. If the compliance check is in progress, the system displays the compliance status as *In progress*.	(number of VMs Compliant|Non-compliant|Pending

You can export the table that contains the list of VMs and their compliance status information to a file in a CSV format. For more information about **Export** option, see Export on page 59.

Categories Tab

The **Categories** tab displays the associated VM categories information.

The following table describes the information displayed in the **Categories** tab:

Table 139: Categories Tab Field Description

Field	Description	Values
Name	Displays the VM category name and its value.	(VM Category Name: Value)
VMs	Displays the count of VMs associated with the selected VM-VM anti-affinity policy.	(number of VMs)
VM Compliance Status	Displays the number of VMs that are compliant and non-compliant with the VM-VM anti-affinity policy. If the compliance check is in progress, the system displays the compliance status as *In progress*.	(number of VMs Compliant|Non-compliant|Pending

You can export the table that contains the list of associated VM categories and their information to a file in a CSV format. For more information about **Export** option, see Export on page 59.

VMs Tab

The **VMs** tab displays the VMs information.

The following table describes the information displayed in the **VMs** tab:

Table 140: VMs Tab Field Description

Field	Description	Values
Name	Displays the VM name associated with the selected VM-VM anti-affinity policy.	(VM name)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2948

Field	Description	Values
Host	Displays the host name associated with the selected VM-VM anti-affinity policy.	(host name)
Cluster	Displays the name of the cluster (on which the host resides) associated with the selected VM-VM anti-affinity policy.	(cluster name)
Category	Displays the VM category name and its value.	(VM category name: Value)
VM Compliance Status	Displays the compliance status of the VM. If the policy is being applied and the compliance status is not yet known, the system displays the compliance status as **Pending** VMs that do not adhere to the anti-affinity placements are displayed as non-compliant. The following are the reasons for displaying a VM as non-compliant: • Cluster Not Supported: When the VM is running on clusters earlier to 6.9 version. • Conflicting Legacy Anti-Affinity Policy: When the VM is already part of the PE based legacy policy. • Conflicting Anti-Affinity Policy: When is VM is part of multiple VM-VM anti-affinity policies, the policy having the oldest creation time is applied on the VM. • Not Enough Hosts: The number of powered on VMs is greater than the number of schedulable hosts. • Not Enough Resources: The scheduler is unable to place the VMs in a manner that conforms with the policy.	(Compliant/Pending/ Cluster Not Supported/ Conflicting Legacy Anti-Affinity Policy/Conflicting Anti-Affinity Policy/ Not Enough Hosts/Not Enough Resources)

You can export the table that contains the list of VM entities related information to a file in a CSV format. For more information about **Export** option, see Export on page 59.

Audits Tab

The **Audits** tab displays the user action-related information for the VM-VM anti-affinity policies.

The following table describes the information displayed in the **Audits** tab:

Table 141: Audits Tab Field Description

Field	Description	Values
Action Description	Displays the user-action for the VM-VM anti-affinity policies.	(action description)
User Name	Displays the name of the user who performed the action.	(host name)
Operation Type	Displays the type of operation performed by the user for the VM-VM anti-affinity policies.	(cluster name)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2949

Field	Description	Values
Request Time	Displays the date and time of the user action.	(date and time)

You can export the table that contains the list of user actions related information to a file in a CSV format. For more information about **Export** option, see Export on page 59.

Limitations of VM-VM Anti-Affinity Policies

This topic outlines the limitations of the VM-VM anti-affinity policies.

The VM-VM anti-affinity policies created in Prism Central have the following limitations:

- When you attach or detach a VM category, Prism Central takes approximately seven minutes to reflect the change in the applicable VM-VM anti-affinity policies.
- When you assign a category to a VM and map the VM category to the VM-VM anti-affinity policy, you can observe that the VM count updates immediately in the VMs Tab on page 477. However, Prism Central takes approximately seven minutes to update the VM count in the VM-VM Anti-Affinity Policies Summary View on page 474.
- You can associate a maximum of 20 VM categories to a single VM-VM anti-affinity policy.
- When the VM is part of multiple VM-VM anti-affinity policies, the policy with the oldest creation time is applied on the VM.
- When the VM is part of a legacy VM-VM anti-affinity policy and PC based VM-VM anti-affinity policy, the legacy VM-VM anti-affinity policy takes precedence over PC based VM-VM anti-affinity policy.

VM-VM Anti-Affinity Policy Configuration Workflow

This topic describes the workflow to create a VM-VM anti-affinity policy.

About this task

To configure a VM-VM anti-affinity policy, follow these steps:

Procedure

1. Create a category.

   For more information, see Creating a Category.

2. Apply the category to the VMs.

   For more information on how to associate a category to the VMs, see Associating VMs with Categories.

3. Create the VM-VM anti-affinity policy.

   For more information, see Creating a VM-VM Anti-Affinity Policy on page 479.

Creating a VM-VM Anti-Affinity Policy

This task describes how to create a VM-VM anti-affinity policy from Prism Central.

Before you begin

Ensure that you meet following prerequisites before you create the VM-VM anti-affinity policy:

- You are on AOS 7.0 or later and pc.2024.3 or later.
- A category is created. For information on how to create a category, see Creating a Category on page 459.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2950

- VMs are associated with VM categories. For more information, see Associating VMs with Categories on page 470.

  Note: Prism Central also allows you to associate VMs with VM category after creation of VM-VM anti-affinity policy.

- If you configured any legacy VM-VM anti-affinity policy (non-category-based anti-affinity policy) associated with the VMs, you must first remove those legacy anti-affinity policies to allow the creation of category-based anti-affinity policies associated with the same VMs. For more information, see Removing a Legacy VM Group on page 481.

About this task

To create a VM-VM anti-affinity policy, follow these steps:

Procedure

1. Log in to Prism Central.
2. From the Application Switcher Function, select **Infrastructure** application and from the navigation bar, select **Compute** > **VMs**.
   The system displays the **List** tab by default.
3. From the **Policies** tab dropdown menu, select **VM-VM Anti-affinity Policies**.
4. Click **Create VM-VM Anti-affinity Policy**.
5. Enter the following information in the **Create VM-VM Anti-affinity Policy** window:
   - **Name**: Enter the VM-VM anti-affinity policy name.
   - (Optional) **Description**: Enter the description for the VM-VM anti-affinity policy.
   - **VM Categories**: Type the name of the VM category. The system displays the list of matching categories based on the typed entry. Use the Add icon and Remove icon to add and remove the required categories.
6. Click **Create**.

Updating a VM-VM Anti-Affinity Policy

This task describes how to update a VM-VM anti-affinity policy from Prism Central.

About this task

To update a VM-VM anti-affinity policy, follow these steps:

Procedure

1. Log in to Prism Central.
2. From the Application Switcher Function, select **Infrastructure** application and from the navigation bar, select **Compute** > **VMs**.
   The system displays the **List** tab by default.
3. From the **Policies** tab dropdown menu, select **VM-VM Anti-affinity Policies**.
   The system displays the VM-VM anti-affinity policies created across registered clusters.
4. Select the target VM-VM anti-affinity policy checkbox, and from the **Actions** dropdown menu, choose **Update**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2951

5. Update the fields in the **Update VM-VM Anti-affinity Policy** window as needed and click **Update**.
   For information on the fields available in the **Update VM-VM Anti-affinity Policy** window, see Creating a VM-VM Anti-Affinity Policy on page 479.

Deleting a VM-VM Anti-Affinity Policy

This task describes how to delete a VM-VM anti-affinity policy from Prism Central.

About this task

To delete a VM-VM anti-affinity policy, follow these steps:

Procedure

1. Log in to Prism Central.
2. From the Application Switcher Function, select **Infrastructure** application and from the navigation bar, select **Compute** > **VMs**.
   The system displays the **List** tab by default.
3. From the **Policies** tab dropdown menu, select **VM-VM Anti-affinity Policies**.
   The system displays the VM-VM anti-affinity policies created across registered clusters.
4. Select the target VM-VM anti-affinity policy checkbox and from the **Actions** dropdown menu, choose **Delete**.
   The system prompts you to confirm the delete action.
5. Click **Delete**.

Removing a Legacy VM Group

This task describes how to remove a legacy VM Group from Prism Central.

About this task

The VM-VM anti-affinity policies configured from aCLI are called legacy anti-affinity policies and the VM groups mapped to these policies are called legacy VM groups in Prism Central. If you previously created any legacy VM groups that are associated with VM-VM anti-affinity policies, you must first remove those legacy VM groups to use the new Prism Central based VM-VM anti-affinity policies for those VMs.

To remove the legacy VM Group from Prism Central, follow these steps:

Procedure

1. Log in to Prism Central.
2. From the Application Switcher Function, select **Infrastructure** application and from the navigation bar, select **Compute** > **VMs**.
   The system displays the **List** tab by default.
3. From the **Policies** tab dropdown menu, select **VM-VM Anti-affinity Policies**.
   The system displays a summary view of VM-VM anti-affinity policies across all registered clusters.
4. Click **You have Legacy VM Group defined through the CLI** banner.
   The system displays **Legacy VM-VM Anti-affinity Policies** window.
5. Select the target **VM Groups** checkbox, and select **Delete selected group**.
6. Click **Delete**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2952

Role Based Access Control for the VM-VM Anti-Affinity Policies

This topic describes the Role Based Access Control (RBAC) requirements and limitations for VM-VM anti-affinity policies.

Using RBAC, you can provide the necessary permissions for users to access the VM-VM anti-affinity policies. For information on RBAC, see Controlling User Access (RBAC) in *Security Guide*.

RBAC Requirements for the VM-VM Anti-Affinity Policies

Before you allocate the VM-VM Anti-Affinity Policy Related Permissions on page 482, ensure that the view VM permission is allocated to the admin user or a custom user to access the VM-VM anti-affinity policies in Prism Central.

VM-VM Anti-Affinity Policy Related Permissions

In addition to the view VM permission, you can also assign the following permissions to the admin or custom user to manage the VM-VM anti-affinity policies in Prism Central:

Table 142: VM-VM Anti-Affinity Policy Related Permissions

Permission	Description
Create_VM_Anti_Affinity_Policy	Admin or custom user can create anti-affinity policies.
View_VM_Anti_Affinity_Policy	Admin or custom user can view anti-affinity policies.
Update_VM_Anti_Affinity_Policy	Admin or custom user can update the existing anti-affinity policies.
View_VM_Anti_Affinity_Policy_VM_Compliance_States	Admin or custom user can view the compliance state of anti-affinity policies.
Delete_VM_Anti_Affinity_Policy	Admin or custom user can delete anti-affinity policies.
View_Legacy_VM_Anti_Affinity_Policy	Admin or custom user can view legacy anti-affinity policies.
Delete_Legacy_VM_Anti_Affinity_Policy	Admin or custom user can delete legacy anti-affinity policies.

RBAC Limitations for the VM-VM Anti-Affinity Policies

The following table describes the limitations that apply to RBAC for the VM-VM anti-affinity policies:

Table 143: RBAC Limitations for VM-VM Anti-Affinity Policies

Permission Assigned to the Admin or Custom User	Admin or Custom User Action	System Behavior	Limitation
Create_VM_Anti_Affinity_Policy Update_VM_Anti_Affinity_Policy	Admin or custom user creates or updates the VM-VM anti-affinity policy.	The system applies the VM-VM anti-affinity policy to all VMs associated with the mapped VM categories.	The system does not check whether the admin or the custom user has permission to access the VMs mapped in the VM-VM anti-affinity policy.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2953

Permission Assigned to the Admin or Custom User	Admin or Custom User Action	System Behavior	Limitation
Update_VM_Categories	Admin or custom user updates a VM category (for example, attaches a VM to a VM category).	The system applies the VM-VM anti-affinity policy to which the VM category is assigned.	The system does not check whether the admin or the custom user has permission to create or update the VM-VM anti-affinity policy.

Management of VM-VM Anti-Affinity Policies for PC-Based Disaster Recovery Solution

This section describes how to manage VM-VM anti-affinity policies in a Prism Central-based Disaster Recovery (DR) setup.

Managing Failover Operation

This section describes how to set up VM-VM anti-affinity policies at the recovery site for a failover operation.

About this task

After the failover is completed, the VM categories assigned to the VM on the primary site (primary AZ) are synchronized to the recovery site (recovery AZ). The synchronized VM categories are also reflected in the Prism Central instance of the recovery site.

To set up the VM-VM anti-affinity policies at the recovery site, perform the following actions before a disaster occurs:

Procedure

1. Create the VM categories at the recovery site with the same name as defined at the primary site.
   For more information, see Creating a Category in *Prism Central Infrastructure Guide*.
2. Reconfigure the VM-VM anti-affinity policies at the recovery site using the VM categories created at the recovery site.
   For more information, see Creating a VM-VM Anti-Affinity Policy in *Prism Central Infrastructure Guide*.

   Important: If the legacy VM-VM anti-affinity policies are defined using Prism element, the policies are not replicated during failover, and you need to manually redefine the anti-affinity policies at the recovery site after failover.

Overview of Failback Operation

This section describes how failback operation functions for VM-VM anti-affinity policies at the primary site in a Prism Central-based Disaster Recovery setup.

After you perform failback, the VM categories are synchronized back to the primary site, and the anti-affinity policies created on the primary site (primary AZ) are enabled for the VMs.

Managing Synchronous Replication

This section describes how to set up VM-VM anti-affinity policies at the recovery site for a synchronous replication operation.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2954

About this task

You can configure the VM-VM anti-affinity policy at the recovery site for the VMs or VM categories that are protected with synchronous replication schedule in the primary site using the following workflow:

Procedure

1. Create the VM categories at the recovery site with the same name as defined at the primary site.
   For more information, see Creating a Category in *Prism Central Infrastructure Guide*.
2. Create the VM-VM anti-affinity policies at the recovery site using the VM categories created at the recovery site.
   For more information, see Creating a VM-VM Anti-Affinity Policy in *Prism Central Infrastructure Guide*.

> **Note:** For more information about how to configure the protection policy with a synchronous replication schedule, see Creating a Protection Policy in *Nutanix Disaster Recovery Guide*.

NGT Policies

NGT policies are used to define the VM reboot action after you install or upgrade the NGT.

If a restart is required post installation or upgrade, you can define a policy on when the restart should happen. You can use these policies when you have different set of VMs which you would like to be restarted at different times, for example if they are in different time zones or if their down times are expected to be different. Policy workflow are defined on the categories. You have to attach the category to the VM and then you can create a policy for the VM.

> **Important:** The NGT policies are applied only when you select **Skip restart** option during installation or upgradation of NGT. However, if you select a different restart option during installation or upgradation of NGT, the NGT policy is not applied. For more information about how to install and upgrade NGT, see NGT Management in Prism Central on page 176.

NGT Policies Summary View

The NGT policies summary view enables you to access a list of all the user-defined Nutanix Guest tools (NGT) policies (VM reboot policies) across registered clusters.

To access the NGT policies summary view, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The system displays the **List** tab by default.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2955

3. Select **NGT Policies** in the **Policies** tab dropdown menu.

   The system displays a view of NGT policies across all registered clusters.

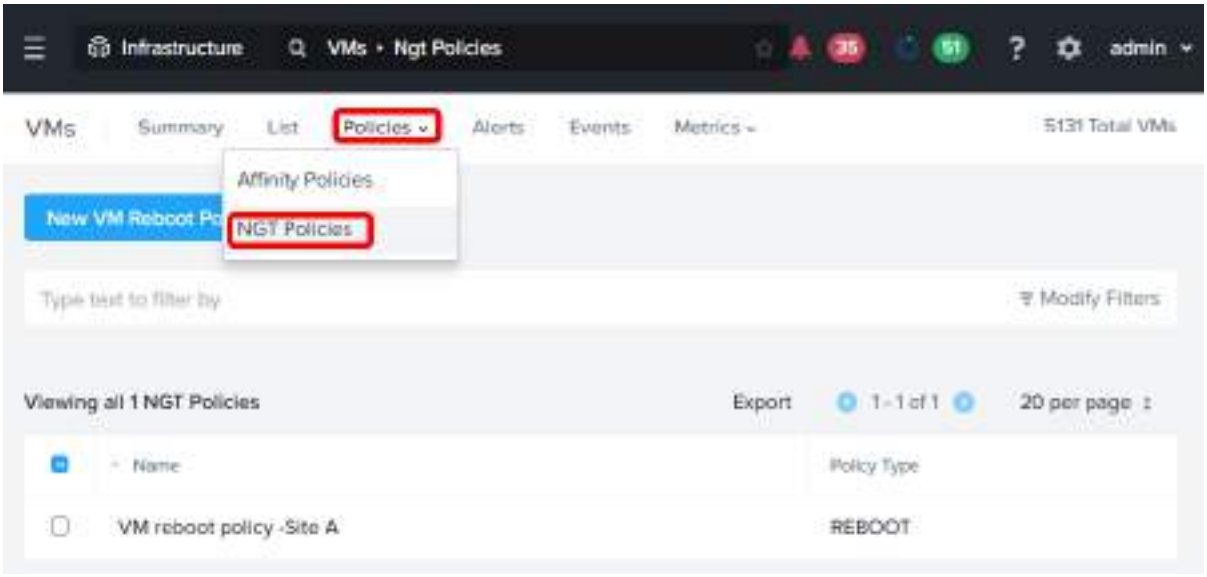


Figure 172: NGT Policies

Table 144: NGT Policies Page - Field Description

Field	Description	Values
Name	Displays the NGT policy name.	(name)
Policy Type	Displays the type of NGT policy.	REBOOT

You can perform the following actions for the NGT policies in the **NGT Policies** summary view:

- Create an NGT policy. For more information, see Creating a NGT Policy on page 485.
- Filter the NGT policies list based on the NGT policy name using **Filters** pane. For more information about **Filters** pane, see Filters Pane on page 55.
- Use the **Actions** dropdown menu to update and delete an NGT policy. For more information, see Managing NGT Policies on page 487.

Creating a NGT Policy

This section describes how to create a NGT Policy (VM reboot policy).

Procedure

To create a NGT policy, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2956

3. Select **NGT Policies** in the **Policies** tab dropdown menu, and click **New VM Reboot Policy**.
   The system displays the **New VM Reboot Policy** window.

4. Specify the following information in the **Create Affinity Policy** window:

   - **Policy Name**: Enter the NGT policy (VM reboot policy) name.
   - (optional) **Policy Description**: Enter the description for the NGT policy.
   - **Guest Restart Schedule**: Select one of the following guest VM restart schedules:

     - **Restart as soon as the install/upgrade is completed**: Select this option if you want to restart the VMs of the selected category right after the install process is completed.
     - **Restart at specific day and time after the upgrade is completed**: Select this option and choose the date and time on which you want to the restart to happen.

       Note: The VMs restart depends on the Prism Element timezone settings.

     - **Add Category**: Click **Add Category** and select the category that you want to apply to the NGT policy. Type the name of the VM category. The system displays the list of matching categories based on the typed entry. Use the Add icon and Remove icon to add and remove the required categories.

       For information about how to create a VM category, see Creating a Category on page 459.

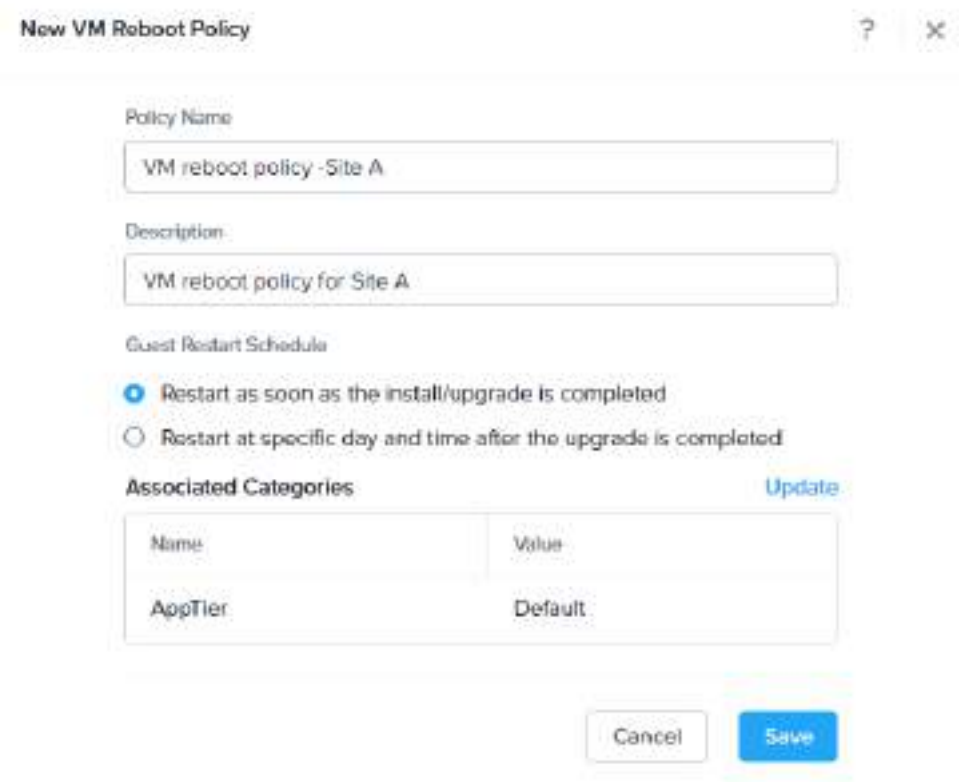


Figure 173: Create VM Reboot Policy

5. Click **Save**.

   Note: Any VM reboot policy you create using this procedure is overridden if you choose to restart the VM during installation or upgradation of NGT by using a different option compared to the option configured in the policy for VM restart. If you choose not to restart the VM during installation or upgradation of NGT, the system continues

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2957

to apply the existing reboot policy for the VM. For example, if you select the **Restart as soon as the install/ upgrade is completed** option as part of the NGT policy, and if you select the **Restart at specific date and time after the install is completed** option during installation or upgradation of NGT, the **Restart at specific date and time after the install is completed** setting take precedence and the VM is restarted at the scheduled date and time. However, if you select the **Skip restart** option during installation or upgradation of NGT, the VM reboot policy takes precedence and the VM restart occurs immediately after an installation or upgrade.

The policy is created and saved in the NGT Policies pane.

Managing NGT Policies

This section describes how to manage the existing NGT policies (VM reboot policies) in Prism Central.

About this task

You can perform the following actions to manage the existing NGT policies in Prism Central:

- Update an NGT policy.
- Delete an NGT policy.

Procedure

To modify a NGT policy, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default.
3. Select the target NGT policy checkbox, and choose **Update** from the **Actions** dropdown menu.
   The system displays the NGT policies created across registered clusters.
4. Update the fields in the **Update VM Reboot Policy** window as per your requirement, and click **Save**. For field details, see Creating a VM-Host Affinity Policy on page 471.

Figure 174: Update VM Reboot Policy

To delete an NGT policy, select the target NGT policy checkbox and choose **Delete** from the **Actions** dropdown menu. The system prompts you to confirm the delete action. Click **Delete** to confirm the delete NGT policy action.

Image Policy Management

In Prism Central, you can create and manage the following types of policies for the images:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2958

- Image Placement Policies (see Image Placement Policies on page 488)
- Bandwidth Throttling Policies (see Bandwidth Throttling Policies on page 496)

Image Placement Policies

Prism Central enables you to upload VM images from your workstation or from a remote server. It also enables you to manually specify a subset of registered clusters as targets for those images. However, image placement decisions are often driven by compliance requirements, policies, and regulations. For example, you might have to confine a VM image to a Nutanix cluster in a specific location. Or, a cluster in one region might require a Windows VM image with a specific set of applications while a cluster in another region might require a Linux VM with its own set of applications.

Prism Central enables you to configure policies that govern which clusters receive the images that you upload. These policies, called image placement policies, map images to target clusters using categories associated with both those entities. For example, an image placement policy states that the Linux images associated with the `OS:Linux` and `distribution:Centos` categories must be uploaded to the clusters associated with the `Location:SFO` category.

Image placement policies also specify how strictly the policy must be enforced. Soft enforcement allows clusters not identified by the policy to use the images, when required, by checking them out. Hard enforcement disallows such usage. By using both soft and hard enforcement on the same category of clusters, you can address more specific use cases. For more information, see Sample Scenarios and Configurations on page 494.

Image placement policies maintain a state of compliance across the clusters registered with Prism Central. They detect and correct violations introduced by changes in category assignments and updates to their configuration (including a switch from soft enforcement to hard enforcement). For more information, see Sample Scenarios and Configurations on page 494.

Image Placement Policies Summary View

The image placement policies summary view allows you to access a list of all the user-defined image placement policies across registered clusters.

To access the summary view of all image placement policies:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The system displays the **List** tab by default.
3. Select **Placement Policies** in the **Policies** tab dropdown menu.

   The system displays a summary view of image placement policies across all registered clusters.

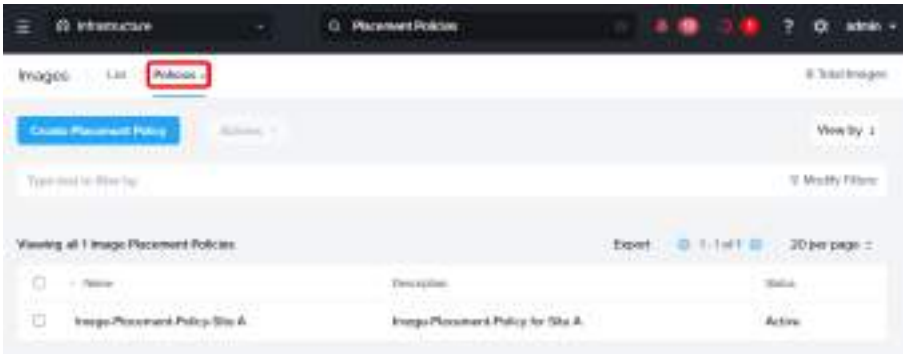


Figure 175: Summary View - All Image Placement Policies

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2959

Table 145: Image Placement Policies Page - Field Description

Field	Description	Values
Name	Displays the image placement policy name.	(name)
Description	Displays the purpose of the image placement policy.	(text string)
Status	Displays the status of the image placement policy.	Active|Suspended

You can perform the following actions in the **Image Placement Policies** summary view:

- Access the detailed information about an individual image placement policy. For more information, see Image Placement Policy Details View on page 489.
- Create an image placement policy. For more information, see Creating an Image Placement Policy on page 491.
- Use the **Actions** dropdown menu to update, delete, suspend enforcement (if status is active) or resume enforcement (if status is suspended). For more information, see Managing Image Placement Policies on page 493.
- Filter the image placement policies list using **Filters** pane. For more information about **Filters** pane, see Filters Pane on page 55.

  For more information about fields, see Table 145: Image Placement Policies Page - Field Description on page 489.
- Export the table that contains the list of image placement policies and their information to a file in a CSV format. For more information about **Export** option, see Export on page 59.
- View image placement policies based on pre-defined criteria or create a custom view. For information about available views and how to create a custom view, see View by on page 56.

Image Placement Policy Details View

To access the details view of an individual image placement policy, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The system displays the **List** tab by default.
3. Select **Placement Policies** in the **Policies** tab.

   The system displays a summary view of image placement policies across all registered clusters.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2960

4. Click the target <*Image_Placement_Policy_Name*> to access the details view individual image placement policy.

> **Note:** Replace <*Image_Placement_Policy_Name*> with the actual image placement policy name at your site.

Figure 176: Image Placement Policy Details view

The details view of an individual image placement policy provides the following information:

- Policy name that appears in the upper left. You can switch from one policy to another by selecting the policy name from the dropdown menu.
- Policy enforcement status appears below the name and indicates whether the enforcement is hard or soft.
- Two columns that specify the target images (on the left) and target clusters (on the right). Click **Expand all** (or **Collapse all**) to display (or hide) the list of images or clusters.

<*Action*> available in the top right corner. Click the appropriate <*Action*> to run that administrative action on the image placement policy. For more information about how to perform any <*Action*>, see Managing Image Placement Policies on page 493.

Configuration Workflow

About this task

To set up an image placement policy, perform the following steps:

Procedure

1. Create categories for the following entities:
   a. Clusters (for example, create categories based on cluster location or region)
   b. Images (for example, create categories based on operating system and size)

   For information about how to create a category, see Creating a Category.
2. Apply the cluster categories to clusters and image categories to images.

   For information about how to associate categories with a Nutanix cluster, see Associating Clusters with Categories on page 490.

   For information about how to associate categories with an image, see Associating an Image with Categories.
3. Configure the image placement policy. For more information, see Configuring an Image Placement Policy.

Associating Clusters with Categories

About this task

To associate categories with a registered Nutanix cluster, perform the following steps:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2961

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Hardware** > **Clusters** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default.
3. Select the target cluster checkboxes that you want to associate with a category, and choose **Manage Categories** from the **Actions** dropdown menu.
   The system displays the **Manage Cluster Categories** window.
4. Type the name of the category in **Set Categories** field.
   The system displays the list of matching categories based on the typed entry.
5. Use the Add icon and Remove icon to add and remove the required categories.
6. Click **Save**.

Associating Images with Categories

About this task

To associate categories with an image, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default.
3. Select the target image checkbox(es) that you want to associate with a category, and choose **Manage Categories** from the **Actions** dropdown menu.
   The system displays the **Manage Image Categories** window.
4. Type the name of the category in **Set Categories** field.
   The system displays the list of matching categories based on the typed entry.
5. Use the Add icon and Remove icon to add and remove the required categories.
6. Click **Save**.

Creating an Image Placement Policy

About this task

This section describes how to create an image placement policy in Prism Central.

Before you begin

Ensure that the following prerequisites are met before you create an image placement policy:

- Cluster and Image categories are created. For information about how to create a category, see Creating a Category on page 459.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2962

- Images are associated with the Image categories, and clusters with the cluster categories. For more information, see Associating Images with Categories on page 491 and Associating Clusters with Categories on page 490.

  Note: The system also allows you to associate images with image category and clusters with cluster category after creation of image placement policy.

- Review existing image placement policies to avoid causing conflicts. For information about issues caused by conflicting policies, see How Prism Central Handles Conflicting Policies on page 494

Procedure

To create an affinity policy, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default.
3. Select **Placement Policies** in the **Policies** tab dropdown menu, and click **Create Placement Policy**.
   The system displays the **Create Image Placement Policy** window.
4. Specify the following information in the **Create Image Placement Policy** window:
   - **Policy Name**: Enter the image placement policy name.
   - (optional) **Description**: Enter the description for the image placement policy.
   - **Assign Images With All Of The Following Categories**: Type the name of the image category. The system displays the list of matching categories based on the typed entry. Use the Add icon and Remove icon to add and remove the required categories.
   - **To Clusters With All Of The Following Categories**: Type the name of the cluster category. The system displays the list of matching categories based on the typed entry. Use the Add icon and Remove icon to add and remove the required categories.
   - **Policy Enforcement**: Select one of the following mechanisms for policy enforcement:
     - **Soft** - The images are uploaded to the set of clusters identified by the image placement policy, and no restriction is placed on using those images on clusters outside the identified set. For example, if clusters A, B, and C are registered with Prism Central, and an image placement policy with a soft enforcement policy uploads an image to clusters A and B, you can use the image to create a VM on cluster C. The checkout to cluster C is not blocked.
     - **Hard** - The images are uploaded to the set of clusters identified by the image placement policy, however you cannot use the image to create a VM on any cluster outside the identified set. For example, if clusters A, B, and C are registered with Prism Central, and an image placement policy with a hard enforcement

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2963

policy uploads an image to clusters A and B, the image is available only on clusters A and B. Cluster C cannot check out the image.

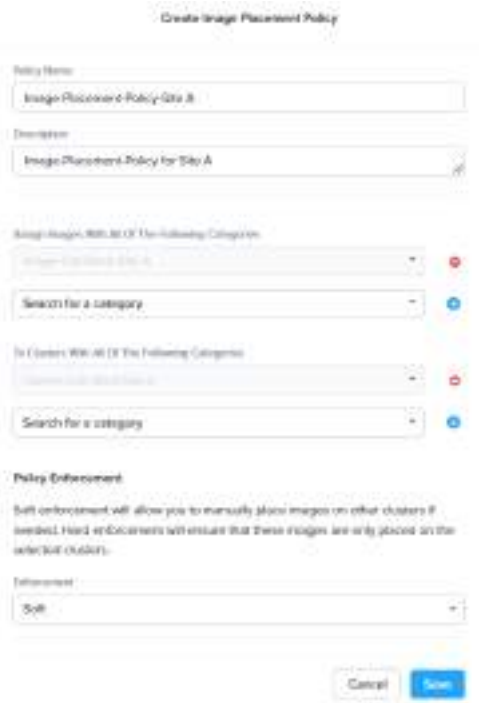


Figure 177: Create Image Placement Policy

5. Click **Save**.

Managing Image Placement Policies

This section describes how to manage the image placement policies in Prism Central.

About this task

You can perform the following actions to manage the image placement policies in Prism Central:

- Update an image placement policy.
- Delete an image placement policy.
- Suspend Enforcement
- Resume Enforcement

Updates to an image placement policy can result in a policy violation. Prism Central attempts to correct the violation by running a series of actions. For example, if you change the cluster category such that the policy now identifies a different set of clusters as targets, Prism Central first copies the images to the clusters in the new category, and then removes the images from the clusters in the previously mentioned category. If you change the policy enforcement setting from Soft to Hard, and if any clusters that are not identified as targets had previously checked out the images, Prism Central corrects the violation by deleting the images from those clusters. An update to a policy might also result in a conflict with one or more of the other policies that apply to the same category of images.

For more information about how Prism Central handles conflicting policies, see How Prism Central Handles Conflicting Policies on page 494.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2964

Procedure

To update an image placement policy, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default.
3. Select **Placement Policies** in the **Policies** tab dropdown menu.
   The system displays the placement policies across all the registered clusters.
4. Select the target image placement policy checkbox, and choose **Update** from the **Actions** dropdown menu.
5. Update the fields in the **Update Image Placement Policy** window as per your requirement, and click **Save**. For field details, see Creating an Image Placement Policy on page 491.

   To delete the image placement policy, select the target image placement policy checkbox and choose **Delete** from the **Actions** dropdown menu. The system prompts you to confirm the delete action. Click **Delete** to confirm the delete action.

   To suspend enforcement of the image placement policy (if Active), select the target image placement policy checkbox and choose **Suspend Enforcement** from the **Actions** dropdown menu. The system prompts you to confirm the **Suspend Enforcement** action. Click **Confirm** to suspend the policy enforcement.

   To resume enforcement of the image placement policy (if Suspended), select the target image placement policy checkbox and choose **Resume Enforcement** from the **Actions** dropdown menu. The system prompts you to confirm the **Resume Enforcement** action. Click **Confirm** to resume the policy enforcement.

How Prism Central Handles Conflicting Policies

Policies are said to be in conflict if they identify the same category of images but their resulting cluster placements are different.

For example, the following policies are conflicting policies if they apply to the same category of images:

- Policy P1, which identifies clusters C1 and C2 as target clusters, and the policy enforcement setting is Soft.
- Policy P2, which identifies clusters C3 and C4 as target clusters, and the policy enforcement setting is Hard.

Prism Central handles such conflicts in the following manner:

- Prism Central ignores conflicting policies and does not perform any action on the images. If policy P1 was configured first, Prism Central stops enforcing P1 as soon as P2 is configured, and it does not enforce P2 either. When there is a policy conflict, the conflict is noted in the **Policies** tab of the details view for that image.
- Prism Central continues to enforce other policies that are not in conflict. For example, if policies P3 and P4 apply to the same categories of images as P1 and P2, Prism Central continues to enforce P3 and P4 as long as they are not in conflict with P1 and P2.

Sample Scenarios and Configurations

The following table describes how to configure image management policies to achieve a desired result. The examples use a Prism Central instance to which three clusters A, B, and C and registered (possibly among other clusters).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2965

Table 146: Sample Scenarios and Configurations

Desired Result	Image Placement Policy Configuration
The images must be available on any one of the clusters (A, B, or C) and can be checked out to the other two clusters and to any other clusters that might be registered with Prism Central now or in the future.	Create an image placement policy that identifies any one of the clusters (A, B, or C) as the target cluster (by the use of categories) and set the policy enforcement to Soft.
The images must be available on all of the clusters A, B, and C and can be checked out to any other clusters that are registered with Prism Central now or in the future.	Create an image placement policy that identifies clusters A, B, and C as the target clusters (by the use of categories) and set the policy enforcement to Soft.
The images must be available on all of the clusters A, B, and C and cannot be checked out to any other clusters that are registered with Prism Central now or in the future.	Do the following: • Create an image placement policy that identifies clusters A, B, and C as the target clusters (by the use of categories) and set the policy enforcement to Soft. (This policy ensures that the images are available on all of the three clusters) • Create a second image placement policy that identifies clusters A, B, and C as the target clusters (by the use of categories) and set the policy enforcement to Hard. (This policy makes sure that the images are available only on these three clusters)
The images must be available only on cluster A and cannot be checked out to clusters B and C now, and the images also cannot be checked out to any other clusters that are registered with Prism Central in the future.	Create an image placement policy that identifies cluster A as the target cluster (by the use of categories) and set the policy enforcement to Hard.
The images are available on cluster A and must now be available on clusters B and C. Cluster A can use the images if required. The policy enforcement is currently Soft.	Do the following: • Dissociate the categories specified in the image placement policy from cluster A and associate them with clusters B and C. • Do not update the image placement policy (no changes are required). Prism Central takes the following corrective actions: 1. Prism Central copies the images to clusters B and C. If clusters B and C had checked out the images before the reassignment of categories to the clusters, the images are not copied. 2. Additionally, because the Soft policy enforcement setting is retained, Prism Central does not remove the image from cluster A.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2966

Desired Result	Image Placement Policy Configuration
The images are available on cluster A and must now be available only on clusters B and C. Cluster A must not be permitted to use the images. The policy enforcement is currently Soft.	Do the following: • Dissociate the categories specified in the image placement policies from cluster A and associate them with clusters B and C. • Change the policy enforcement setting in the image placement policy to Hard. Prism Central takes the following corrective actions: 1. Prism Central copies the images to clusters B and C. If clusters B and C had checked out the images before the reassignment of categories to the clusters, the images are not copied. 2. To honor the Hard policy enforcement setting, Prism Central removes the image from cluster A.

Bandwidth Throttling Policies

Prism Central uses the bandwidth throttling policy feature to manage the usage of bandwidth when you create a new image or transfer an image from one cluster to another cluster using Prism Central. The bandwidth throttling policy allows you to limit the bandwidth consumed during image creation using the URL option in specific clusters. For information about how to add a image using the URL option, see Adding Images from a Remote Server on page 253.

Without bandwidth throttling policy, an image creation from the remote server consumes as much bandwidth as available. High bandwidth consumption for creating a new image limits the bandwidth availability for the other cluster operations.

Bandwidth Throttling Policies Summary View

The bandwidth throttling policies summary view allows you to access a list of all the user-defined bandwidth-throttling policies across registered clusters.

Summary View of all Bandwidth Throttling Policies

To access the bandwidth throttling summary view, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The system displays the **List** tab by default.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2967

3. Select **Bandwidth Throttling Policies** in the **Policies** tab dropdown menu.

   The system displays a view of bandwidth throttling policies across all registered clusters.

Figure 178: Bandwidth Throttling Policies

Table 147: Bandwidth Throttling Policies Page - Field Description

Field	Description	Values
Policy Name	Displays the policy name.	(name)
Description	Describes the purpose of the policy.	(description)
Bandwidth Throttle Limit	Describes the bandwidth throttle limit configured for the policy in MBps	xx MBps
Last Updated On	Describes the date and time when the bandwidth throttling policy was created or updated.	(date and time)

You can perform the following actions for the bandwidth throttling policies in the **Bandwidth Throttling Policies** summary view:

- Access the detailed information about an individual bandwidth throttling policy. For more information, see Bandwidth Throttling Policy Details View on page 497.
- Create a bandwidth throttling policy. For more information, see Creating a Bandwidth Throttling Policy on page 499.
- Filter the bandwidth throttling policies list using **Filters** pane. For more information about **Filters** pane, see Filters Pane on page 55

  For more information about fields, see Table 147: Bandwidth Throttling Policies Page - Field Description on page 497.
- Export the table that contains the list of bandwidth throttling policies and their information to a file in a CSV format. For more information about **Export** option, see Export on page 59.
- View bandwidth throttling policies based on pre-defined criteria or create a custom view. For information about available views and how to create a custom view, see View by on page 56.
- Use the **Actions** dropdown menu to update and delete a bandwidth throttling policy. For more information, see Managing Bandwidth Throttling Policies on page 501.

Bandwidth Throttling Policy Details View

To access the details view of an individual bandwidth throttling policy, perform the following steps:

1. Log in to Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2968

2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The system displays the **List** tab by default.
3. Select **Bandwidth Throttling Policies** in the **Policies** tab.

   The system displays a summary view of bandwidth throttling policies across all registered clusters.
4. Click the target <*Bandwidth_Throttling_Policy_Name*> to access the details view individual bandwidth throttling policy.

   Note: Replace <*Bandwidth_Throttling_Policy_Name*> with the actual bandwidth throttling policy name at your site.

Figure 179: Bandwidth Throttling Policy Details view

The details view of an individual bandwidth throttling policy provides the following information:

- Policy name that appears in the upper left.
- **Enrolled Cluster** tab that displays the following cluster information:
  - **Cluster Name** - Displays the name of the cluster that is configured with bandwidth throttling policy.
  - **Effective Bandwidth Limit** - The selected cluster uses the **Effective Bandwidth Limit** configured to add a new image next time. In a scenario where multiple bandwidth throttling policies are applied to the same cluster, the minimum of all the applicable bandwidth throttling policies is enforced on the cluster.

    For example, you have a cluster named **PE-123**, and you have created multiple bandwidth throttling policies with different **Bandwidth Limit**, then during the cluster association with the bandwidth throttling policy (step 6), the cluster is associated with the bandwidth throttling policy which has the least **Bandwidth Limit** configured on it.
  - **Hypervisor** - Displays the Hypervisor name.
  - **Health** - Displays the cluster health.
  - **Host Count** - Displays the number of hosts in the cluster

<*Action*> available above the detailed view column. Click the appropriate <*Action*> to run that administrative action on the bandwidth throttling policy. For more information about how to perform any <*Action*>, see Managing Bandwidth Throttling Policies on page 501 .

Requirements for Bandwidth Throttling Policy

Ensure that the following prerequisites are met to configure the bandwidth throttling policy feature in Prism Central:

- Prism Central release 2021.9 or later and AOS version 6.0 or later are deployed at your site.
- The clusters are registered with Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2969

- A cluster category is created and associated with the cluster.

  For information about how to create a cluster category, see Creating a Category on page 459.

  For information about how to associate a category to a cluster, see Assigning a Category on page 460.

- AHV Hypervisor is deployed at your site.

  Note: The bandwidth throttling policy is not supported with ESXi and Hyper-V hypervisors.

Limitations with Bandwidth Throttling Policy

The following limitations apply to the bandwidth throttling policies:

- Prism Central enforces bandwidth throttling policy only for new images created by using the URL option on clusters registered with Prism Central. For information about how to add a image using the URL option, see Adding Images from a Remote Server on page 253.
- You cannot enforce a bandwidth throttling policy if you create an image directly from a Prism Element.
- The least applicable bandwidth throttling policy on the source and destination cluster is enforced when you transfer an image from one cluster to another cluster.

Creating a Bandwidth Throttling Policy

About this task

This section describes how to create a bandwidth throttling policy in Prism Central.

Perform the following procedure to create a new bandwidth throttling policy.

Before you begin

Ensure that the following prerequisites are met before you create a bandwidth throttling policy in Prism Central:

- Requirements that are described in Requirements for Bandwidth Throttling Policy on page 498 are followed.
- Limitations that are described in Limitations with Bandwidth Throttling Policy on page 499 are observed.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2970

3. Select **Bandwidth Throttling Policies** in the **Policies** tab dropdown menu, and click **Create Policy**. The system displays the **Create Image Bandwidth Throttling Policy** window.

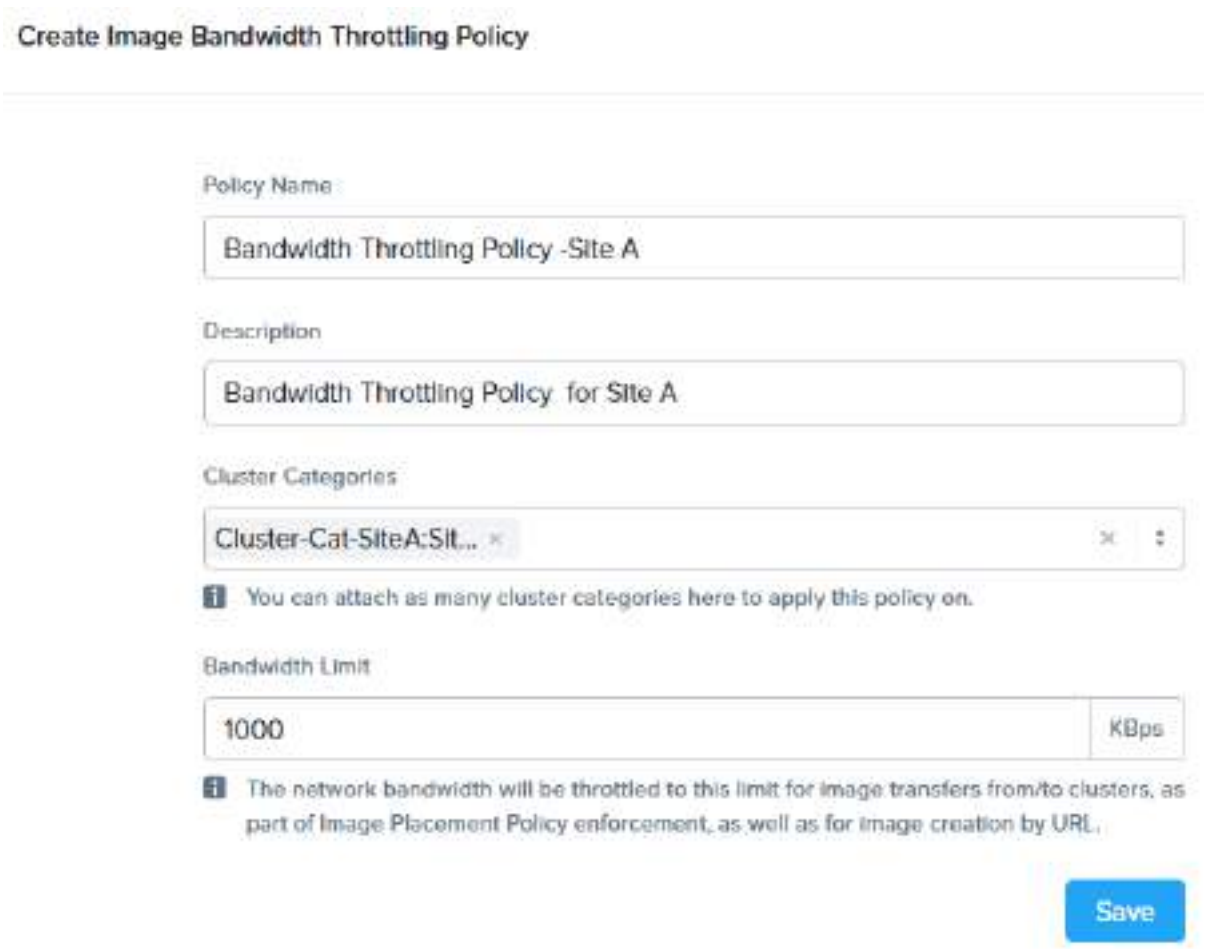


Figure 180: Create Bandwidth Throttling Policy

4. Specify the following information in the **Create Image Bandwidth Throttling Policy** window:

   - **Policy Name**: Enter the image placement policy name.
   - (optional) **Description**: Enter the description for the image placement policy.
   - **Cluster Categories**: Type the name of the cluster category. The system displays the list of matching categories based on the typed entry. Use the Add icon and Remove icon to add and remove the required categories.

     For more information about categories, see Category Management on page 456 .
   - **Bandwidth Limit**: Enter the bandwidth throttling value in KBps. The system considers this value when you add the image using the URL option and while enforcing image placement policy to transfer image transfer from one cluster to another.

     Note: The bandwidth limit task is serialized on each cluster to strictly enforce the bandwidth limit on each cluster. For example, when you create a new image, only one image create task runs on the cluster at a time. The second image creation task configured with another bandwidth limit can start only after completion of the first image creation task.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2971

5. Click **Save**.

Managing Bandwidth Throttling Policies

This section describes how to manage the bandwidth throttling policies in Prism Central.

About this task

You can perform the following actions to manage the bandwidth throttling policies in Prism Central:

- Update an bandwidth throttling policy
- Delete an bandwidth throttling policy.

Procedure

To manage the bandwidth throttling policies, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default.
3. Select **Bandwidth Throttling Policies** in the **Policies** tab dropdown menu.
   The system displays the bandwidth throttling policies across all the registered clusters.
4. Select the target bandwidth throttling policy checkbox, and choose **Update** from the **Actions** dropdown menu.
5. Update the information as per your requirement in the **Update Image Bandwidth Throttling Policy** window, and click **Save**. For more information about fields, see Creating a Bandwidth Throttling Policy on page 499.

   To delete the bandwidth throttling policy, select the target bandwidth throttling policy checkbox and choose **Delete** from the **Actions** dropdown menu. The system prompts you to confirm the delete action. Click **Delete** to confirm the delete action.

Security Policy Management

Security policies inspect traffic that originates and terminates within a data center and help eliminate the need for additional firewalls within the data center.

Security policies are defined using Nutanix Flow which provides a policy-driven security framework. You can enable Nutanix Flow using the Flow-specific settings from the **Prism Central Settings** page. For more information, see Prism Central Settings (Infrastructure) on page 49.

For information about how to create and apply security policies, see Flow Microsegmentation Guide.

For information about how to view the security policies across all clusters in prism Central, see Security Policies Summary View on page 501.

For information about how to view the detailed information about an individual security policy, see Security Policy Details View on page 505.

Security Policies Summary View

The Security policies summary view allows you to access a list of all the user-defined security policies across registered clusters.

To access the security summary view, perform the following steps:

1. Log in to Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2972

2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Network & Security** > **Security Policies** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The system displays the **Policies** tab by default with consolidated view of security policies across all registered clusters.
3. Select **Security Policies** in the **Policies** tab dropdown menu.

   The system displays a view of security policies across all registered clusters.

Figure 181: Security Policies

Table 148: Security Policies Page - Field Description

Field	Description	Values
Name	Displays the security policy name. The policy is one of three types: application, quarantine, or isolation.	(name), Application, Quarantine, Isolation
Purpose	Describes the purpose of the security policy.	(text string)
Policy	Displays a high-level view of the policy configuration.	(boxed text)
Status	Displays the current status of the security policy as either Enforced or in Monitoring mode.	Enforced, Monitoring
Last Modified	Displays the time-line for the security policy. Last modified time-line or the creation time-line if the policy has never been modified.	Time-line. For example, 4 days ago, 6 minutes ago

You can perform the following actions for the security policies in the **Security Policies** summary view:

- Access the detailed information about an individual security policy. For more information, see Security Policy Details View on page 505.
- Create, import, or export a security policy. For more information, see Flow Microsegmentation Guide.
- Filter the security policies list using **Filters** pane. For more information about **Filters** pane, see Filters Pane - Security Policies Page on page 504
- Use the **Actions** dropdown menu to update, delete, enforce (if initial selection is monitoring), or monitor (if initial selection is enforce) a security policy. For more information, see Flow Microsegmentation Guide.

Services Tab

Service is a group of protocol-port combination. You can use any of the default services or create a custom service.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2973

The **Services** tab displays the list of all system and user-defined (custom) services.

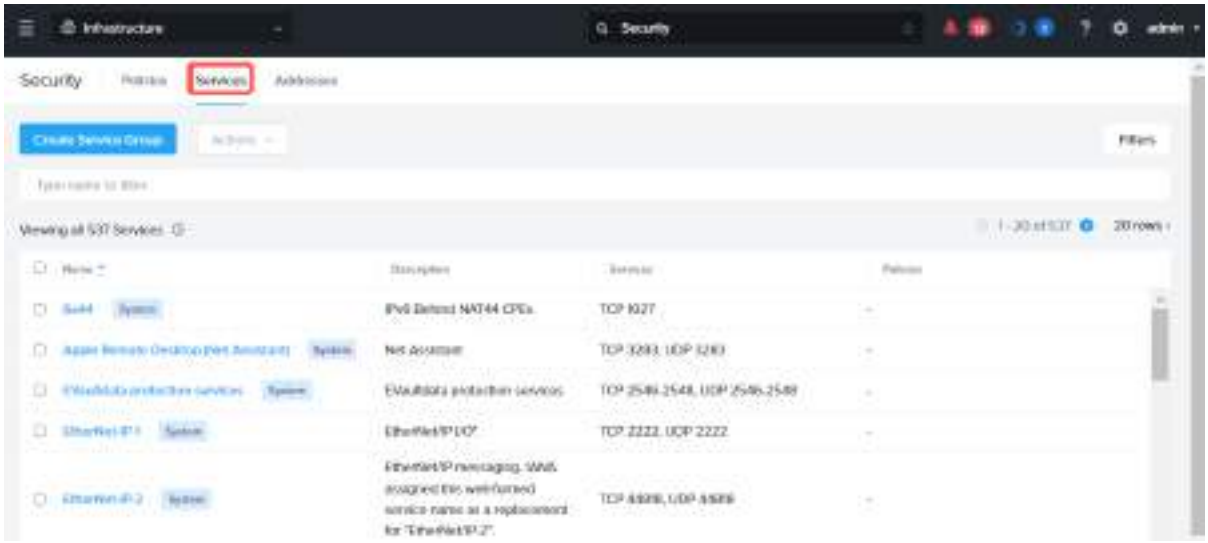


Figure 182: Security Services Tab

The following table describes the fields that appear in the **Services** tab of **Security**page:

Table 149: Security Services Tab - Field Description

Field	Description	Values
Name	Displays the service name.	(service name)
Description	Displays the description of the service.	(description, string)
Services	Displays the protocol and port combination of the service	(Protocol-Port combination) For example, TCP 1027
Policies	Displays the security policies in which the services are attached.	(policy name)

You can perform the following actions for the services in the **Services** tab:

- Filter the services list based on the available field values using **Filters** pane. For more information about **Filters** pane, see Filters Pane - Security Policies Page on page 504.
- Create a service group. For more information about how to create a service group, see Flow Microsegmentation Guide.
- Use the **Actions** dropdown menu to update, delete, or clone a service. For more information, see Flow Microsegmentation Guide.

> **Note:** The **Actions** dropdown menu is grayed out unless you select a service or if you select multiple services.

Addresses Tab

Address Group is a way to group one or many IP address or range. It can be used when you define security policies.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2974

The **Addresses** tab displays the list of all user-defined addresses.

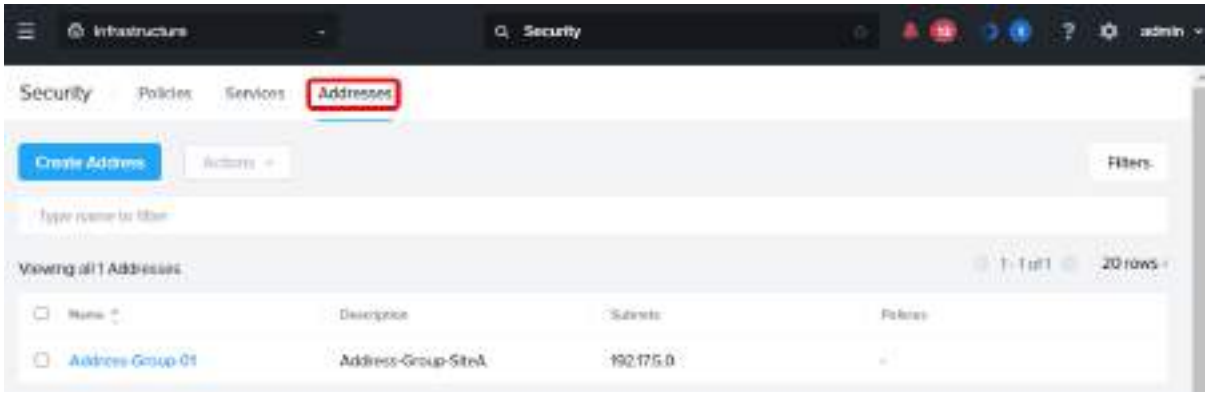


Figure 183: Security Addresses Tab

The following table describes the fields that appear in the **Addresses** tab of **Security**page:

Table 150: Security Addresses Tab - Field Description

Field	Description	Values
Name	Displays the address group name.	(address group name)
Description	Displays the description of the address group.	(description, string)
Subnets	Displays the subnet information	(subnet IP)
Policies	Displays the security policies in which the addresses are used.	(policy name)

You can perform the following actions for the addresses in the **Addresses** tab:

- Filter the services list based on the available field values using **Filters** pane. For more information about **Filters** pane, see Filters Pane - Security Policies Page on page 504.
- Create Address. For more information about how to create a address, see Flow Microsegmentation Guide.
- Use the **Actions** dropdown menu to update or delete an address. For more information, see Flow Microsegmentation Guide.

> **Note:** The **Actions** dropdown menu is grayed out unless you select a address or if you select multiple addresses.

Filters Pane - Security Policies Page

The following table describes the fields available in the **Filters** pane:

Table 151: Filter Pane Fields - Security Policies

Field	Description	Values
Filter pane fields in **Policies** tab.		

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2975

Field	Description	Values
Name	Filters based on the security policy name. Select a condition from the dropdown menu and enter a string in the field. The system returns a list of security policies that satisfy the security policy name condition/string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	(security policy name string)
Type	Filters on the security policy type. Select the checkbox for one or more of the policy types (application, quarantine, isolation, and VDI).	Application, Quarantine, Isolation, VDI
Status	Filters on the security policy status. Select the checkbox for Enforced, or Monitoring, or both.	Enforced, Monitoring
Filter pane fields in **Services** tab.		
Name	Filters based on the service name. Select a condition from the dropdown menu and enter a string in the field. The system returns a list of services that satisfy the service name condition/ string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	(service name)
Description	Filters based on the description of the service.	(description, string)
Protocol	Filters based on the service protocol; TCP, UDP, and ICMP.	TCP|UDP|ICMP
Filter pane fields in **Addresses** tab.		
Name	Filters based on the address name. Select a condition from the dropdown menu and enter a string in the field. The system returns a list of addresses that satisfy the address name condition/ string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	(address name)
Description	Filters based on the description of the address.	(description, string)

Security Policy Details View

To access the details view of an individual security policy, perform the following steps:

1. Log in to Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2976

2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Network & Security** > **Security Policies** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The system displays the **Policies** tab by default with consolidated view of security policies across all registered clusters. .
3. Select **Security Policies** in the **Policies** tab dropdown menu.

   The system displays a view of security policies across all registered clusters.
4. Click the target <*Security_Policy_Name*> to access the details view individual security policy.

> **Note:** Replace <*Security_Policy_Name*> with the actual security policy name at your site.

Figure 184: Security Policy Details view

Figure 185: Security Policy Details View: Enforced Policy Example

You can perform the following actions in the **Security Policies** details view:

- Use toggle **Show Blocked Traffic** to view or hide the blocked traffic data. This toggle is available when policy status is **Enforced**.
- Use toggle **Show Discovered Traffic** to view or hide the discovered traffic data. This toggle is available when policy status is **Monitoring**.
- Update, delete, enforce (if initial selection is monitoring), or monitor (if initial selection is enforce) a security policy. For more information, see Flow Microsegmentation Guide.
- Click the Help icon to open a help page in a separate tab or window.

The available actions appear in bold; other actions are grayed out. For grayed out options, the system displays a tool tip with the reason.

Storage Policy Management

Storage Policies in Prism Central let you manage the storage attributes like Replication factor, encryption, compression, and QoS of entities like Virtual Machines (VMs) and Volume Groups (VGs). A single storage policy can manage the attributes of several entities that are associated with various Categories. You can configure entity-centric storage policies to manage the storage attributes of the entities as required.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2977

When you install or upgrade the Prism Central instance to Prism Central pc.2024.1 or later versions, Prism Central configures a predefined or default storage policy.

For more information on the default storage policy, see Default Storage Policy on page 509.

A storage policy uses categories to associate with entities such as VMs and VGs. Using a storage policy, you can manage parameters of the entities such as Replication Factor, encryption, type of data compression (such as Inline, No compression, or Post Process compression), and IOPS or Throughput throttling to be applied to the entities. When you apply storage policies to the entities using categories, the attributes are configured for the entities, and the entity data is transformed to comply with the storage policy. This mechanism is described in Storage Policy Compliance on page 518.

Important Considerations

- Prism Central supports storage policies only on AHV.
- Prism Central supports Data-at-rest encryption at the entity level with storage policies. In other words, when Prism Central applies a storage policy on an entity such as a VM or VG, it applies the policy even if data-at-rest encryption is not enabled on the cluster. Storage policies support entity-centric data-at-rest encryption only if the encryption on the underlying clusters is enabled during deployment.

  > **Note:** After you enable encryption using storage policies, you cannot turn it off. However, you can delete the storage policy on which the encryption is enabled. In such cases, any new data written into the entities is not encrypted. The data that was written prior to the deletion of the storage policy remains encrypted.

- Prism Central supports storage policies for VMs and volume groups (VGs).
- Prism Central applies storage policies to Categories. You need to tag the VMs and VGs in Categories. You might also attach VGs to VMs. When you apply different storage policies through different categories to a VG and VM tagged to each other, the storage policies are applied independently. The storage policy applied to the tagged VG does not affect the tagged VM and vice versa.
- The storage policy engine takes 30 minutes or more to apply a newly created storage policy to the associated entities like VMs. The time taken depends on the number of entities associated with the storage policy.
- Storage policies use categories to associate with entities like VMs and VGs. You cannot associate an entity such as a VM or a VG directly with the storage policy. Create a category for the entities, and then assign the category with the storage policy.

  When you associate a category with a storage policy, Prism Central associates all the entities that are associated with that category with the storage policy.

  For information about how to create a category and assign a category to a VM or VG, see Category Management on page 456.
- A cloned entity like a cloned VM or VG inherits the category and the attached storage policy of the original entity from which it is cloned. Thus, the storage policy engine applies the storage policy that is associated with the inherited category to the cloned entities.
- A cloned entity like a cloned VM does not inherit the compliance state of the storage policy applied to the entity from which it is cloned. The cluster runs a full compliance cycle to establish compliance with the storage policy of the cloned entity. In this case, the system displays the **Compliance State** of the cloned entity as **In Progress**, and not inherit the **Compliant** state.

  For example, if VM1 has a storage policy applied to it and is in a **Compliant** state and VM2 is cloned from VM1, then VM2 does not automatically inherit the **Compliant** state of VM1.
- Shared data between the encrypted VMs and unencrypted VMs is encrypted.
- Shared data between a VM with Replication Factor 2 and another VM with Replication Factor 3 configurations complies with Replication Factor 3. In other words, in such a case, the shared data has three copies.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2978

- For disaster recovery, when you use a snapshot or recovery point of a VM on which you have applied a storage policy, the snapshot restores the category of the VM and, therefore, the storage policy as well.

  Note: The recovery point or snapshot of a VG does not restore the category, and therefore the storage policy, of the VG.

Requirements

Ensure that you meet the following requirements to complete the built-in pre-checks and successfully create a storage policy.

Note: The storage policy engine performs the pre-checks based on these requirements in the sequence listed below. For example, suppose you repeat an existing storage policy name for a new storage policy. In that case, the policy engine fails the storage policy creation, generates the failure message stating, Duplicate name , and stops other checks. The engine triggers the storage policy creation only after all the pre-checks are validated.

1. A unique name is assigned to every storage policy. Prism Central displays an error if the storage policy name matches any existing storage policy entry.
2. A *defined* (non-default) value for at least one storage policy attribute or property. For example, for **Compression** the default value is **Inherit from Cluster**, so you might instead select **On** with **Inline** as the value. You could select or provide a defined value for any one ore more properties of the storage policy.

   For the list of properties that you can configure during creation or updating of a storage policy, see Creating a Storage Policy on page 520.
3. The throttled IOPS value is set greater than 99 (to enable rate-limiting or throttling) or equal to -1 (to clear the throttling) in the storage policies.
4. The replication factor you set is supported by the fault tolerance of the cluster that hosts the VMs or VGs.

   For example, if the fault tolerance of the cluster is 1N/1D, then select the replication factor **2** in the policy.

Limitations

- Prism Central does not support storage policies for entities running on ESXi and Hyper-V.
- Prism Central does not support storage policies for Nutanix Disaster Recovery with on-premises recovery AZ (on-prem recovery cluster managed by a Prism Central or Nutanix Disaster Recovery with multiple Prism Central deployments. For more information, see Nutanix Disaster Recovery Guide.
- Nutanix supports storage policies for Nutanix Disaster Recovery with single Prism Central. However, the storage properties defined for the container are applied to the snapshots replicated to the replication cluster. In other words, the snapshot data replicated to the remote site is transformed based on the settings defined for the remote site containers. The storage policies are applied only after the VM failover.
- You can associate multiple categories with one storage policy. However, you can associate one category with only one storage policy. After associating a category with one storage policy, you cannot associate the same category with another storage policy. When you associate the same category with another storage policy, Prism Central adds the category to the **Associated Categories** list but displays an alert (an exclamation mark) and turns off the **Save** button until you remove the category. The following message pops up when you hover on or click the alert (exclamation mark):

  ```
  This category has an existing storage policy (<name of storage policy>)
   associated with it.
  ```

- You can create a maximum of 100 storage policies irrespective of the type of Prism Central deployed (whether x-large, large, small, or x-small Prism Central with scale-out or single instance).

  For information on Prism Central scalability and the type of Prism Central deployments, see the *Prism Central Scalability* topic in the release notes for the Prism Central version to be installed.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2979

- You cannot create or apply a storage policy for a snapshot. Prism Central applies a storage policy to a live vDisk and the entire chain of snapshots of that vDisk.
- Prism Central does not encrypt the snapshots of the vDisk that are in the storage if the live vDisk is deleted before AOS applies the storage policy to the vDisk.
- Role-based access control (RBAC) can be configured for **Storage Policies**. Prism Central supports only Super Admin, Prism Admin, or Prism Viewer roles for Storage Policies. Prism Central does not support granular RBAC for Storage Policies. Do not attempt to configure permissions using APIs. Use **Super Admin** role permissions for **Storage Policies** operations.

  You can create custom roles to assign specific permissions such as create, update, delete, or view permissions.
- If two entities that share data have different Replication Factor, then the higher Replication Factor is applied to the shared data.
- If two entities share data and one or both entities have a storage policy with encryption enabled, then the shared data is encrypted.
- If two entities share data and only one of the entities has a storage policy with compression enabled, then the shared data is not compressed.
- Suppose you associate an entity with multiple storage policies. In that case, the policy engine sorts the storage policy list using a method based on the policy name and applies the highest-ranking policy from the sorted list to the entity. The highest-ranking storage policy is the one with the lexicographically smallest name in the list. Suppose you add another storage policy later, and this newly added policy becomes the highest-ranking policy in the newly sorted list. In that case, the engine continues to apply the previously applied storage policy. To apply the newly added storage policy to the entity, remove the association of the entity with the previously applied storage policy.

Default Storage Policy

Storage Policies in Prism Central lets you manage the storage attributes like Replication factor, encryption, compression, and QoS of entities like Virtual Machines (VMs) and Volume Groups (VGs). You can configure custom entity-centric storage policies to manage the storage attributes of the entities as required.

When you install or upgrade the Prism Central instance to pc.2024.1 or later versions, Prism Central configures a predefined or default storage policy. The default storage policy only defines the Replication Factor (RF) and Compression parameters. It allows the values for the other parameters to be taken from the cluster storage settings.

The default storage policy requires a minimum Prism Central version of pc.2024.1. AOS 6.8 and later versions fully support the default storage policy. Older versions of AOS do not fully support the default storage policy, even if they support storage policies broadly.

The **Storage Policies** dashboard in Prism Central provides an introductory dialog that describes the **Default Storage Policy**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2980

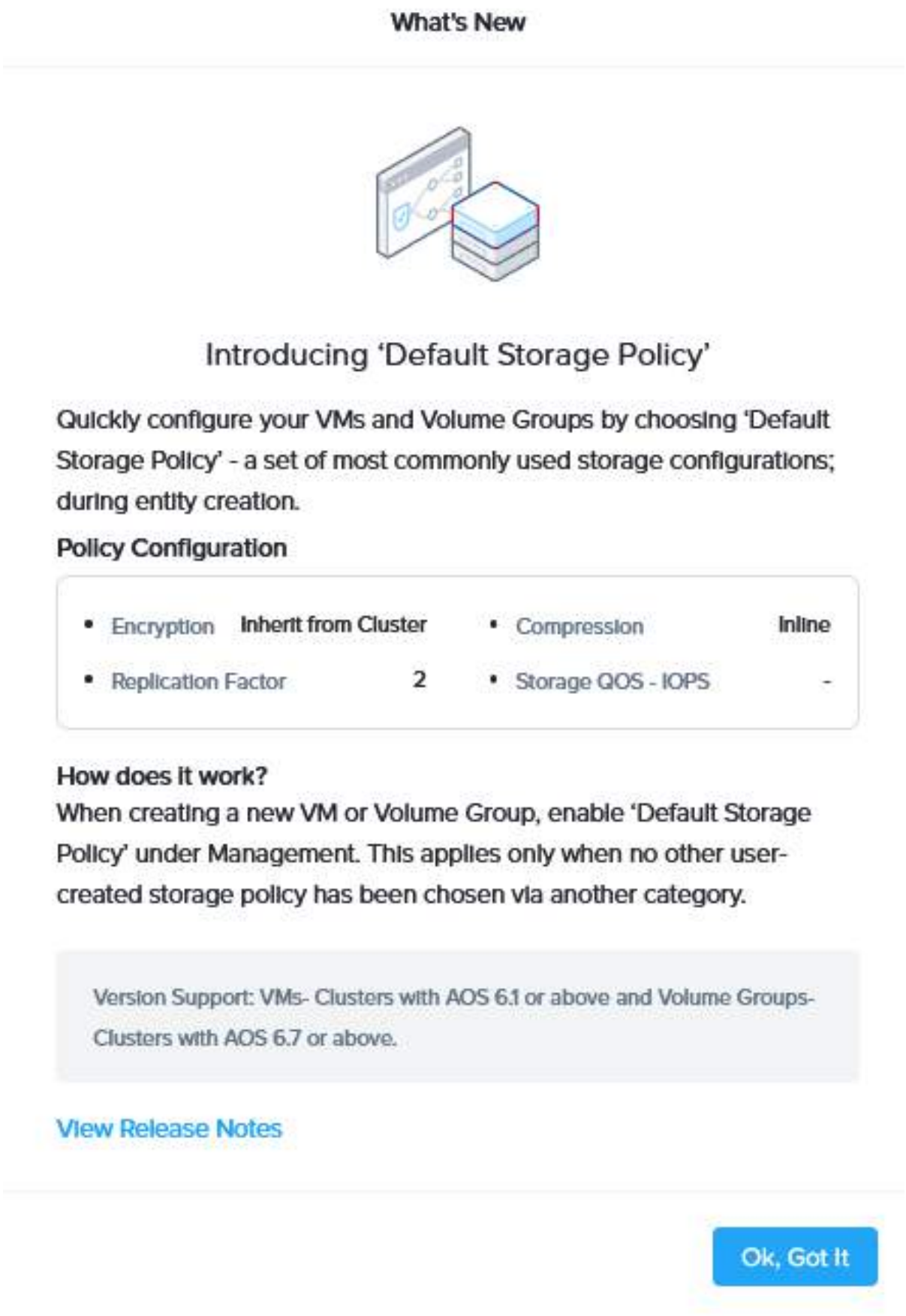


Figure 186: Introducing 'Default Storage Policy'

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2981

You can apply the default storage policy to any entity, such as VMs and VGs, by enabling the **Enable 'Default-Storage' policy** toggle switch when you create or update a VM or VG. The default storage policy is associated with the **Storage:$Default** category. When you turn on the **Enable 'Default-Storage' policy** toggle switch, the default storage policy is applied, like any other storage policy, to the VM or VG that is associated with the **Storage: $Default** category.

The standard configuration of the default storage policy is as follows:

- Replication Factor (RF) is set to **2**.
- Encryption is set to **Inherit from Cluster**.
- Compression is set to **Inline**.
- No values are set for QoS.

Limitations for Default Storage Policy

- If the name of an existing storage policy conflicts with the **Default Storage** policy during its creation, Prism Central creates the **Default Storage** policy but does not issue any alert. Rename the existing policy. The **Default Storage** policy cannot be updated.
- When you create or update an entity like a VM or a VG,
  - The default storage policy (**Enable 'Default-Storage' policy** toggle switch) is not enabled for the entity by default.
  - If you assign a category associated with a non-default storage policy to an entity and also enable the **Enable 'Default-Storage' policy** toggle switch, the non-default storage policy gets precedence over the default storage policy. The default storage policy is not applied to the entity in such a case.
- **Storage: $Default Category**

  The **Storage: $Default** category is used to assign the default storage policy to an entity such as a VM or a VG. You cannot associate any other storage policy with this category. Nutanix recommends that you do not associate any other policy with the **Storage: $Default** category or make any other changes to this category.

  Do not assign any other category that is already associated with another storage policy to the entity, such as a VM or VG, if you want to enable the **Enable 'Default-Storage' policy** switch for that entity. If you enable the **Enable 'Default-Storage' policy** switch for an entity that is already associated with another category, the **Storage: $Default** category is enabled, but the storage policy associated with the other category overrides the default storage policy.
- **Edit the Default Storage Policy**

  You cannot edit the default storage policy. You can only apply it to an entity by associating the entity with the **Storage: $Default** category, enabling the **Enable 'Default-Storage' policy** switch for that entity, and ensuring that no other categories with storage policies are applied to that entity, thus overriding the default storage policy.

Storage Policies Summary View

The Storage policies summary view allows you to access a list of all the user-defined storage policies across registered clusters.

> **Note:** The **Storage Policies** page is available if you are logged on as a view-only user. However, you cannot create a storage policy or modify an existing one.

To access the storage policies summary view, perform the following steps:

1. Log in to Prism Central.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2982

2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Storage** > **Storage Policies** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The system displays the **List** tab by default with a summary view of storage policies across all registered clusters. When you open the **Storage Policies** page for the first time, Prism Central displays the **Introducing 'Default Storage Policy'** page. Select **OK, Got it** to go to the **List** tab of the **Storage Policies** summary view.

   For more information on the default storage policy, see Default Storage Policy on page 509.

Table 152: Storage Policies Page - Field Description

Field	Description	Values
Name	Displays the name of the Storage Policy. You can click the name to view the details page of the selected storage policy. The default storage policy (see Default Storage Policy on page 509) is named **Default Storage** and marked `SYSTEM`.	(Name of storage policy)
Replication Factor	Displays the Replication Factor selected.	Inherit from Container or 2 or 3
Encryption	Displays the encryption mode selected.	Enabled or Inherit from Cluster
Compression	Displays the compression mode selected.	Inline or Post Process (if On) Off Inherit from Cluster
Throttled Throughput (IOPS)	Displays the throttled throughput value in terms of IOPS.	(Integer number)
Throttled Throughput (MB/s)	Displays the throttled throughput value in MBps.	(Integer number)
Total Categories	Displays the total number of categories that are associated with the storage policy.	(Integer number)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2983

Field	Description	Values
Realized Entities	Indicates the number of entities to which the storage policy is applied. **Note:** A single storage policy can be applied to multiple entities. Multiple storage policies cannot be applied to a single entity.	(Integer number)

You can perform the following actions for the storage policies in the **Storage Policies** summary view:

- Access the detailed information about an individual storage policy. For more information, see Storage Policy Details View on page 514.
- Create a storage policy. For more information, see Creating a Storage Policy on page 520.
- Update, clone, or delete a storage policy. For more information, see Managing Storage Policies on page 525.

  Note: You cannot update or delete the **Default Storage** policy. You can only clone the **Default Storage** policy. Cloning the default storage policy does not create another default policy. It creates another non-default storage policy that you can modify to suit the needs of your deployment.

- Filter the storage policies list using **Filters** pane. For more information on **Filters** pane, see Filters Pane on page 55.

  For field details, see Table 152: Storage Policies Page - Field Description on page 512.

- Export the table that contains the list of storage policies and their information to a file in a CSV format. For more information on **Export** option, see Export on page 59.
- Use the **Actions** dropdown menu to update, clone, or delete a storage policy. For more information, see Managing Storage Policies on page 525.

Associations Tab

The **Associations** tab displays the compliance state of the storage policies across the registered clusters.

The following table describes the fields that appear in the **Associations** tab of **Storage**page:

Note: A dash (-) is displayed in a field when a value is not available or applicable.

Table 153: Storage Associations Tab - Field Description

Parameter	Description	Values
Name	Indicates the name of the Storage Policy. You can click the name to view the details page of the selected storage policy.	(Name of storage policy)
Associated Categories	Displays the number of categories associated with the storage policy.	(Integer number)
Unrealized Entities		

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2984

Parameter	Description	Values
VMs	Displays the number of VMs that the system considers for compliance check and to apply the storage policy.	(Integer number)
VGs	Displays the number of VGs that the system considers for compliance check and to apply the storage policy.	(Integer number)
Realized Entities		
VMs	Indicates the number of VMs to which the storage policy is applied.	(Integer number)
VGs	Indicates the number of VGs to which the storage policy is applied.	(Integer number)
Compliance for Realized Entities	Provides a link to a dialog window that displays the state of compliance of the VMs and VGs covered by the policy.	(Integer) **in Progress** (Integer) **Non Compliant** (Integer) **Compliant**

Figure 187: Storage Policy Compliance Pop-up Window

You can filter the storage policies list based on the storage policy name using **Filters** pane in the **Associations** tab. For more information, see Filters Pane on page 55.

For more information about Storage Policies, see Storage Policy Management on page 506.

- For information about creating or updating storage policies, see Creating a Storage Policy on page 520.
- For information about deleting storage policies, see Deleting a Storage Policy on page 527.

Storage Policy Details View

To access the details page for a storage policy, go to the storage policy **List** tab (see Storage Policy Management on page 506) and click the name of the storage policy you want to view the details of. You can also access the

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2985

details page by clicking the name of the storage policy wherever that name appears, such as in a dashboard widget or search result.

Figure 188: Storage Policies details view

The storage policy details page includes the following tabs:

- **Summary**—displayed by default when you open the storage policy details page. This tab provides information about the storage policy summarized into widgets.
- **Entities**—displays the list of entities including VMs and VGs associated with the storage policy.

The **Summary** tab of an individual storage policy provides the following widgets:

- **Configuration** - Displays the configuration attributes of the storage policy.
- **Associations**- Displays the count of associated realized and unrealized VMs, VGs,and their categories.
- **Compliance Status** - Displays the compliance status of the entities associated with this policy. If the policy is being applied and the compliance status is not yet known, the status is displayed as **In Progress**. For information about the fields available in the widgets, see Storage Policy Widgets- Field Details on page 515.

<*Action*> available above the widgets. Click the appropriate <*Action*> , such as **Update**, **Clone**, or **Delete** to run that administrative action on the storage policy. For more information about how to perform any <*Action*>, see Managing Storage Policies on page 525.

Storage Policy Widgets- Field Details

The following table describes the fields in the **Configuration**, **Associations**, and **Compliance Status** widgets.

Table 154: Storage Policy Widgets- Field Description

Field	Description	Values
Configuration widget		
Replication Factor	Indicates the Replication Factor selected.	Inherit from Container or 2 or 3
Encryption	Indicates the encryption mode selected.	Enabled or Inherit from Cluster

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2986

Field	Description	Values
Compression	Indicates the compression mode selected.	Inline or Post Process (if On) Off Inherit from Cluster
QoS Metric (Throttled IOPS)	Indicates the throttled throughput value in terms of IOPS.	(Integer number)
QoS Metric (Throttled Throughput)	Indicates the throttled throughput value in MBps.	(Integer number)
Associations widget		
Categories	Displays the count of VM and VG categories mapped to the selected storage policy.	(number of VM and VG categories)
Realized Entities	Indicates the number of entities that the storage policy is applied to. The storage policy acts on these entities and defines their storage properties.	(Integer number)
Non-realized Entities	Indicates the number of entities that the storage policy is not applied to. The storage policy is associated with these entities but does not act on them. When a storage policy is not applied to an entity like a VM or a VG, then the entity is listed as **Non-realized Entity**.	(Integer number)
Compliance Status widget		
Realized Entities	Indicates the number of entities that the storage policy is applied to. **Note:** A single storage policy can be applied to multiple entities. Multiple storage policies cannot be applied to a single entity.	(Integer number)
Compliance State	Indicates the number of entities in each of the following compliance states: • In Progress: Indicates the number of entities that the policy has already been applied to and data transformation of entity's data (compliance) is in progress. • Compliant: Indicates the number of entities that are in compliance. • Non Compliant: Indicates the number of entities that are not in compliance	Compliant, In Progress, or Non compliant

Entities Tab

The **Entities** tab enables you to view the realized and non-realized VMs for the selected storage policy:

- Select **Realized** from the **Entities** tab dropdown menu to view the entities that the storage policy is applied to.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2987

- Select **Unrealized** from the **Entities** tab dropdown menu to view the entities that the storage policy is not applied to.

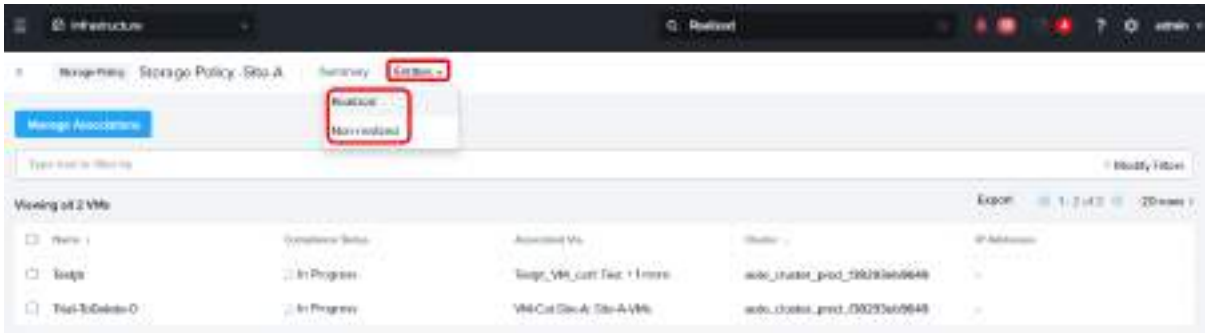


Figure 189: Entities Tab

The following table describes the fields that appear in the **Entities** tab of storage policies details view:

Table 155: Entities Tab - Field Details

Field	Description	Values
Name	Indicates the name of the entity like VMs and VGs.	(entity name such as the name of the VM or VG)
Compliance Status	Indicates the compliance status of the entity as **In Progress**, **Compliant** or **Non Compliant**.	In Progress | Compliant | Non Compliant
Associated Via	Indicates the categories to which the entity and the storage policy are concurrently associated. The storage policy is associated with the entity because the storage policy is associated with this category that is associated with the entity. For example, StoragePolicy1 is associated with CategoryA which is in turn associated with VM1. The category displayed in **Associated via** is CategoryA. The other categories associated with VM1 but not associated with StoragePolicy1 are not displayed here.	(category name)
Cluster	Indicates the name of the cluster on which the entity resides.	(cluster name)
IP Addresses	Indicates the IP addresses configured for the entity.	(IP address)

You can perform the following actions for the storage policies in the **Entities** tab:

- Filter the storage policies list using **Filters** pane. For more information, see Filters Pane on page 55.

  For field details, see Table 155: Entities Tab - Field Details on page 517.
- Export the table that contains the list of storage policies and their information to a file in a CSV format. For more information about this option, see Export on page 59.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2988

Storage Policy Compliance

When you create a policy like a storage policy and apply it to entities like VMs and VGs, there is no way to know whether the application configured or transformed the entities to the parameters set in the policy. You need a mechanism to track the application of the policy and the changes made to the entities in alignment with the parameters set in the policies. Compliance provides that mechanism to track the application of policies and the transformation of the entities and provide feedback on the status at an entity level.

The compliance process begins when you associate a storage policy to a category and, therefore, to entities that the category is assigned to. The association applies the storage policies to the entities that the category is assigned to. For the several reasons, a storage policy is not applied to an entity.

After application, the parameters of the entities such as replication factor, encryption, and compression are transformed according to the configuration of the storage policy. Such transformation (compliance) does not occur for some entities that the category may be assigned to, any of the following, but not restricted to, reasons:

- Incompatible hypervisor: The node is running a hypervisor or version that does not support storage policies. Only AHV supports storage policies.
- Incompatible AOS version: The cluster is running an AOS version that does not support storage policies.
- Multiple storage policies applied: When you apply multiple storage policies to an entity, only one is applied. Other storage policies report that entity as non compliant.

Compliance, thus, tracks the process from application to transformation and reports the status in the storage policy **Summary** tab. AOS applies the storage policy parameters in a specific order that **Compliance** also uses to report status. This order of implementation and tracking of the storage policy parameters is as follows:

- Replication Factor: Replication Factor indicates data availability which is the most factor for an entity.
- Encryption: Encryption indicates data security which is the second most important factor for an entity.
- Compression: There may be cases where compression may not be possible for an entity. So in such a case, if Replication Factor and Encryption parameters are applied and entity data is transformed accordingly, then the compliance engine reports the state for the entity as **Compliant**.
- Throughput: This parameter has lower priority in implementation and compliance reporting. The implementation is similar to the Compression parameter.

Compliance reports the states separately for VMs and VGs, even if the VMs or VGs are tagged to each other. For example, if VM1 is tagged to VG1. VM1 is associated with Category1 and VG1 is associated with Category2. storage policies SP1 and SP2 are associated to Category1 and Category2 respectively. **Compliance** reports the states of VM1 and VG1 separately. It reports the states separately even if VM1 and VG1 are associated to the same Category1, and hence storage policy SP1.

Compliance reports the following states:

Realized Entities

The compliance engine reports this state when a storage policy is applied to the entity. Application of storage policy means that the parameters set in the storage policy are identified for the entity that it is applied to. So when the system reads the storage policy and identifies the Replication Factor, Encryption, Compression and throttled throughput QOS metric parameters for the entity, the compliance engine reports the entity as **Realized Entity**.

Non-realized Entities

There may be several reasons why a storage policy could not be applied to (realized on) an entity. For example, storage policies cannot be applied to ESXi VMs (non-Nutanix entity).

In Progress

Compliance engine reports this state when the one or more parameters set in the storage policy are applied to an entity and the entity data is being transformed to comply with those parameters.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2989

Compliant

The compliance engine reports this state when the transformation of the entity data is complete and all the high priority parameters like Replication Factor and Encryption have been set for the entity in accordance with the settings in the storage policy.

Non Compliant

The compliance engine reports this state when the transformation of the entity data could not be completed and one or more high priority parameters like Replication Factor and Encryption could not be set for the entity in accordance with the settings in the storage policy. **Non Compliant** also indicates unknown state of transformation.

The compliance states are displayed on the storage policy details page. For more information, see Storage Policy Details View on page 514.

Storage Policy Based Replication Factor

Replication Factor is the number of replication copies of any data made on the cluster. For example if you have a Replication Factor of 2 for a container, then the data in that container is written twice on nodes in different fault tolerance domains. This is dependent on how you have configured the fault tolerance domains.

You can use a storage policy to apply Replication Factor to entities like VMs and VGs. When you apply a storage policy to an entity, the Replication Factor defined in the storage policy is applied to the entity. Storage policy compliance checks whether the entity data is compliant with the Replication Factor setting in the storage policy. You can use a storage policy to apply Replication Factor with Deduplication enabled.

> **Note:** Prism Central supports Policy-based replication factor configuration for entities on storage containers that have Deduplication enabled.

Limitations

Configuring Replication Factor for entities using storage policies is not possible in some cases.

- Storage Policies do not support setting Replication Factor of 1. You can only use a storage policy to set Replication Factor (RF) 2 or 3.
- Prism Central does not support Policy-based replication factor configuration for entities on storage containers that have Erasure Coding.
- A storage policy Replication Factor setting is not applied when the RF setting in the storage policy is higher than the Replication Factor setting in the cluster.

  For example, if the RF of a cluster is 2, but a storage policy with RF 3 is applied to an entity in that cluster, the entity is reported as **Realized** but **Non-compliant**.
- Shared data between a VM with Replication Factor 2 and another VM with Replication Factor 3 configurations complies with Replication Factor 3. In other words, the shared data has 3 copies.
- A cloned entity like a cloned VM or VG inherits the category, and the storage policy attached thereto, of the original entity that it is cloned from. Thus, the storage policy engine applies the storage policy that is associated with the inherited category to the cloned entities.

Storage Policy Based Encryption

Storage policies allow you to make data-at-rest encryption choices at the entity level.

Deployments can continue to have data-at-rest encryption capabilities scoped for the entire cluster. Storage policy provides the additional option to control the encryption scope decisions at the entity (VM or VG) level.

> **Note:** Prism Central does not support Policy based encryption for storage containers on which Erasure Coding or Deduplication is enabled.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2990

The Key Manager System (KMS) choice is configured as a cluster-wide setting, leveraging either Nutanix Built-in Native Key manager or leveraging a third party Key Manager. As part of the Key manager configuration, the scope of encryption-at-rest is defined either as Cluster-wide or specific entity-scoping. Entity-scoping means that the encryption-at-rest scope is defined at the container or the data policy level.

Important:

- When you select the cluster, you can manage the KMS type by clicking **Actions** > **Manage KMS Type**.
- From Prism Central, if you try to configure storage policy based encryption for any single VM or Category entity without enabling **Entity Encryption** on that cluster, the entity is marked as **Non Compliant**, and Prism Central does not transform the entity data to be encrypted.

  Log on to Prism Central and perform the following steps:

  1. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Hardware** > **Clusters**
  2. Select the target cluster, and choose **Enable Data-at-Rest Encryption** from the **Actions** dropdown menu.
  3. In the **Data-at-Rest Encryption** window, specify the following information:

     - **Select Encryption Type** - Select **Entity Encryption** and click **Save Encryption Type**.
     - **Select Key Management Server (KMS)** - Select **Native KMS (Local)** and click **Enable Encryption**.

     The system prompts you to confirm the action.
  4. Enter **SET** in the **Type SET to Confirm** window, and click **Set Encryption**

When a storage policy is used, AOS data for the VM or VG is encrypted on the disk for all the vDisks attached to the VM or VG. The main features include:

- Once encryption is enabled in a policy, it cannot be disabled. If the VM or VG moves out of the policy or the policy is deleted, then the new writes to the VM or VG are unencrypted and existing data remains encrypted.
- The system automatically generates a unique key for each storage container.
- Multi-tenant requirements having a unique key per tenant can be fulfilled by ensuring that the set of VMs belonging to each tenant is mapped to its own container. Nutanix recommends having only 50 tenants or less per cluster.
- Encryption can be enabled for new and existing VMs or VGs.
- Storage policies supports Volume Group. For any VG attached to a VM that is associated with a storage policy enabling encryption, the data stored in the VG is encrypted only if the storage policy associated with the VG also enables encryption. In other words, data encryption in a VG attached to a VM is independent of the storage policy associated with the VM. It is not derived from the storage policy applied to the VM that the VG is attached to.
- Unencrypted VM needs to remain unencrypted during the cloning process.
- Shared data between the encrypted entities and unencrypted entities is encrypted.

For information about containers, see the Storage Management section in the *Prism Element Web Console Guide*.

For information about configuring key manager, see the Security Guide.

Creating a Storage Policy

You can create or update a storage policy in Prism Central only.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2991

Before you begin

Ensure that you have created the necessary categories and assigned the entities such as VMs and VGs to the categories.

For more information about how to create a category, see Creating a Category on page 459.

For more information about how to assign a category to the entity, see Assigning a Category on page 460.

About this task

Prism Central provides a two-step framework to create a storage policy that involves the following steps:

- **Configuration** step - Enables you to configure the data replication (Replication Factor), data security (Encryption), data reduction (Compression) and QoS (IOPS or Throughput throttling) aspects of the storage policy.
- **Association** step - Enables you to associate the storage policy with categories that the entities (like VM or VG) are associated with.

Procedure

To create a storage policy, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and go to **Storage** > **Storage Policies** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The system displays the **List** tab by default with summary view of storage policies across all registered clusters.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2992

3. Click **Create Storage Policy**.
   The system displays the **Create Storage Policy** window with the **Configuration** step.

Figure 190: Create Storage Policy - Configuration Step

Configure the following fields in the **Configuration** step. Select a defined (non-default) value for a least one of the properties.

Table 156: Configuration Step - Field Description

Field	Description and Values
Name	Enter a unique name for the storage policy. **Note:** Do not repeat a name previously used for another storage policy. The built-in pre-check fails if you enter a non-unique name.
Data Redundancy	

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2993

Field	Description and Values
Replication Factor	Select one of the following values from the dropdown list. • **Inherit from Container** (default)—the category or entity inherits the replication factor (2 or 3) configuration from the container. This is the default value for Replication Factor. • **2**—to enable replication factor 2 (replication factor 2—Original plus 1 copy) through the storage policy. • **3**—to enable Replication Factor 3 (replication factor 3—Original plus 2 copies) through the storage policy. **Note:** The replication factor selected must be supported by the fault tolerance of the cluster. For example, if the fault tolerance of the cluster is 1N/1D, then selecting replication factor **3** in the policy leads to non-compliance.
Data Security	
Encryption Value	Select one of the following values from the dropdown list. • **Enabled**—to enable encryption through the storage policy. **Note:** After you enable encryption using storage policies, you cannot disable it. • **Inherit from Cluster** (default)—the category or entity inherits the encryption configuration from the cluster. This is the default value for Encryption.
Data Reduction	
Compression Value	Select one of the following values from the dropdown list. • **On**—to enable compression. If you select **On** then you must select the type of compression that you want to apply. You can select **Inline** compression (default) or **Post Process** compression. If you select **Post Process**, the data is compressed with some delay (up to 3600 seconds) that is set by the system default. • **Off**—to disable compression. • **Inherit from Cluster** (default)—the category or entity inherits the compression configuration from the cluster. This is the default value for compression.
IO Performance (Also see the *Relationship between Block Size, IOPS and Throughput* table for information about how Throttle IOPS or Throughput is calculated based on block size)	
Quality Metric	Select one of the following values from the dropdown list. • **Throughput** • **IOPS**

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2994

Field	Description and Values
Throttled Value	Provide a numeric value. **Note:** For **IOPS** the value must be greater than 99 or equal to -1 (minus 1).

Throttle IOPS or Throughput Relationship: Set the Throttle IOPS or Throughput based on the block size. Nutanix uses a fixed block size of 32k. For example, with a block size of 32K, if you set a Throttle IOPS value of 1000 IOPS, the Throttle Throughput would be 31.25 MBps. See the table.

Table 157: Relationship between Block Size, IOPS and Throughput

Block Size	IOPS	Throughput (MBps)
8k	1000	7.81
16K	1000	15.63
32K	1000	31.25
64K	500	31.25
128K	250	31.25

4. Click **Next**.

   If you did not select or enter an appropriate value and the pre-checks failed, the relevant error is displayed below the field that failed the pre-check. Select or enter an appropriate value, and click **Next** again.

   The system displays the **Association** step.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2995

5. In the **Association** step, select the category or categories you want to associate with the storage policy in the **Add Category** field.

   Type the first 2-3 characters of the category name you want to associate with in the **Add Category** field. The system displays a dropdown list of the matching categories based on the typed entry.

   Use the Add icon and Remove icon to add and remove the required categories in the**Associated Categories** list.

   > **Note:** You can add multiple categories for one storage policy. When you associate a category with one storage policy, you cannot associate the same category with another storage policy.

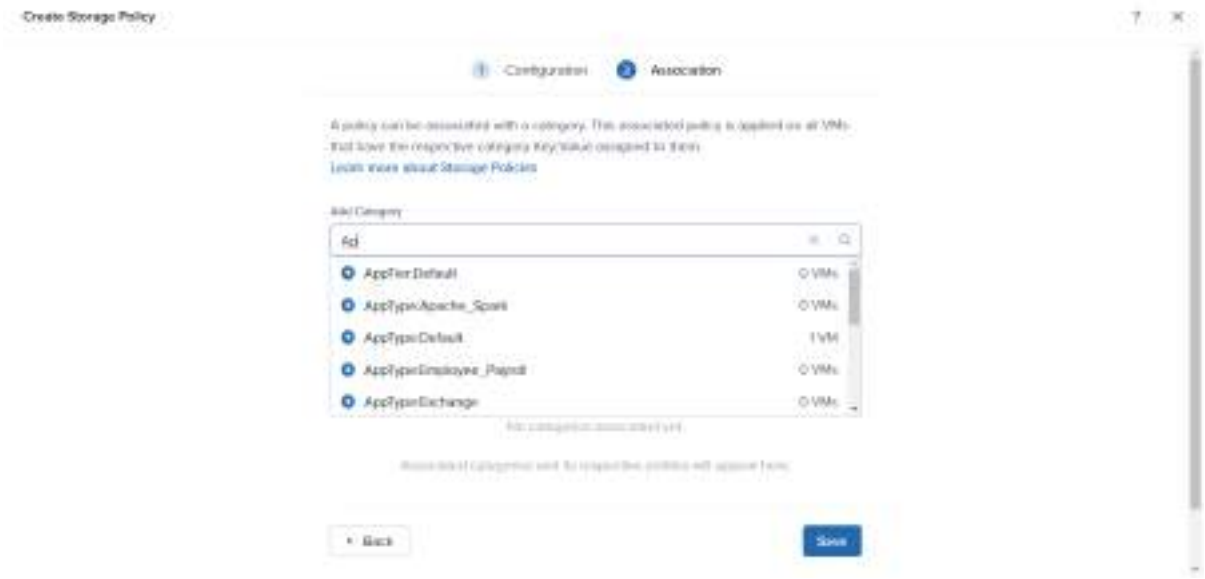


Figure 191: Create Storage Policy - Association Step

6. Click **Save** to save the storage policy.

Managing Storage Policies

This section describes how to update, clone, and delete the storage policies in Prism Central

About this task

You can perform the following actions to manage the Storage policies in Prism Central:

- Update a Storage policy.

  > **Note:** You cannot update the **Default Storage** policy.

- Clone a Storage policy.

  > **Note:** You can clone the **Default Storage** policy.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2996

- Delete a Storage policy.

  > **Note:** You cannot delete the **Default Storage** policy.

  When you delete a storage policy, the entities associated with the deleted storage policy return to their default state, or the configurations from any other storage policy associated with the category are applied to the entities. Nutanix recommends that you remove all the categories and entities associated with the storage policy.

  When a storage policy is deleted, it is marked for removal in the database. Prism Central stops displaying that storage policy. The process stops applying the storage attributes of the policy and instead applies the storage attributes configured for the container. However, the VM continues to display the storage policy as if it still applies until the next system scan occurs and the policy is removed from the VM information. A Kanon service scan occurs every 1800 seconds and refreshes the information.

- Manage associations.

  > **Note:** You cannot update the category association of the **Default Storage** policy. The **Default Storage** policy is associated with the **Storage:$Default** category.

Procedure

To update a storage policy, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Storage** > **Storage Policies** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default.
3. Select the target storage policy check box, and choose **Update** from the **Actions** dropdown menu.
4. Update the information as per your requirement in the **Update Storage Policy** window, and click **Save**. For field details, see Creating a Bandwidth Throttling Policy on page 499.

   To delete the storage policy, select the target storage policy check box and choose **Delete** from the **Actions** dropdown menu. The command prompt prompts you to confirm the deletion action. Click **Delete** to confirm the delete action.

   > **Note:** You can also click **Preview changes** to view the categories and entities that are affected by the deletion of the storage policy.

   To clone the storage policy, select the target storage policy check box and choose **Clone** from the **Actions** dropdown menu. The system displays the **Create copy of <Storage Policy-Name>** window with the same values populated in it as specified for the selected storage policy.

   > **Note:** The **<Storage Policy-Name>** indicates the actual name of the storage policy you selected to clone.
   >
   > During cloning, the categories to which the original storage policy is attached are removed. The clone storage policy does not inherit the categories from the original storage policy.

   Enter the field details as per your requirement, and click **Save**. For field details, see Creating a Storage Policy on page 520.

   To update the category associations only in an existing storage policy, navigate to the **Entities** tab in Storage Policy Details View on page 514and click **Manage Associations**. Type the first 2-3 characters of the

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2997

category name in the **Add Category** field and use the Add icon and Remove icon to add and remove the required categories in the**Associated Categories** list.

> **Note:** You can associate multiple categories with one storage policy. When you associate a category with only one storage policy. You cannot associate one category with multiple storage policies
>
> The **Storage: $Default** category is associated with the **Default Storage** policy. Do not associate the **Storage: $Default** category with any other storage policy.

Deleting a Storage Policy

You can delete a storage policy. When you do so, the entities associated with the deleted storage policy return to their default state or the configurations from any other storage policy that is associated with the category are applied to the entities.

Before you begin

Nutanix recommends that you remove all the categories and entities associated with the storage policy.

About this task

When a storage policy is deleted, it is marked for removal in the database. Prism Central stops displaying that storage policy. The process stops applying the storage attributes of the policy and instead applies the storage attributes configured for the container. However, the VM continues to display the storage policy as if it still applies, until the next system scan occurs and removes the policy from VM information.

Remove associations of the storage policy to categories in the **Categories** or **Entities** tabs of the storage policy details page.

Delete a storage policy from the **Storage Policies** dashboard or the **Summary** tab of the storage policy details page.

Do the following to delete a storage policy:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 2998

Procedure

1. Click the name of the storage policy. On the storage policy details page, click **Delete**.
   The **Delete <storage-policy-name>** dialog box is displayed as follows:

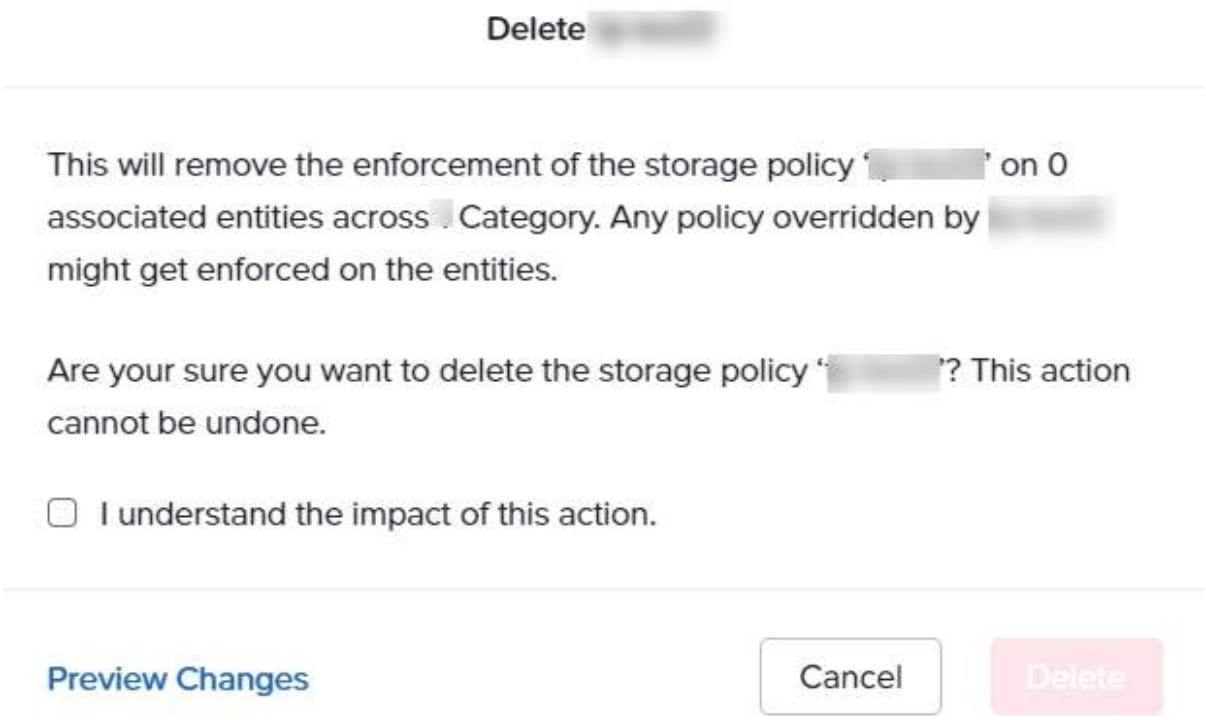


Figure 192: Delete Storage Policy

2. (Optional) Click **Preview Changes** to view the **Changes Preview** dialog box.

   The **Changes Preview** dialog box lists the categories and entities that are affected by the deletion of the storage policy.

   Tip: If you have already removed all the associations of the storage policy, then the list of categories and entities is empty.

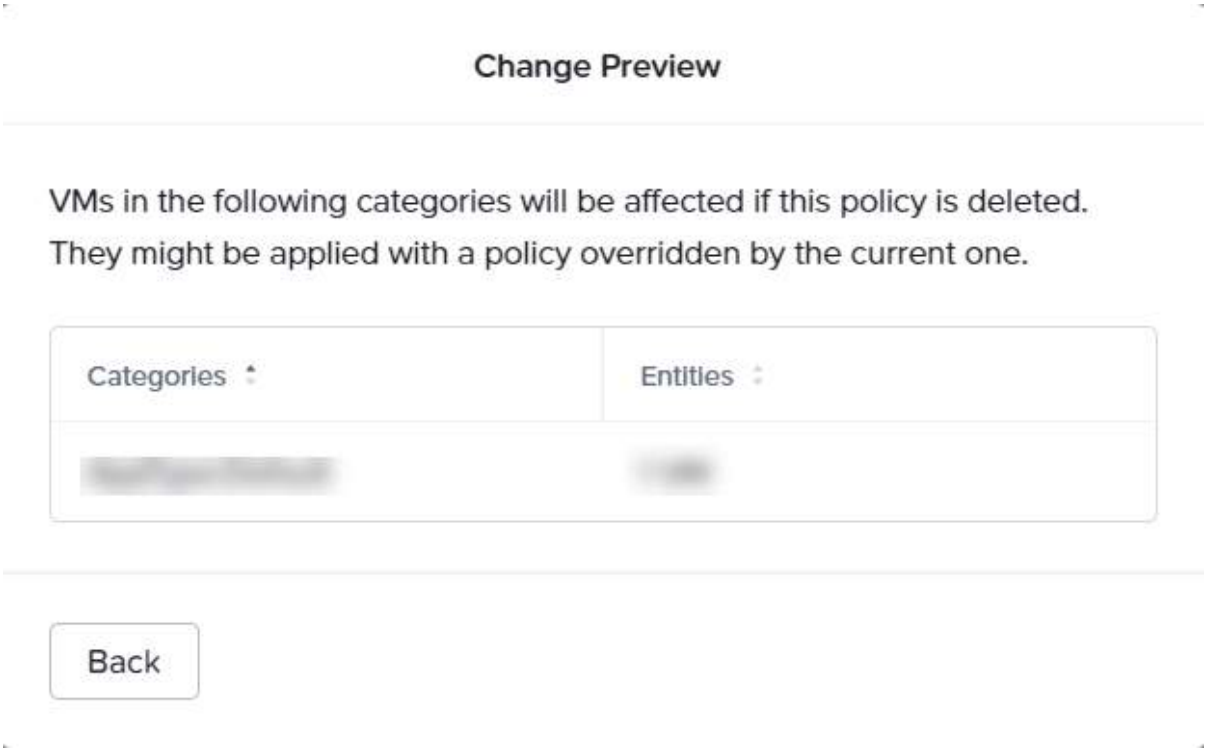


Figure 193: Change Preview

   After you preview the impact, click **Back** to go back to the **Delete <storage-policy-name>** window.

3. Select the **I understand the impact of this action.** checkbox.

   The **Delete** is enabled only after you select the **I understand the impact of this action.** checkbox.

4. Click **Delete**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3000

PRISM SELF SERVICE ADMINISTRATION

This section describes how to configure and administer Prism Self Service.

The Prism Self Service feature allows you to create projects where consumers of IT infrastructure within an enterprise—individual users or teams such as development, test, and DevOps—can provision and manage VMs in a self-service manner, without having to engage IT in day-to-day operations.

For information about user roles and configuration workflow for Prism Self Service, see Prism Self Service Setup on page 530.

Prism Self Service Setup

Prism Self Service represents a special view within Prism Central. While Prism Central enables infrastructure management across clusters, Prism Self Service allows end users to consume that infrastructure in a self-service manner. Prism Self Service uses the resources provided by a single AHV cluster.

Important: Prism Self Service is only supported with AHV hypervisor, and not supported with other hypervisors.

Note: A SelfServiceContainer storage container is created on the target cluster and used by Prism Self Service for storage and other feature operations. To ensure proper operation of these features, do not delete this storage container. For more information about storage containers, see Storage Container Management on page 272

Prism Self Service Roles

There are three roles to consider when configuring Prism Self Service:

1. *Prism Central administrator*. The Prism Central administrator adds an Active Directory or OpenLDAP directory service that includes the pool of self-service users and (optionally) creates one or more self-service administrators. Prism Central administrators also create VMs, images, and network configurations that may be consumed by self-service users.
2. *Self-service administrator*. The self-service administrator performs the following tasks:

   - Creates a project for each team that needs self service and adds users and groups to the projects.
   - Configures roles for project members. A project member can access only the entities or perform only the actions defined in the role assigned to that project member.
   - Publishes VM templates and images to the catalog.
   - Monitors resource usage by various projects and its VMs and members, and then adjusts resource quotas as necessary.

   It is optional to configure a separate self-service administrator because a Prism Central administrator can perform any of these tasks. However, if you would like to authorize users to administer end-user VM or application provisioning, you can use this role to give them access to virtual infrastructure without giving them access to physical infrastructure.

   Caution: Self-service administrators have full access to all VMs running on the Nutanix cluster, including infrastructure VMs not tied to a project. Self-service administrators can assign infrastructure VMs to project members, add them to the catalog, and delete them even if they do not have administrative access to Prism Central. Consider these privileges when appointing self-service administrators, and make sure to communicate to self-service administrators the need to exercise caution when working with infrastructure VMs.

   After a Prism Central administrator has designated a user as a self-service administrator, the Prism Central administrator cannot limit the user's privileges. Therefore, if you plan to delegate self-service administration responsibilities to an Active Directory or OpenLDAP directory group, be sure that you want to delegate the responsibility to all the users in the group. If the user group is large or includes users that must not have self-service administrator privileges, Nutanix recommends that you create a

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3001

separate Active Directory or OpenLDAP directory group for the users to whom you want to delegate self-service administration responsibilities.

3. *Project user*. These are the users assigned to a project by a self-service administrator. They can perform any action that the self-service administrator grants them. The permissions are determined by the roles assigned to the users and groups in the project. When project users log in, they see a custom self-service GUI interface that shows only what the role permissions allow. Project users create and manage only what they need.

Prism Self Service Workflow

To configure Prism Self Service, perform the following tasks:

Table 158: Prism Self Service Workflow

Sequence	Tasks	Description
1	Specify an Active Directory or OpenLDAP directory service for Prism Self Service.	For more information, see Configuring Centralized Authentication (Active Directory/OpenLDAP) information in *Security Guide*.
2	Add one or more self-service administrators.	For more information, see Managing Prism Self Service Admins information in *Prism Central Admin Center Guide*.
3	Create a project for each team that needs self service and add users and groups to the projects.	For more information, see Project Overview information in *Prism Central Admin Center Guide*.
4	Configure roles for project members. You can also allow project members to create their own VMs	For more information, see Controlling User Access (RBAC) in *Security Guide*. **Note:** Role Based Access Control (RBAC) is an independent feature, so you can configure RBAC without configuring self service or creating projects. However, projects allow you to enforce RBAC in a more granular way.
5	Add VM templates and images to the catalog.	For more information, see Catalog Management on page 266.
6	Create VMs as needed and assign them to project members as appropriate.	For information about how to create a VM, see Creating a VM (Self Service) on page 532 and Creating a VM from Catalog Items (Self Service) on page 532. For information about how to assign a VM to a project member, see Assigning a VM to a Project Member on page 539.
7	Monitor resource usage for the projects and adjust resource quotas as needed.	For more information, see the following information in *Prism Central Admin Center Guide*: • Project Details View - To monitor resource usage for a project. • Quota Policy Overview - To define the resource quotas.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3002

Creating a VM (Self Service)

About this task

When you are logged in to Prism Central as a self-service administrator or a project member, you can create a VM if you have the required permissions to create a VM.

Procedure

In Prism Central Self Service framework, you can create a VM in the following two ways:

- Using the workflow that an admin user follows. For more information, see Creating a VM through Prism Central (AHV) on page 130.
- Using a source file (image or VM template) that is stored in the Prism Central catalog. For more information, see Creating a VM from Catalog Items (Self Service) on page 532.

  For information about Prism Self Service, see Prism Self Service Administration on page 530.

Creating a VM from Catalog Items (Self Service)

This section describes how to create a VM from catalog items.

About this task

When you are logged on as a self-service administrator or a project member with permission to create a VM, you can create a VM based on a source file stored in the Prism Central catalog. For information about how to add a source file (image or VM template) to a catalog, see Adding a Catalog Item on page 268.

For information about Prism Self Service, see Prism Self Service Administration on page 530.

> **Note:** If you are not logged in as a self-service administrator or a project member and you want to create a VM without the source file stored in the Prism Central catalog, you can follow the procedure as described in Creating a VM through Prism Central (AHV) on page 130.

Procedure

To create a VM from catalog items, perform the following steps:

1. Log in to Prism Central as a self-service administrator or a project member.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3003

2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
The system displays the **List** tab by default with all the VMs across registered AHV clusters.

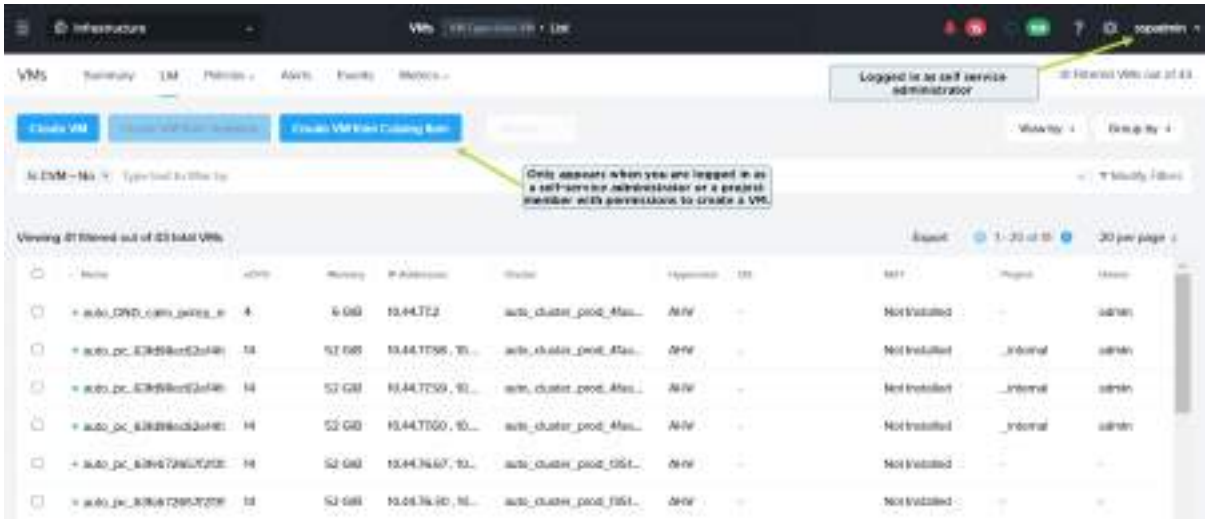


Figure 194: VM Summary View - Self Service Administrator login

3. Click **Create VM from Catalog Item**.

> **Note:** The **Create VM from Catalog Item** option only appears if you are logged in as self-service administrator or a project member with permissions to create a VM.

The system displays the **Create VM from Catalog Item** page.

4. In **Catalog Type**, select one of the following source for the VM:

» **VM Template** - Used to create a VM from a VM template in the catalog.

A VM template includes all the configuration information required to create a VM. You can use a template to quickly deploy a VM without specifying all the configuration information.

» **Image**- Used to create a VM from a mounted disk image.

Disk images can be CD-ROM images such as installer ISO images or images of hard drives that contain pre-installed applications and data. Disk images enable you to share data with other VMs, however you need to specify configuration information for the VM that you create using the disk image.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3004

5. In **Catalog Item** field, perform either of the following actions based on the source you select in the **Catalog Type** field:

   - If **VM Template** is selected as the source in the **Catalog Type** field, select the target VM template in the **Catalog Item** field. The available VM templates from the catalog are listed. If the target VM image does not appear in the list, you can search for it by name in the search field.

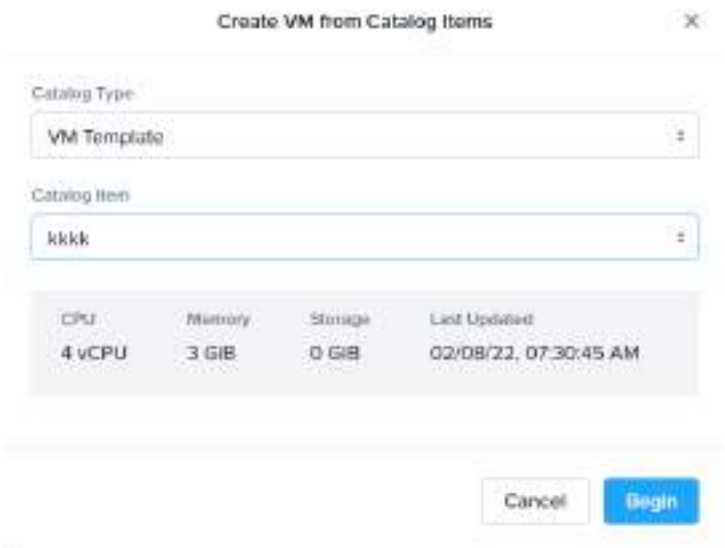


Figure 195: Create VM from Catalog Items

   - If **Image** is selected as the source in the **Catalog Type** field, select one or more of the disk images. The available disk images from the catalog are listed. If the target disk image does not appear in the list, you can search for it by name in the search field.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3005

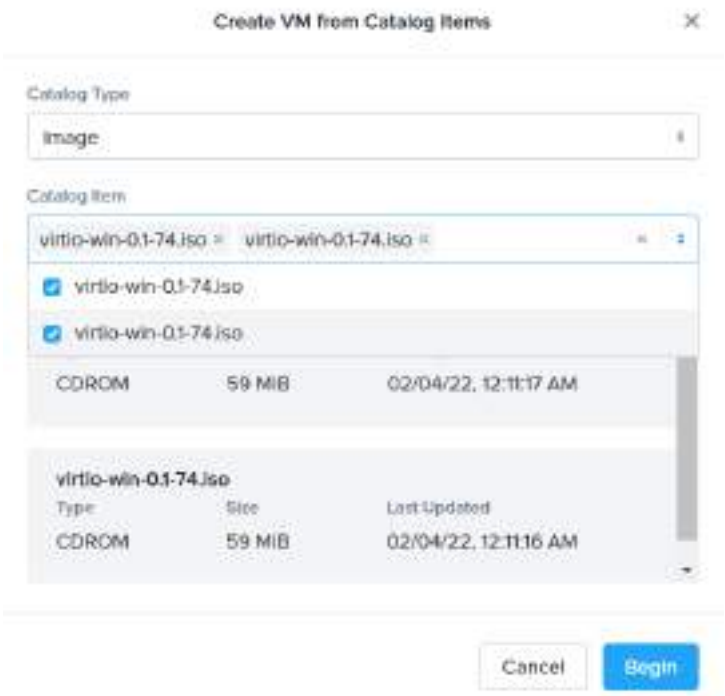


Figure 196: Create VM Window (Configuration)

6. Click **Begin**.

   The **Create VM** page appears.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3006

7. In the **Configuration** step, specify the following information:

   a. **Name**: Enter a name for the VM.

   b. **Project**: Select the project associated with this VM from the dropdown menu.

   c. **Cluster**: Select the target cluster from the dropdown menu on which you intend to create the VM.

   d. **Number of VMs**: Enter the number of VMs you intend to create. The VM names are suffixed with sequential numbers (1 to 5).

   e. **vCPU(s)**: Enter the number of virtual CPUs to allocate to this VM.

   f. **Number of Cores per vCPU**: Enter the number of cores assigned to each virtual CPU.

   g. **Memory**: Enter the amount of memory (in GB) to allocate to this VM.

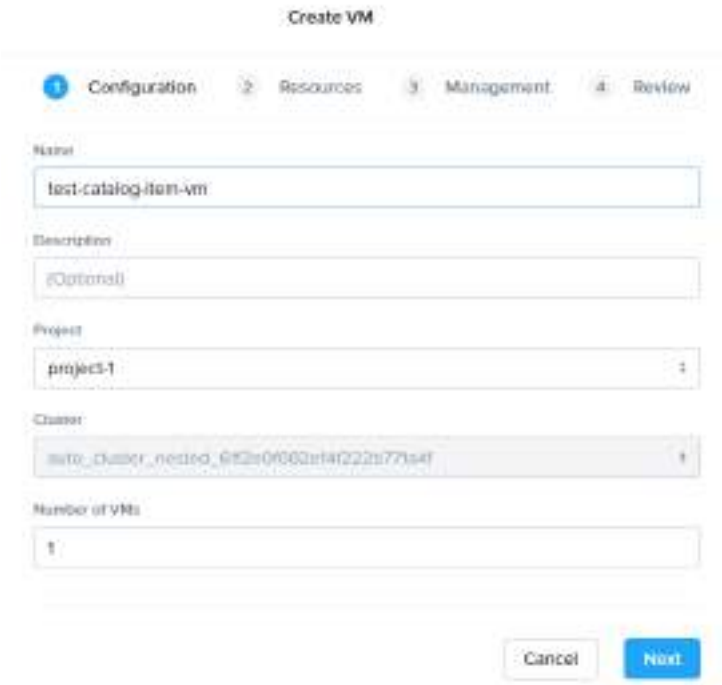


Figure 197: Create VM Window (Configuration)

8. In the **Resources** step, specify the following information.

   - **Disks**: Displays the disks and CD-ROMs attached to this VM.

     - If **VM Template** is selected as the source in **Catalog Type** field, the system displays a fixed list of devices. Select the device from which you want to boot the VM.
     - If **Image** is selected as the source in **Catalog Type** field, there are **+ New Disk** and **+ New CDROM** links above the list.

       - Click **+ New Disk** to add a disk. The system displays a new line at the bottom of the list. Specify the disk size and then click **Save** at the end of line to add the disk. The name and type field values are entered automatically.
       - Click **+ New CDROM** to add a CD-ROM. The system displays a new line at the bottom of the list. Click **Save** at the end of line to add the CD-ROM. All the field values are entered automatically.

     Repeat this action until you have added all the desired disks and CD-ROMs. When the list is complete, select the device from which you want to boot the VM.

9. In the **Resources** step, perform the following actions to configure the network interface for the VM:

   a. Click **Attach to Subnet**. The system displays the **Attach to Subnet** window.

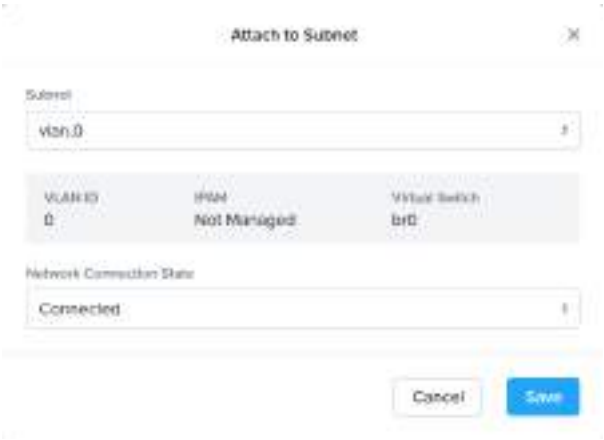


Figure 198: Attach to Subnet Window

   b. Select the target subnet from the **Subnet Name** dropdown menu.

      The list includes all defined networks. For more information, see Network Configuration for VM Interfaces information in *Prism Element Web Console Guide*.

   c. **VLAN ID**: This is a read-only field that displays the VLAN ID.

   d. **IPAM**: This is a read-only field that informs you if the subnet is IPAM managed or not.

   e. **Virtual Switch**: This is a read-only field that displays the name of the virtual switch associated with the subnet.

   f. Select the state for the network that you want it to operate in after VM creation in **Network Connection State** field. The options are `Connected` or `Disconnected`.:

   g. Click **Save** to create a network interface for the VM. The system returns to the **Create VM** window.

   h.

   Repeat this step to create additional network interfaces for the VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3008

10. In the **Resources** step, perform the following action to specify boot configuration for the VM:

    Select one of the following firmware to boot the VM in **Boot Configuration** field:

    » **Legacy BIOS Mode**: Select legacy BIOS to boot the VM with legacy BIOS firmware.

    » **UEFI BIOS Mode**: Select UEFI to boot the VM with UEFI firmware. UEFI firmware supports larger hard drives, faster boot time, and provides more security features. For more information about UEFI firmware, see the UEFI Support for VM section in the *AHV Administration Guide*.

11. (Optional) In the **Management** step, perform the following action to assign a VM category.

    Enter the category name or select one from the **Categories**dropdown menu. The policies associated with the category value are assigned to the VM.

    This field acts like a search field; it provides a list of matching categories as you enter a string. Select the desired category value when you see it in the list. You can repeat this step for as many categories as desired.

12. In the **Management** step, perform the following actions for guest customization:

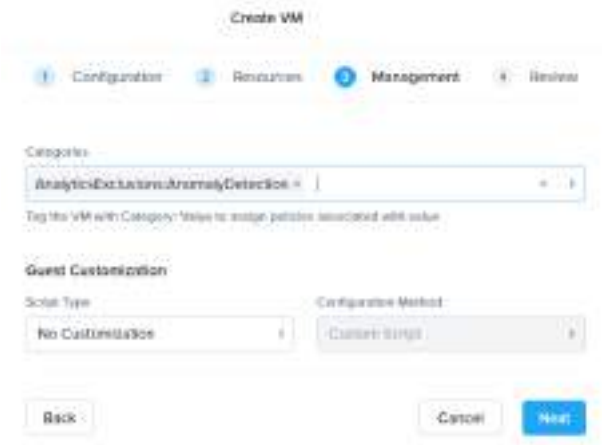


Figure 199: Create VM Window (Management)

- Select Cloud-init (for Linux VMs) or Sysprep (for Windows VMs) in the **Guest Customization** dropdown menu.
- Select the VM script customization type from the **Script Type** dropdown menu. The options are `No Customization`, `Sysprep(Windows)`, or `Cloud-init (Linux)`.
- Select the VM script customization method in the **Configuration Method** dropdown menu. This field is activated when the **Script Type** is either `Sysprep(Windows)` or `Cloud-init (Linux)`. The options are `Custom Script` or `Guided Script`.

The system displays the fields required to configure Cloud-init and Sysprep, such as options to specify a configuration script and the option to upload a script.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3009

13. To specify a user data file (Linux VMs) or answer file (Windows VMs) the script for unattended provisioning, perform one of the following actions:

    » If the file is available on your local computer, click **Upload Script**, and select and upload the file.

    » Create or paste the contents of the file in the text box below the **Upload Script**.

    Note: The script type supports the following file formats.

    - Sysprep: XML
    - Cloud-init (Linux): YAML, JSON, or Shell.

14. In the **Review** step, Click **Create VM** to create the VM and close the **Create VM** window.
    The system displays the new VM in the VMs Summary View on page 104.

Managing a VM (Self Service)

About this task

After you log in to Prism Central as a self-service administrator or a project member you can perform various actions on the VM to manage the VM configuration.

For information about all the actions, see Managing a VM through Prism Central (AHV) on page 143.

Note:

- The system allows you to perform only those actions for which you have permission.
- The available actions appear in bold; other actions are grayed out. The available actions depend on the current state of the VM and your permissions.

Procedure

You can perform these actions using any of the following methods:

- Select the target VM in the **List** tab of the **VMs** page, and choose the required action from the **Actions** dropdown menu. For more information, see VMs Summary View on page 104.
- Right-click on the target VM in the **List** tab of the **VMs** page, and select the required action from the **Actions** dropdown menu.
- Go to the details page of the target individual VM, and perform the required action. For more information, see VM Details View on page 117.

Assigning a VM to a Project Member

This section describes how to assign a VM to a project member.

About this task

A VM is assigned to a member within the scope of a particular project. You can assign a VM to only one project member.

Procedure

To assign a VM to a project member, perform the following steps:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3010

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Compute** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.
   The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment. For information about how to access the list of non-nutanix VMs managed by an external *vCenter*, see VMs Summary View on page 104.
3. Select the **Manage Ownership** action using any of the following methods:
   - Select the target VM checkbox in the **List** tab, and choose the **Manage Ownership** from the from the **Actions** dropdown menu.
   - Right-click on the target VM in the **List** tab, and select **Manage Ownership** from the displayed dropdown menu.
   - Select the **Manage Ownership** action from the **More** dropdown menu in VM Details View on page 117.

   The system displays the **Manage VM Ownership** window.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3011

4. Enter the following information in the **Manage VM Ownership** window, and click **Save**.

   - **Project**: Select the target project from the dropdown menu.
   - **User**: Enter a user name. A list of matches appears as you enter a string; select the user name from the list when it appears.

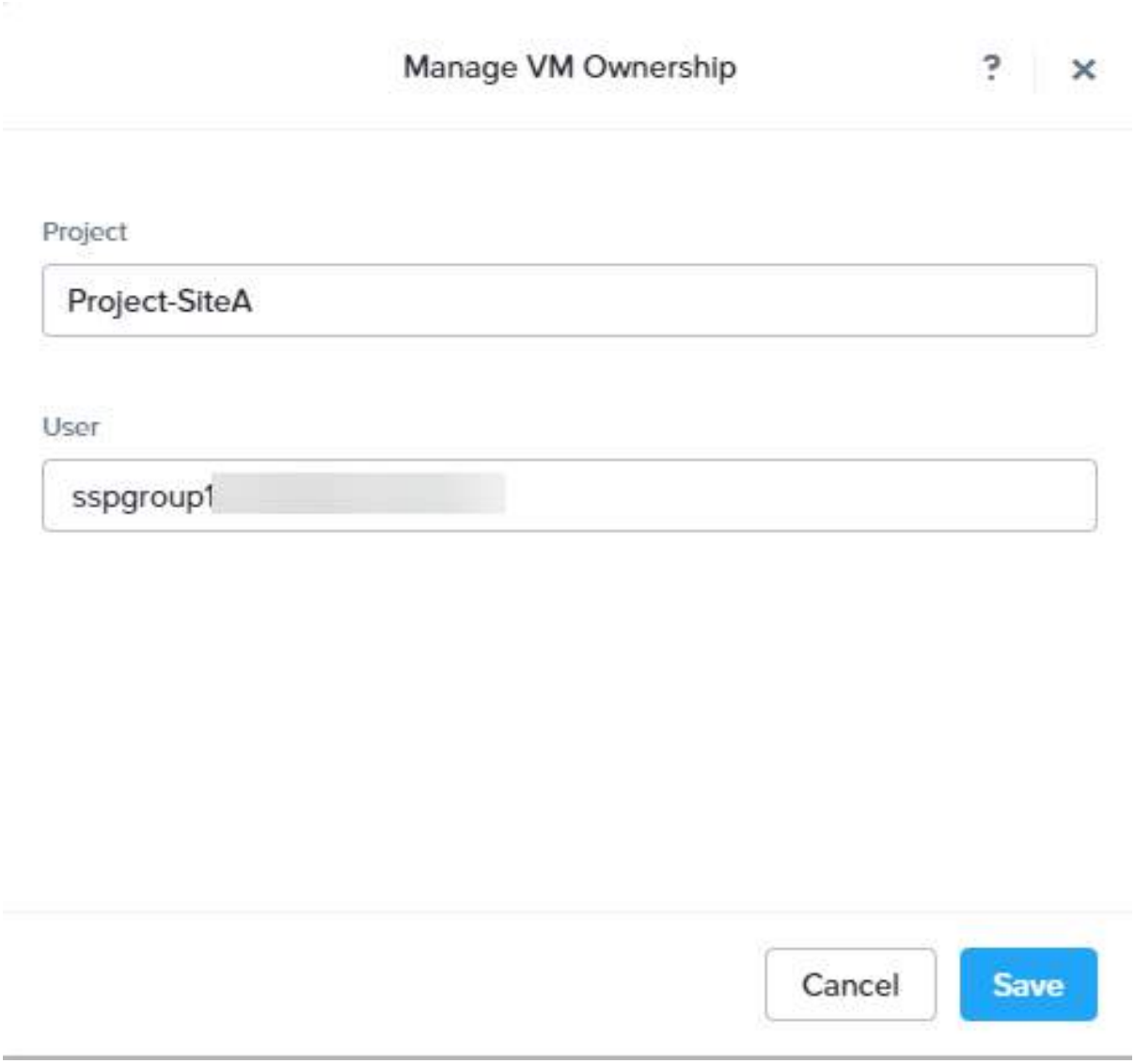


Figure 200: Assign VM to a Project Member

The selected VM is assigned to the project member.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3012

ADDITIONAL OPERATIONS

After installing Prism Central, you can perform the following additional operations:

> **Note:** For information about how to install Prism Central, see Prism Central Deployment on page 12.

- Log in and out through any supported browser. For more information, see Logging Into Prism Central on page 39 and Logging Out of Prism Central on page 584.
- Monitor the status of this Prism Central instance. For more information, see Managing Prism Central on page 542.
- Check version information. For more information, see Finding the Prism Central Version on page 571.
- Modify login page and automatic log off settings. For more information, see Configuring Prism Central UI Settings in *Prism Central Admin Center Guide*.
- Register clusters with this Prism Central instance. For more information, see Registering or Unregistering a Cluster with Prism Central on page 61.
- Expand Prism Central from a single VM to a multi-VM instance. For more information, see Expanding (Scale Out) Prism Central on page 573.
- Shutdown or Start Up a Prism Central VM. For more information, see Shutting Down or Starting Up Prism Central VM on page 578.
- Protect Prism Central with up to three AHV or ESXi clusters registered to it. For more information, see Backing up Prism Central on page 558.
- Recover Prism Central from Prism Element running on the registered AHV or ESXi cluster. For more information, see Restoring Prism Central (1-Click Recovery) on page 562.

Managing Prism Central

Prism Central consists of one or more VMs treated as a single instance that monitors and manages registered clusters. You can view information about the Prism Central VMs by clicking the gear icon in the main menu and then selecting **Prism Central Management** from the **Settings** menu (see Prism Central Settings (Infrastructure) on page 49). This displays the **Manage Prism Central** page.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3013

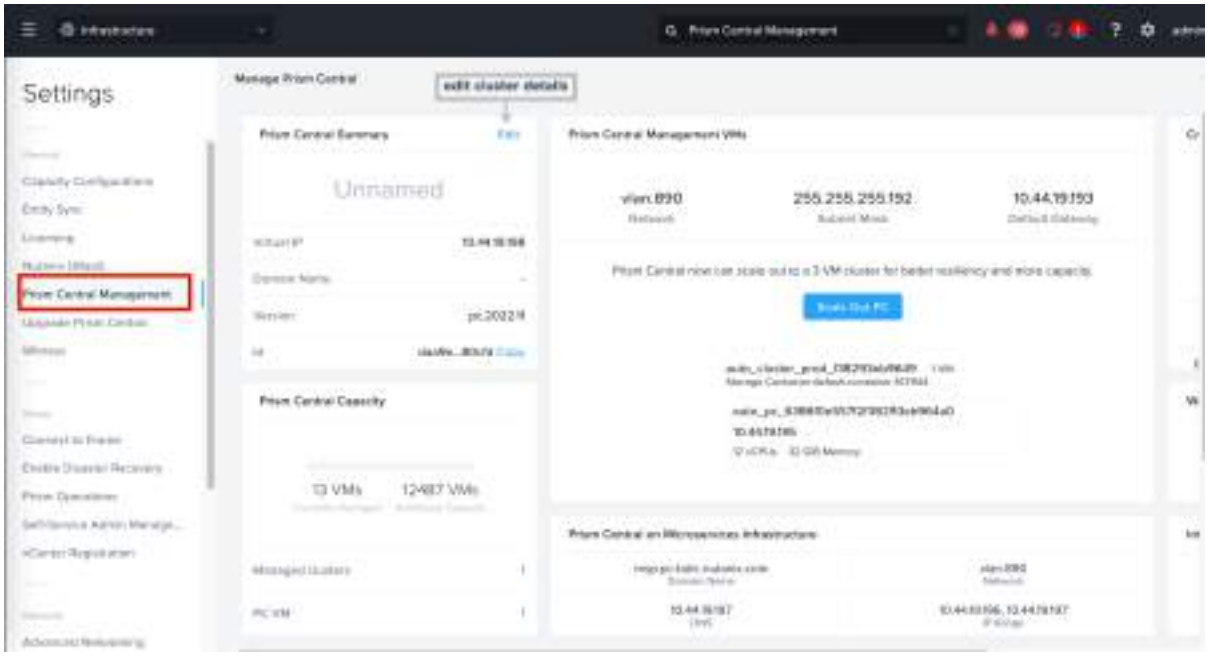


Figure 201: Manage Prism Central Page (1-VM instance)

The **Prism Central Management** page contains the following widgets:

- A **Prism Central Summary** widget on the upper left that displays fields for
  - Cluster name, which is **Unnamed** by default.
  - Domain name. A dash appears if a domain name is not specified.
  - Version. This is the Prism Central version number.
  - ID number. Click the copy link to copy the ID number so you can paste it elsewhere.
- A **Prism Central Capacity** widget on the lower left that displays fields for
  - Number of VMs monitored currently by this Prism Central instance.
  - Number of additional VMs (remaining capacity) this Prism Central instance can monitor.
  - Number of clusters registered to this Prism Central instance; click the number to display the clusters page. For more information, see Clusters Summary View on page 398.
  - Number of VMs that comprise this Prism Central instance; click the number to display the VMs page. For more information, see VMs Summary View on page 104.
- A **Prism Central VMs** widget in the middle that displays network address information (network name, subnet mask, and default gateway address) at the top and information below about each VM in the Prism Central instance (VM name and name of storage container in which it is located, IP address, number of vCPUs, and memory size). In addition, single VM instances include a **Scale Out PC** option to scale out this Prism Central instance . For more information, see Expanding (Scale Out) Prism Central on page 573.
- An **Alerts** widget on the right that displays a list of Prism Central-related alerts broken into Critical, Warning, and Info sections. For more information about alerts, see Prism Central Alerts and Events Reference Guide.

When the Prism Central instance consists of three VMs, the display changes slightly. The **Scale Out PC** option disappears, and a new **Add PCVM** option appears (top right). Prism Central instances are limited to a maximum of

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3014

three VMs, but if you lose one of those VMs for any reason, you can add a replacement by clicking **Add PCVM**. The system displays the **Add PC VMs** page (similar to the **Scale Out PC** page) from which you can add the new VM.

> **Note:** Verify that the prerequisites in Expanding (Scale Out) Prism Central on page 573 are satisfied before adding a Prism Central VM.

To add or change the Prism Central domain name or virtual IP, click the **Edit** link in the **Prism Central Summary** widget. The **Cluster Details** window appears. Do the following:

1. In the **Cluster Name** field, enter a name for the cluster (default "Unnamed"). After naming the cluster, the field no longer appears when subsequently opening the window. Naming the cluster is optional.
2. In the **FQDN** field, enter the fully qualified domain name (FQDN) for the Prism Central cluster. This requires an administrator to configure the domain name in the DNS server to resolve to all the external IPs of the Prism Central VMs.
3. In the **Virtual IP** field, enter an IP address that will be used as a virtual IP for the cluster. This is relevant if you have a multi-VM Prism Central.

   > **Note:** FQDN and virtual IP settings in Prism Central are mutually exclusive. Do not enter a virtual IP in this field if you specified a FQDN in the previous field. A virtual IP provides resiliency but not load balancing. A FQDN does both.

4. When the fields are correct, click **Update** to save the changes and close the window.

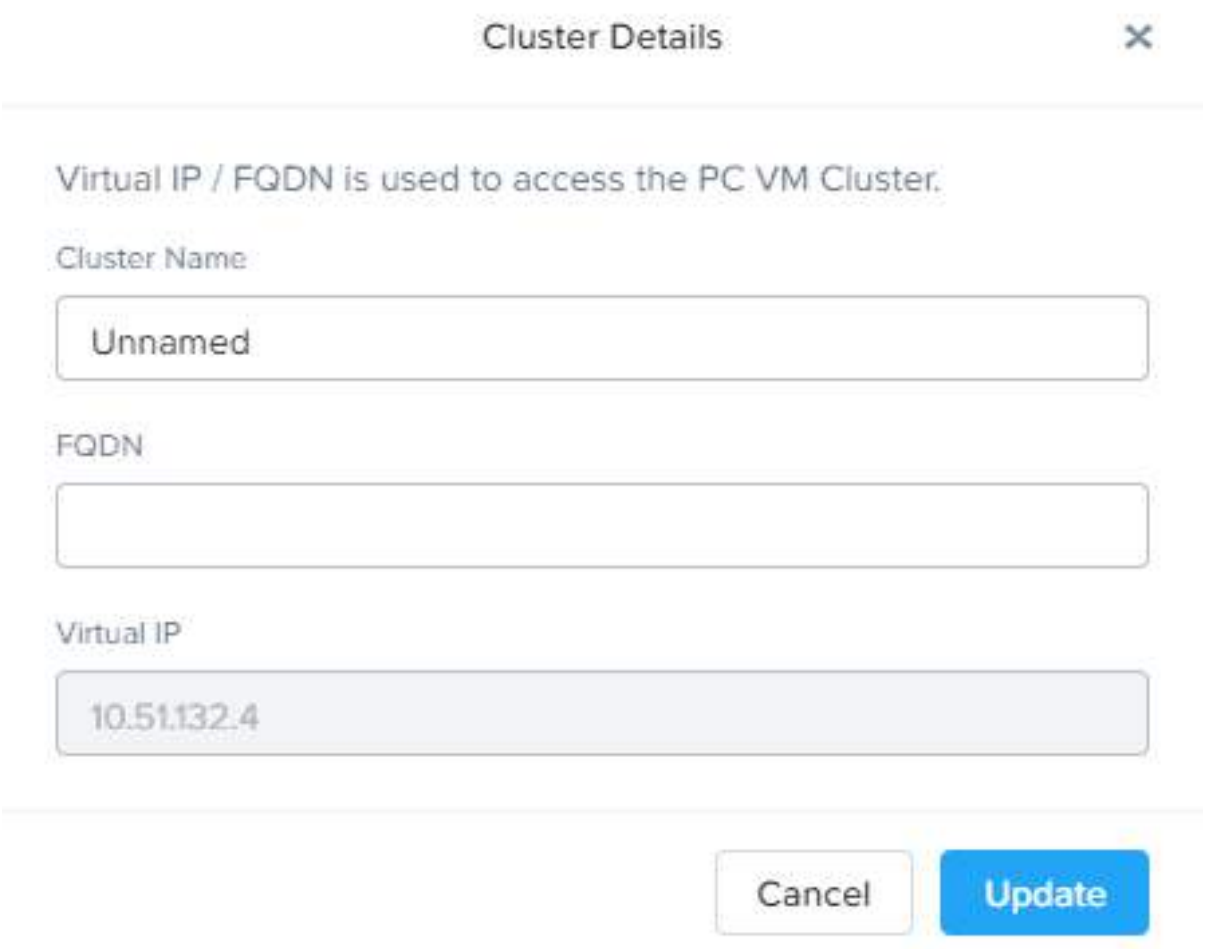


Figure 202: Cluster Details

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3015

Microservices Infrastructure

Microservices Infrastructure (also referred to as MSP) provides a common framework and services to deploy the container-based services associated with Prism Central based components like Flow Virtual Networking and Objects. It deploys services like Identity and Access Management (IAM), Load Balancing (LB), and Virtual Private Networking (VPN). Such services are packaged in containers as microservices. Microservices Infrastructure is a shared Kubernetes cluster that containerizes multiple Prism Central services and the resources associated with the Prism Central services.

Microservices Infrastructure is enabled by default when you:

- install Prism Central version pc.2022.9 or later on a compatible AOS version (6.6 or later)
- upgrade to Prism Central version pc.2022.9 or later on a compatible AOS version (6.1.x or later)

Note:

- You cannot disable Microservices Infrastructure.
- Upgrading Prism Central to a version that enables Microservices Infrastructure by default takes up to 40 minutes longer than a normal Prism Central upgrade.
- If you have enabled Objects in the Prism Central managing the cluster, ensure that the Objects VMs are healthy and running when Prism Central upgrade process enables Microservices Infrastructure. If the Objects VMs are not healthy and running, the task for enabling Microservices Infrastructure might fail. To start the Objects VMs, see Starting the Objects VMs in the *Objects User Guide*.

For information about upgrading Prism Central to a version that enables Microservices Infrastructure by default, see Prism Central Deployment on page 12.

Microservices Infrastructure Prerequisites and Considerations

The Prism Central and cluster deployment must fulfil some prerequisites for Microservices Infrastructure to be enabled by default. These prerequisites apply to manually enabling Microservices Infrastructure as well.

Make sure you meet the prerequisites listed before you enable the Microservices Infrastructure.

Note: Microservices Infrastructure uses several ports and protocols for its operations. For information about the ports that are used by Microservices Infrastructure and need to be open in the firewalls accordingly, see Ports and Protocols for Microservices Infrastructure and Ports and Protocols for Prism Central. For more information on the ports, protocols, IP addresses, and subnets that Microservices Infrastructure uses and needs to be managed in the firewalls, see the Firewall Access to URLs section in this topic.

Microservices Infrastructure Prerequisites

- **Only if you have Prism Central Disaster Recovery (PC DR) enabled**

  If you have enabled PC DR in Prism Central, then do the following:

  1. Disable PC DR in Prism Central. For more information, see Disabling Prism Central Backup and Restore on page 566.

     Note: When you disable PC DR, you cannot enable it again after the Prism Central upgrade until you upgrade at least one Prism Element in the Prism Central cluster (Availability Zone) to *minimum supporting AOS version*.
  2. Upgrade Prism Central to *minimum supporting Prism Central version* (pc.2022.9 or later version that enables Microservices Infrastructure by default).
  3. Upgrade at least one Prism Element in the Prism Central cluster (Availability Zone) to *minimum supporting AOS version*.
  4. Enable Prism Central Disaster Recovery.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3016

- **Minimum AOS Versions**

  - Nutanix supports fresh installation or deployment of Prism Central clusters with CMSP enabled by default on AOS versions. With a minimum Prism Central version of PC.2023.3, fresh installation or deployment is supported on AOS versions 6.5.3.x and later, and 6.6 and later.
  - To upgrade a PC instance to *minimum supporting Prism Central version*, the hosting PE cluster must run *minimum supporting AOS version* 6.5.x or 6.6. If the hosting PE cluster is not running a *minimum supporting AOS version*, then upgrade the AOS version to a *minimum supporting AOS version*.

    This requirement of *minimum supporting AOS version* is not applicable if the Prism Central instance is registered to the hosting PE cluster.
  - When upgrading a PC instance to *minimum supporting Prism Central version*:

    - If the PC instance is not registered to the hosting PE cluster, then register the PC instance to the hosting PE cluster and then run the upgrade workflow.
    - If the PC instance cannot be registered to the hosting PE cluster, enable Microservices Infrastructure to establish trust between the PC instance and the hosting PE cluster.
  - If the PC instance is not registered to the hosting PE cluster or Microservices Infrastructure is not enabled (with trust setup) on the PC instance, then the PC upgrade fails.

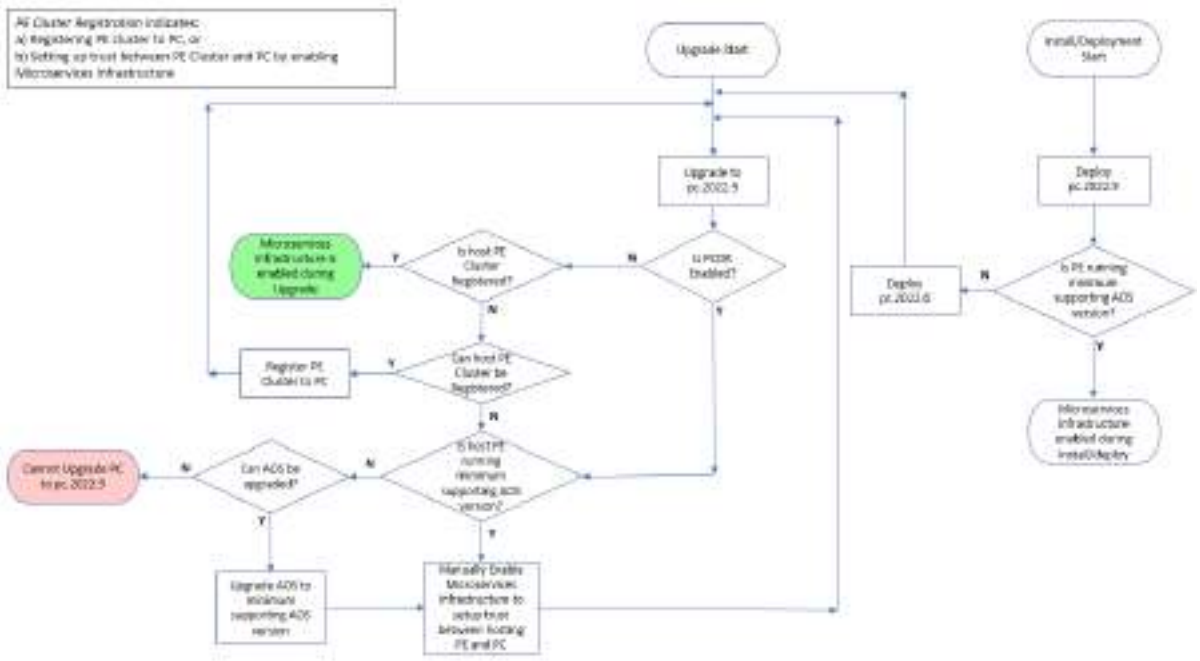


Figure 203: Upgrade/Install Minimum Supporting Prism Central - Process

- **Hypervisor**

  Clusters running AHV or ESXi only support Microservices Infrastructure. For ESXi clusters, enter your vCenter credentials (user name and password) and a network for deployment.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3017

- **Prism Element Cluster and Prism Central IP Addresses**

  Ensure that you have configured virtual IP address and iSCSI data services IP address on the Prism Element that hosts Prism Central. For more information, see Modifying Cluster Details information in the *Prism Element Web Console Guide*).

  Note:

  - You can only change these IP addresses of Prism Central or Prism Element cluster after Microservices Infrastructure is enabled (whether enabled by default or manually enabled). You cannot remove any of these IP addresses. If you remove the current IP address, you must add another IP address before you save the configuration.
  - If a Prism Central instance (on which Microservices Infrastructure is enabled or will be enabled during upgrade) manages multiple Prism Element clusters, configure the iSCSI Data Service IP address on the Prism Element cluster hosting the Prism Central instance. Ensure that the iSCSI Data Service IP address is configured on the hosting Prism Element cluster before you install the or upgrade to the Prism Central that enables Microservices Infrastructure by default.

- **Cold Migration and CLI-based Prism Central Disaster Recovery Support**

  Cold Migration and CLI-based Prism Central Disaster Recovery of Prism Central VMs are not supported.

- **Name and NTP Servers**

  Ensure that you have configured at a minimum, one Name server and one NTP server in both the host Prism Element cluster and Prism Central.

  Warning: Do not remove the Name and NTP server configurations when Microservices Infrastructure is enabled.

- **Prism Central Memory**

  KB 8932 lists the Prism Central VM memory requirements. If your Prism Central VM resources do not meet the recommended amount, manually increase the memory.

- **Prism Central Registration and Trust Configuration**

  Ensure that you have registered the Prism Central instance to the Prism Element cluster. For more information, see Registering or Unregistering a Cluster with Prism Central on page 61.

  Note: If you unregister the Prism Element cluster from the Prism Central instance after you enable Microservices Infrastructure, then trust is automatically configured between the Prism Element cluster and the Prism Central

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3018

instance. There is no impact to Prism Central. This behavior is supported with a minimum Prism Central version of pc.2022.1 with Prism Element cluster running minimum AOS versions 6.1 or 6.5.

If you do not want to register the Prism Central instance with the Prism Element, then you must complete the trust configuration procedure to enable Microservices Infrastructure.

The workflow to enable Microservices Infrastructure includes steps to set up trust between the unregistered Prism Central and the Prism Element. For more information, see Configuring Trust Between Prism Central and Host Cluster.

Trust setup is supported on Prism Element cluster running minimum AOS versions 6.1 or 6.5 and Prism Central running minimum version pc.2022.1.

Note: Ensure that Prism Element cluster is running a minimum version of AOS 6.5 or AOS 6.6 before upgrading the AOS or Prism Central, for which trust is already set up.

If the Prism Element cluster is running a version of AOS older than *minimum supporting AOS version* and the Prism Central is not registered to the host Prism Element, then, before initiating the Prism Central upgrade, register Prism Central with the Prism Element cluster to enable Microservices Infrastructure by default.

If you upgrade the Prism Central version even though it is not registered to the Prism Element cluster, you need to enable Microservices Infrastructure manually after the upgrade is complete.

- **Default Private VXLAN**

  If the Prism Central that you want to upgrade is registered to the Prism Element cluster, then the upgrade process enables Microservices Infrastructure by default using private VXLAN network. If the private VXLAN is used, the ports 9440, 3205, and 3260 are required to be opened from Prism Central to all the Controller VM IP addresses and Controller VM virtual IP addresses in the clusters managed by the Prism Central, and the iSCSI Data Services IP (DSIP) addresses configured for the clusters managed by the Prism Central.

- **Firewall Access to URLs**

  Microservices infrastructure requires access to the following URLs:

  - *.docker.io
  - *.production.cloudflare.docker.com
  - *.nutanix.github.io
  - download.nutanix.com

  Allowlist these URLs in the firewalls to ensure that Prism Central and Prism Element clusters have access to these URLs.

  Microservices Infrastructure requires the following IP address ranges or subnets open (in the firewall) to access the Prism Element Controller VM IP addresses, Controller VM virtual IP addresses, and the Prism Central VIP addresses of port 0, for ICMP traffic. Microservices Infrastructure also requires these IP address ranges or subnets to access the Prism Element Controller VM IP addresses and Controller VM virtual IP addresses, the Prism Element iSCSI Data Services IP (DSIP), and the Prism Central virtual IP addresses on ports 9440, 3205, and 3260. Therefore, ports 0, 3205, 3260 and 9440 must be open in the firewall for these IP address ranges or subnets to reach the all the Prism Element Controller VM IP addresses and Controller VM virtual IP addresses, Prism Element iSCSI Data Services IP (DSIP) address, and the Prism Central virtual IP addresses as required.

  The firewall must also allow any specific IP address range or subnets that are or might be configured as the private networks for Microservices infrastructure.

  Note: Do not use the IP addresses in the subnet 10.200.32.0/24 for operational purposes such as DNS or CVM networks. This prevents any negative impact and maintain seamless operations in the networking.

  For more information, see Ports and Protocols to see the access requirements for all the Nutanix software.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3019

Table 159: Subnets for Microservices Infrastructure

Subnet	Purpose
10.100.0.0/16	Reserved for Kubernetes pod network
10.200.32.0/24	Reserved for Kubernetes services network

- **Prism Central Service Domain Name**.

  Microservices Infrastructure uses a shared Kubernetes cluster that containerizes multiple Prism Central services and the services resources associated with the services. During the Microservices Infrastructure deployment process, a Domain Name Service (DNS) is deployed within Prism Central. Microservices Infrastructure uses this DNS to discover and manage the available Prism Central microservices. The Prism Central Domain is set up for discovery of the microservices and communication of the microservices with each other. The Prism Central Domain facilitates the discovery and communication using the DNS service deployed for the Microservices Infrastructure within Prism Central.

  Ensure that the following caveats are considered when selecting a valid Prism Central Domain Name:

  - The selected FQDN must contain at least three labels in the `<subdomain>.<second-level domain>.<top-level domain>` format.

    For example, if `test` is the subdomain, `nutanix` is second-level domain and `com` is the top-level domain then `test.nutanix.com` is the valid Prism Central service domain formed with these three labels.
  - The selected FQDN labels must be at least two characters long.
  - The selected FQDN must be unique. It must not exactly match any other FQDN currently in use in the, since such duplication complicates the configuration of forwarding or redirection of queries.
  - The selected FQDN must comply with the following label restrictions:
    - The top-level domain must not exceed 6 characters.
    - The top-level domain must not end with `test`.
    - The subdomain must not exceed 16 characters.
  - The selected FQDN must be added to the allowlist with a * preceding the domain name (*.defined_domian_name), if Prism Central has a proxy configuration.

    For example, if you use the domain name test.nutanix.com, then allowlist *.test.nutanix.com.

  The following are examples of valid domain configurations:

  - my.cluster.domain
  - my.test.cluster.test.domain
  - test.nutanix.com

  The following are examples of domains not supported:

  - my.cluster.test (top-level domain, being test, is not allowed)
  - my.test.clusters.test.domain (number of characters of subdomain (my.test.clusters), being 17, is exceeding 16)
  - prism-central-cmsp.test.domain (number of characters of subdomain, being 18, is exceeding 16)
  - microservices-domain.prismcentral.services (number of characters in subdomain, being 21, is exceeding 16, and in top-level domain being 8, is exceeding 6)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3020

- **Flow Microsegmentation container**

  When Flow Microsegmentation is enabled, a Kafka container called flow_data is automatically created on the cluster that hosts Prism Central. The flow_data container stores data that is required and essential for Flow visualization. Do not delete this container.

Limitations

The following limitations apply after Microservices Infrastructure is enabled (whether by default or manually):

- **Hypervisor Support**

  Nutanix does supports Microservices Infrastructure only on an on-premises Prism Central (PC) deployment hosted on an AOS cluster running AHV or ESXi. Clusters running other hypervisors are not supported.

- **Nutanix Move**

  Moving a Prism Central enabled with Microservices Infrastructure from ESXi host to AHV host using Nutanix Move is not supported.

- **Scale-out and Single PCVM deployments**

  Scale-out three-node Prism Central VMs deployment: Small, large, or x-large Prism Central VMs are supported. Reverting the deployment to a single Prism Central VM deployment is not supported.

  Single Prism Central VM deployment: Small, large, or x-large Prism Central VM are supported. You can expand a single PCVM deployment to a scale-out three-node PC deployment on a minimum Prism Central version of pc.2022.1 and minimum AOS version of 6.1. Expanding a single node Prism Central with Microservices Infrastructure is supported only on a minimum Prism Central version of pc.2022.1 and minimum AOS version of 6.1.

  For information on Prism Central scalability and the type of Prism Central deployments, see the *Prism Central Scalability* topic in the release notes for the Prism Central version to be installed.

- **IP Address Restrictions**

  Ensure that the IP addresses in subnet that you configure for Microservices Infrastructure do not conflict with the IP addresses in the management subnet.

  > **Note:** Do not use the IP addresses in the subnet 10.200.32.0/24 for operational purposes such as DNS or CVM network.

Trust Configuration and Manually Enable Microservices Infrastructure

The following two workflows are closely associated with each other:

- Trust setup between the Prism Central that Microservices Infrastructure is enabled in, and the Prism Element cluster that hosts the Prism Central.
- Manually enabling Microservices Infrastructure in Prism Central.

The trust configuration workflow occurs as the starting point in the workflow to manually enable microservices infrastructure (see Enabling Microservices Infrastructure Manually on page 552).

The steps to manually enable Microservices Infrastructure follows the trust configuration steps.

The starting point for the workflows is the **Enable Now** in the **Prism Central on Microservices Infrastructure** widget on the **Prism Central Management** page in **Prism Central Settings**page.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3021

Configuring Trust Between Prism Central and Host Cluster

If Prism Central is not registered to the host cluster Prism Element, it must have a trust relationship setup with the Prism Element cluster.

Before you begin

Ensure that you have satisfied these requirements.

- The Prism Central instance is deployed with a minimum Prism Central version of pc.2022.1. The Prism Element cluster is deployed with a minimum AOS version of 6.1 (STS) or 6.5 (LTS). If required, upgrade the AOS version of the Prism Element cluster AOS version of the host cluster before you manually enable microservices infrastructure.
- Add the domain used (like *.prism-central.cluster.local) by the Prism Central to the allow-list.
- Ensure that requirements provided in Microservices Infrastructure Prerequisites and Considerations on page 545 are met.

About this task

If the Prism Central instance is not registered to the Prism Element cluster that hosts it, then after you click **Continue** on the **Important Information** window, Prism Central displays the **Enable Microservices Infrastructure** window with the trust configuration parameters.

Procedure

1. Go to the **Prism Central Management** page (see Managing Prism Central on page 542).
2. In the **Prism Central on Microservices Infrastructure** widget, click **Enable Now**.

Figure 204: Prism Central on Microservices Infrastructure widget

3. Read the information and then click **Continue**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3022

4. On the **Enable Microservices Infrastructure** window, provide the following information:

   - Virtual IP Address or FQDN of the host Prism Element.
   - Admin user name used to log on to the host Prism Element.
   - Password for the admin user name provided to log on to the host Prism Element.

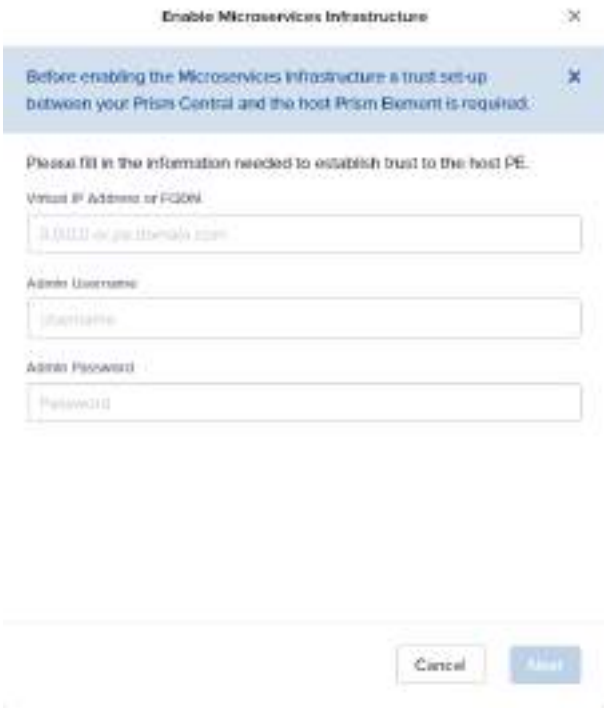


Figure 205: Enable Microservices Infrastructure - Trust setup

5. Click **Next**.
   The **Enable Microservices Infrastructure** main dialog box provides the parameters to enable microservices infrastructure.

6. Complete manually enabling microservices infrastructure. See Enabling Microservices Infrastructure Manually on page 552.

Enabling Microservices Infrastructure Manually

The microservices infrastructure enabled by default. This topic provides the procedure to enable microservices infrastructure manually.

Before you begin

Ensure that all the requirements provided in Microservices Infrastructure Prerequisites and Considerations on page 545 are fulfilled before enabling the microservices infrastructure.

If the Prism Central instance is not registered to the Prism Element cluster hosting the Prism Central, then set up trust between the Prism Central and the Prism Element cluster hosting the Prism Central by completing the steps provided in Configuring Trust Between Prism Central and Host Cluster on page 551.

About this task

To enable the microservices infrastructure, do the following:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3023

Procedure

1. Read the information, and then click **Continue**.

   > **Important:** If the Prism Central deployment is not registered with the Prism Element, then the **Enable Microservices Infrastructure** window provides the parameters for establishing trust between Prism Central and Prism Element that hosts the Prism Central instance.
   >
   > Complete the steps mentioned in Configuring Trust Between Prism Central and Host Cluster on page 551. Then, the main **Enable Microservices Infrastructure** dialog box is displayed.

   The main **Enable Microservices Infrastructure** dialog box is also displayed if the Prism Central instance is already registered with the host Prism Element.

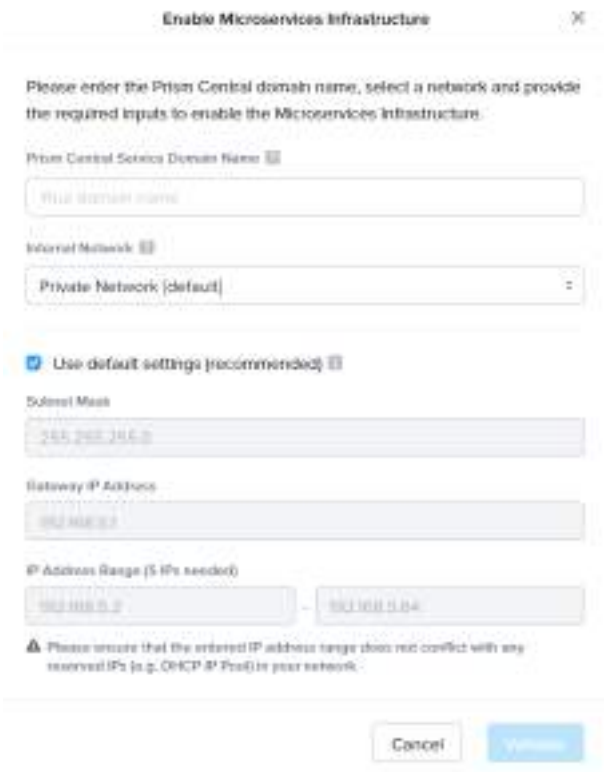


Figure 206: Enable Microservices Infrastructure

2. Provide the following information in the main **Enable Microservices Infrastructure** box.

   - **Prism Central Service Domain Name**: Enter a domain name for the service. See **Prism Central Service Domain Name** restrictions in Microservices Infrastructure Prerequisites and Considerations on page 545.
   - **Internal Network**: Select the network to use for Prism Central micro services communication from the dropdown list.

     The default selection **Private Network [default]** is a pre-configured private VxLAN network. Instead, if you want microservices infrastructure to use a different network, you can select the network (managed or

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3024

unmanaged) from the drop-down list. If the network you want microservices infrastructure to use does not appear in the list, you must first configure it. For more information, see Network Configuration on page 346.

- The **Use default settings (recommended)** checkbox is available only when you have retained the default selection (**Private Network [default]**) for **Internal Network** in the preceding step. This checkbox is checked by default. Do one of the following:

  - Retain the check mark for the **Use default settings (recommended)** checkbox and click **Validate**. (Go to step 3 on page 554.)

    Retaining the check mark for the **Use default settings (recommended)** checkbox allows Prism Central to use the **Private Network [default]** with the default values for **Subnet Mask**, **Gateway IP Address** and **IP Address Range**.

  - Clear the **Use default settings (recommended)** checkbox, if you want Prism Central to use the **Private Network [default]** setting with specific (non-default or custom) values for **Subnet Mask**, **Gateway IP Address** and **IP Address Range**.

Configure the **Internal Network** for microservices infrastructure if you did one of the following:

- Selected a managed or unmanaged network other than **Private Network [default]** for **Internal Network**.

  If you selected a managed network, the values in the **Subnet Mask**, **Gateway IP Address** and **IP Address Range** fields are already configured. If you selected an unmanaged network, you must enter the necessary values in the respective fields.

- Cleared the **Use default settings (recommended)** checkbox with the **Private Network [default]** selection for **Internal Network**.

Enter the values for the following parameters to configure **Internal Network**:

Parameter	Description
Subnet Mask	Enter the subnet mask.
Gateway IP Address	Enter the IP address for the gateway.
IP Address Range	Enter a range of IP addresses that the network can use. Enter a range of at least 10 available (unreserved) addresses for a 3-VM (scale out) Prism Central instance or at least 5 addresses for a 1-VM Prism Central instance. The addresses must be consecutive or sequential. For a managed network, the range of addresses for microservices infrastructure must be outside the range of reserved IP addresses (for example, DHCP IP Pool) in the selected network.

3. After you check that the values entered for all the fields are correct, click **Validate**.
   The system checks the settings. When the settings are confirmed, a Validation was successful message appears and the **Validate** changes to **Enable**.

4. Click **Enable**.
   The process begins, which takes about 45 minutes. You can monitor progress from the tasks dashboard (see Tasks View on page 452). When the microservices infrastructure is enabled, the contents of the enable box in the **Manage Prism Central** page changes to display configuration information such as the domain name, the used IP addresses, and the service domain's DNS IP address.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3025

What to do next

After the tasks are completed, including the **IAM Migration & Bootstrap** task, log out of Prism Central. Wait at least 15 minutes before logging on to Prism Central.

Enabling Microservices Infrastructure (dark site)

Manually enabling the Microservices Infrastructure when there is no Internet access (dark site) requires some extra steps from the standard procedure.

About this task

To enable the Microservices Infrastructure at a dark site, do the following:

Procedure

1. From a device that has public Internet access, log on to the Nutanix support portal, select **Downloads** > **LCM** from the entity menu (hamburger icon), and then download the LCM Dark Site Bundle tar file.
2. Set up a local web server, upload LCM Dark Site Bundle to the server, and extract the files in a directory in the base of the web server.

   For more information, see the Local Web Server Setup section in the *Life Cycle Manager Guide*. Set the following file types in the LCM web server when you are using Windows Web Server: .json, .xz, .qcow2, .sign, .gz

   For the mime types associated with the above file types, see the Local Web Server Setup section in the *Life Cycle Manager Guide*.
3. In the Nutanix support portal **Downloads** page, select **Microservices Platform (MSP)**, download the **Upgrade (Darksite)** bundle to the web server base directory you used in step 2, and extract the files.

   > **Note:** With a minimum Prism Central version of pc.2023.4, to upgrade Microservices Infrastructure in a darksite, download and use the **Prism Central LCM Bundle**. Do not download Microservices Infrastructure **Upgrade (Darksite)** bundle for dark site upgrades.
4. Now follow the standard procedure for enabling the Microservices Infrastructure through Prism Central (see Enabling Microservices Infrastructure Manually on page 552).

Microservices Infrastructure Cluster Upgrade

When you enable Microservices Infrastructure, it creates a Kubernetes cluster with a version that is deployed by the Microservices Infrastructure controller. When you upgrade Prism Central version, it upgrades the Microservices Infrastructure controller version. The cluster is not upgraded. The controller upgrade process upgrades the base services running on the cluster instead of upgrading the cluster.

Starting with Prism Central pc.2024.3, the Prism Central upgrade process upgrades the Microservices Infrastructure controller version, the Microservices Infrastructure Kubernetes cluster version and the base services running on the cluster.

> **Note:** The Prism Central upgrade fails if the Microservices Infrastructure cluster version upgrade fails. In other words, the Microservices Infrastructure cluster version upgrade failure leads to Prism Central upgrade failure. The Prism Central upgrade task failure details reflect the failure of the Microservices Infrastructure cluster upgrade failure. The error message is prefixed with `CMSP cluster upgrade failed:`.

Displaying the Cluster Version

About this task

Perform the following steps to ascertain the Microservices Infrastructure cluster version.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3026

Procedure

1. SSH to the Prism Central VM.
2. Run the following command:

```
nutanix@pcvm$ mspctl cls version
```

The following is a sample output of this command:

```
COMPONENT       VERSION
Cluster         1.x.x
```

Prism Central Backup, Restore, and Migration

Prism Central Backup and Restore (PCBR) is a robust solution for protecting your Prism Central instances (including scale-out configurations) against unforeseen events such as natural disasters, network outages, or power failures. You can also use PCBR to migrate Prism Central instances from one cluster to another. The feature enables the following automated backup solutions to ensure the resilience of your instances and service configurations across both on-prem environments and public cloud platforms such as AWS.

Continuous Backup

Enables almost real-time backup of your Prism Central instances (and various service configurations within it) to up to three AHV or ESXi clusters registered to the same on-prem Prism Central instance, ensuring minimal data loss and swift recovery after disruptions.

Point in Time Backup

Enables scheduled backups of your Prism Central instances (and various service configurations within it) to one S3 object-based storage (bucket) on AWS, allowing for recovery to specific points in time and protection against ransomware attacks and datacenter failures.

You can configure continuous or point-in-time backup for your instance (and various service configurations within it) in the following combinations to up to four locations. You can also configure continuous and point-in-time backup together for your instance.

Backup Type	Number of Backup Targets Supported
On-prem	Upto three AHV or ESXi clusters
Cloud	One S3 object-based storage. An S3 bucket can be used to back up multiple Prism Central deployments.
Hybrid (On-prem + Cloud)	A combination of up to three AHV or ESXi clusters and one S3 object-based storage.

The 1-Click recovery restores the important service configurations along with the entire Prism Central instance, minimizing downtime and operational impact. To know the supported and unsupported services, see *Supported Services for Backup and Recovery* and *Unsupported Services for Backup and Recovery* in Implementation Considerations and Limitations on page 556.

This document describes the GUI-based PCBR solution.

Implementation Considerations and Limitations

Unsupported Backup Methods

Protecting your Prism Central instances using protection domain-based disaster recovery, protection policy-based workflows, third-party backup software, or any unsupported methods renders those instances unrecoverable.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3027

Prism Central Migration

The Prism Central Backup and Restore (PCBR) capability can be used to migrate Prism Central instances to other clusters. While the PCBR workflow ensures the successful migration of important service configurations to the remote cluster, the services listed in the *Unsupported Services for PCBR* section of this document are not migrated. For more information on migrating Prism Central instances, see Migrating a Prism Central Instance on page 565.

> **Note:** Migration of Prism Central instances using vMotion is not supported.

Supported Services for PCBR

The following services can be backed up, and data associated with them can be recovered.

- Nutanix Disaster Recovery (formerly known as Leap)
- Flow Network Security (formerly known as Flow Microsegmentation)
- Networking (such as AHV-based VLAN and Virtual Switch configurations)
- Flow Virtual Networking (Virtual Private Clouds (VPCs) and virtual networks using Networking Controller (ANC) and Networking Gateway)
- Intelligent Operations
- VM management
- Cluster management
- Categories
- Licensing
- LCM
- Reporting templates
- Files

Unsupported Services for PCBR

Although the following services continue to run, their data is not backed up and, therefore, is not recoverable.

- NCM Self-Service (formerly known as Calm)

  > **Important:** To do a planned restore of an NCM Self-Service-enabled Prism Central instance to a recovery cluster, perform the following steps.
  >
  > 1. Manually backup the NCM Self-Service-related entities in Prism Central at the primary cluster. For more information, see Backing up Calm Data in *Calm Administration and Operations Guide*.
  > 2. Restore Prism Central in the recovery cluster.
  >
  >   > **Caution:** Before you restore the Prism Central instance in a recovery cluster, ensure the Prism Central backup is synched at least once with the recovery cluster you select to restore the Prism Central instance.
  >
  > 3. Restore the NCM Self-Service-related in the new Prism Central instance at the recovery cluster. For more information, see Restoring Calm Data in *Calm Administration and Operations Guide*.

- Nutanix Kubernetes Engine (formerly known as Karbon)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3028

- Objects
- Catalog
- Power service monitoring
- Images
- VM templates

For Nutanix Disaster Recovery jobs (RPJs) in progress, see this Note. Metrics older than 90 days also cannot recovered.

Backup Suspension During Upgrades

For enabled Prism Central Backup and Restore (PCBR), the system pauses the backup of Prism Central configuration data when a Prism Central upgrade is initiated. The backup resumes after the upgrade process is completed.

Backing up Prism Central

You can protect or back up a Prism Central instance to its registered Nutanix clusters, AWS S3 object-based storage, or Nutanix clusters and AWS S3 object-based storage together that fulfill the requirements. Backup to registered Nutanix clusters is called continuous backup as it happens continuously at a RPO of 30 minutes. Backup to s3 endpoints is called point-in-time backup as it is taken at specified intervals ranging from 1 hour to 24 hours. The system enables you to back up a Prism Central instance to at most three AHV or ESXi clusters and one S3 object-based storage. Clusters running Hyper-V are not supported. .

Before you begin

Ensure that the following requirements are met before protecting or backing up the Prism Central instance.

- To back up a Prism Central instance to AWS S3 object-based storage, which is called point-in-time backup in the Prism Central web console, the Prism Central instance must run on a minimum version of pc. 2024.1 or later.

  Note: All current versions of Prism Central support backing up to Nutanix clusters, which is called continuous backup in the Prism Central web console.

- The Prism Central instance must have an NTP configuration to synchronize time between the Prism Central instance and the registered clusters. For more information on NTP configuration, see Configuring NTP Servers (Prism Central) in the *Prism Central Admin Center Guide*.
- The Nutanix clusters used to back up the Prism Central instance must be running a minimum version of AOS 6.0 or later.
- For continuous backup, at least one cluster used to back up the Prism Central instance must be running AOS 6.5.3.1 or later because the Prism Central instance can be restored only on clusters running AOS 6.5.3.1 or later. For more information, see Restoring Prism Central (1-Click Recovery) on page 562.
- For point-in-time backup, at least one cluster used to back up the Prism Central instance must be running AOS 6.8 or later because the Prism Central instance can be restored only on clusters running AOS 6.8 or later. For more information on the supported AOS versions, see Compatibility and Interoperability Matrix.
- To configure an AWS bucket for point-in-time backup, perform the operations noted in Configuring Amazon S3 Object Lifecycle and Policies on page 560.
- The Nutanix clusters used to back up the Prism Central instance must be registered to Prism Central instance you want to back up.
- You must note the Files version. In the case of a disaster, you might need it later to restore Files to the pre-disaster version.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3029

About this task

To protect or back up a Prism Central instance, perform the following steps.

Procedure

1. Log in to the Prism Central web console.
2. Click the Settings icon and navigate to **General** > **Prism Central Management** from the **Settings** menu. For more information, see Prism Central Settings (Infrastructure).
   The **Prism Central Management** page appears. This page provides information about this Prism Central instance.

   > **Tip:** The **Whats's New** page appears when you go to the **Prism Central Management** page for the first time.

3. Select one of the following in the **Prism Central Backup and Restore** widget.

   » **Continuous Backup**. To enable real-time backup of your Prism Central instances (and various service configurations within it) to the clusters registered to the same on-prem Prism Central instance, ensuring minimal data loss and swift recovery after disruptions.

   > **Note:** The RPO and RTO for recovery from a continuous backup are 5 minutes and 90 minutes, respectively. You can recover the Prism Central instance only from the latest backup.

   » **Point-in-Time Backup**. To enable scheduled backups of your Prism Central instances (and various service configurations within it) to S3 object-based storage on AWS, allowing for recovery to specific points in time.

   > **Note:** The RPO and RTO for recovery from a point-in-time backup are 2 hours and 90 minutes, respectively. You can recover the Prism Central instance from any available restore points.

4. Click **Protect Now**.

   > **Note:** The **Protect Now** option is available only when one or more clusters are registered to the Prism Central instance, or you want to configure S3 buckets on AWS.

   The **Protect Prism Central** window appears. This window shows the services data that will be backed up and those that will not be backed up.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3030

5. Click **Continue**, and do one of the following according to the backup type you selected in Step 3.

   - For continuous backup, select one or more clusters to back up the Prism Central instance.

     Note: You can select a maximum of 3 clusters.

   - For point-in-time backup, specify the following details in the **Protect Prism Central** window.

     Note: Perform the operations noted in Configuring Amazon S3 Object Lifecycle and Policies on page 560 before you proceed to specify the following details.

     - **AWS Region Name**. Enter an AWS region name. For more information, see *AWS documentation*.
     - **AWS Bucket Name**. Enter a bucket name. For more information, see *AWS documentation*.
     - (Optional for NC2 environments) **Access Key**. Enter your access key.
     - (Optional for NC2 environments) **Secret Access Key**. Enter your secret access key.

     Note: The first restore point is created immediately, and then restore points are created every two hours (RPO). Up to 30 days of restore points are supported for restoring the Prism Central instance.

6. Click **Proceed**.
   The system synchronizes Prism Central configuration data to the selected clusters or S3 object-based storage. While the configuration data is synchronizing, the **Status** is shown Sync in Progress. The **Status** turns to Synced when the configuration data is synchronized. For continuous backup, the first backup creation on the selected clusters takes at least 30 minutes. After the first backup, the system synchronizes Prism Central configuration data with the selected clusters every 30 minutes. For point-in-time backup, the process of taking the first backup starts immediately when you submit the S3 bucket details and takes at least 15 minutes. After the first backup, the system synchronizes Prism Central configuration data with the S3 bucket every 2 hours.

7. (Optional) If you want to back up the Prism Central instance to more Nutanix clusters or S3 buckets, click **+ Add Backup** in the **Prism Central Backup and Restore** widget.
   However, the number of entities backing up the Prism Central instance must be at most four— to three on-prem clusters and one S3 object-based storage. You can use a cluster only once to back up the same Prism Central instance.

8. (Optional) If you want to remove a Nutanix cluster or a bucket from backing up the Prism Central instance, click **Remove** in front of the cluster, type Remove (not case sensitive), and click **Remove**.

Configuring Amazon S3 Object Lifecycle and Policies

About this task

When you have created an Amazon S3 bucket in a suitable region to store the backup data, you must perform the following configurations for it.

Procedure

1. Enable versioning.
   A version of the file is created each time the system writes the seed data file on the new key path to the bucket. The previous version becomes noncurrent, and the currently written file becomes current. For more information on the current and noncurrent items and how to enable bucket versioning, see *Amazon S3 documentation*)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3031

2. Enable object lock for objects to enable WORM (write-once-read-multiple) configuration and to create point-in-time snapshots of Prism Central configuration.

   Configure object lock when you create a bucket. To ensure that the backup data put into the bucket is retained for some time and deleted at that time, the system retains the data for 31 days. Configure the retention mode as Governance. For more information on how to enable object lock, see *Amazon S3 documentation*.

3. Configure an object lifecycle rule to auto-delete older backup data.

   To enable the automatic deletion of objects after a certain time as they become stale, configure an object lifecycle rule from the Amazon S3 console that applies to all objects in the bucket. For more information on how to configure a lifecycle rule, see *Amazon S3 documentation*.

   > **Note:** Configure a maximum time of 31 days for deleting noncurrent objects. Nutanix recommends setting the deletion of expired object delete markers, the expiration of the current version of objects, and the deletion of incomplete multipart uploads to a day.

   The rule you created is listed as the following.

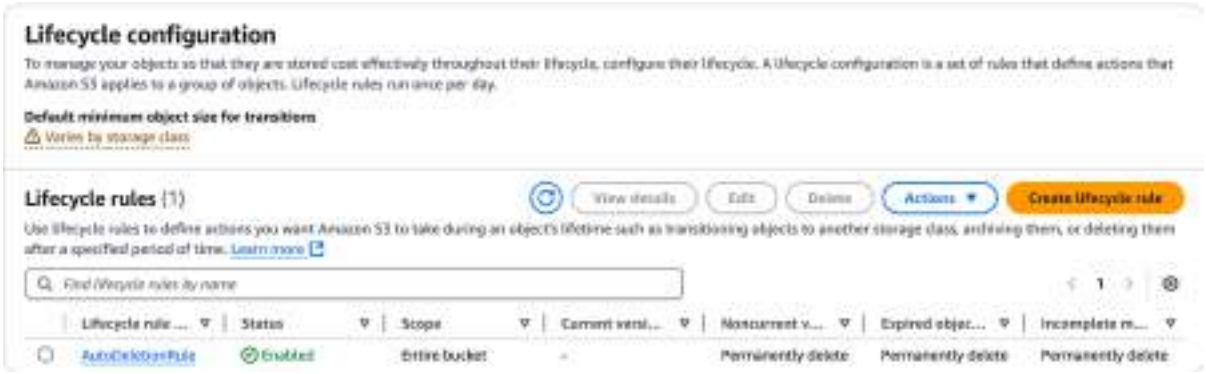


Figure 207: Lifecycle Configuration

4. By default, public access is blocked for buckets in the AWS console. To enable access, log on as the root user of the AWS account and navigate to the IAM service.

   For more information, see *AWS S3 documentation*.

5. Create a user from the Amazon S3 console. Do not provide console access to this user since an access key is to be generated for this user to enable programmatic access from outside of AWS.

   a. When the user is created, create a policy with an identifiable name and paste the following JSON in the text box.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetObjectVersion",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion"
            ],
            "Resource": "arn:aws:s3:::Bucket_name/*"
        },
        {
            "Effect": "Allow",
            "Action": [
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3032

```
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:GetLifecycleConfiguration"
            ],
            "Resource": "arn:aws:s3:::Bucket_name"
        }
    ]
}
```

Replace *Bucket_name* with the name of your Amazon S3 bucket.

b. Find the policy created in the previous step and attach it with the user you created in Step 6.

c. Create an access key with a descriptive name and select **Application running outside AWS** from the AWS console.

d. Save the access key. Nutanix recommends downloading the CSV file. The same key needs to be input on the Prism Central web console while configuring this S3 bucket as the target endpoint for storing your Prism Central configuration backups.

For more information, see *AWS S3 documentation*.

Restoring Prism Central (1-Click Recovery)

If you protected or backed up your Prism Central instance, you can use an AHV or ESXi cluster to restore the Prism Central instance. For continuous backups (backups stored on on-prem Nutanix clusters), you can recover the Prism Central instance from a registered cluster only. For point-in-time backups (backups stored on Amazon S3), you can recover the instance on a registered cluster, or you can recover it on a cluster that is not registered with any Prism Central instance.

Before you begin

Ensure that the Nutanix cluster you use to restore the Prism Central instance meets the following requirements.

- Registered to the protected Prism Central instance.
- To restore from a continuous backup, the cluster must run AOS 6.5.3.1 or later. For more information on the supported AOS versions, see Compatibility and Interoperability Matrix.
- To restore from a point-in-time backup, the cluster must run AOS 6.8 or later. For more information on the supported AOS versions, see Compatibility and Interoperability Matrix.
- Configured with ISCSI data service IP address for efficient recovery of Nutanix Disaster Recovery or NCM Self-Service configurations.

> **Note:** The Nutanix cluster takes about 10 minutes to stabilize the Prism Central instance after the recovery task on the Prism Element web console is displayed as complete. This is because Microservices Infrastructure causes the system to rotate certificates after the restoration and restart services like IAM and Flow Virtual Networking.

About this task

> **Important:**
>
> After restoring your Prism Central instance, ensure that you manually restore Files to the pre-disaster version. For more information, see Manually Failing Over to a Remote Site in the *Files Manager User Guide*.
>
> Accessing Prism Central (PC) using APIs or any other alternative method is strongly discouraged until the restoration process has been fully completed, as such actions may lead to locking of PC username credentials resulting in subsequent login issues.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3033

To restore a Prism Central instance, perform the following steps.

Procedure

1. Log in to any Prism Element web console registered to the Prism Central instance you want to restore.

   The Prism Element dashboard shows the Prism Central widget, which contains Prism Central information (IP address and connection status). If this is a fresh Prism Element that you created and you have yet to register to a Prism Central instance, it won't appear. Instead, you see the **Register or Deploy Prism Central**.

2. Click the Settings icon and navigate to **Data Resiliency** > **Restore Prism Central** from the **Settings** menu. For more information, see Settings Menu in the `Prism Element Web Console Guide`.
   The **Restore Prism Central** page appears. This page provides you options to restore the Prism Central instance from a Prism Element cluster or S3-compatible object storage.

3. Select from where you want to restore the Prism Central instance and click **Restore Now**.

   > **Note:** If you configured only continuous backup, the **Restore Now** option is available only when Prism Central is in a disconnected state(shown **Disconnected** in the Prism Element web console.

   The **Restore Prism Central** window appears. This window shows the service data that will be recovered and those that will not.

4. Click **Continue** and specify the following information according to the source from where you want to recover.

   » To recover from a continuous backup, see Restore Prism Central-Field Information for Continuous Backup on page 564.

   » To recover from a point-in-time backup, see Restore Prism Central-Field Information for S3-based Object Storage on page 564.

   The Prism Central instance is restored in 60 to 90 minutes, depending on the configuration data of the hosts. The restoration involves the deployment of Prism Central and the restoration of its configuration data from the backup, which can take anywhere between 60 and 120 minutes, depending on the size of the data. The restored Prism Central instance takes an additional 30 to 40 minutes to show all the guest VMs, disks, and metrics. Wait to perform any actions on the restored Prism Central instance until all the recovery tasks are complete on the cluster. You can see the restoration status and the related processes in the **Tasks** window.

What to do next

Consider the following after the Prism Central restoration.

- Use the newly restored Prism Central instance only.

  If the old Prism Central instance becomes available, shut down or delete the old instance because running the old Prism Central instance can cause data corruption.

  > **Note:** If the Prism Central restoration fails, contact Nutanix Support. Do not bring up the old Prism Central instance.

- Reset the credentials.

  Prism Central restores with the default credentials. Nutanix recommends changing the default credentials. For information about changing the default credentials, see Logging Into Prism Central in the *Prism Central Infrastructure Guide*.

  > **Note:** If you have both S3-compatible object storage and Nutanix on-prem clusters configured as backup targets and you recovered the Prism Central instance through an on-prem cluster. In that case, you must reconfigure the s3 bucket credentials after the recovery through the **Prism Central Backup and Restore** widget in **Settings** > **Prism Central Management**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3034

- Reconfigure the proxy server. For information on how to configure the HTTP proxy through the Prism Central web console, see Configuring an HTTP Proxy in the *Prism Central Admin Center Guide*

  If the old Prism Central instance had a proxy server, reconfigure the proxy server so that the recovered Prism Central instance maps to the correct IP address.

- Reconfigure the fully qualified domain name (FQDN).

  If the old Prism Central instance had an FQDN, reconfigure the FQDN so that the recovered Prism Central instance maps to the correct IP address.

- Recovery plan jobs (RPJ) in progress: Perform the steps in KB-10962.

  If the old Prism Central instance had a failover task running (Nutanix Disaster Recovery) or protection policy with guest VMs protected with synchronous replication schedule, perform the steps in KB 10962 to ensure that all the failover tasks stuck in the running state are terminated and a script is executed for efficient recovery of the Prism Central instance.

- Reconfigure Life Cycle Manager (LCM) if you do not use the Nutanix portal or if you use LCM in the dark site. For information on how to configure LCM on a dark site, see LCM Settings for Dark Sites - No Internet Connectivity. For information on reconfiguration of LCM 3.1, see KB 17966.

Restore Prism Central-Field Information for Continuous Backup

Procedure

1. Select the cluster where you want to restore the Prism Central instance.
2. Verify the version of Prism Central instance that would restore on the selected cluster.
3. Select the network where you want to restore and install Prism Central instances.

   The **Subnet Mask**, **Gateway**, and **DNS Address(s)** fields show the relevant information associated with the selected network.
4. Enter details (name, IP address) for the Prism Central instance you want to restore and click **Save**.
5. Review the summary and click **Recover**.

Restore Prism Central-Field Information for S3-based Object Storage

Procedure

1. In **Connect** tab, specify the following details, then click **Next**.

   a. **AWS Region Name**. Enter an AWS region name. For more information, see `AWS documentation`.

   a. **AWS Bucket Name**. Enter a bucket name. For more information, see `AWS documentation`.

   b. (Optional for NC2 environments) **Access Key**. Enter your access key.

   c. (Optional for NC2 environments) **Secret Access Key**. Enter your secret access key.
2. In **Source** tab, select the Prism Central backup you want to restore, and click **Next**.

   An S3 bucket can be used to back up multiple Prism Central instances. The instances are listed as the `PC_<IP_ADDRESS>` or the FQDN if configured.
3. In **Restore Point** tab, specify the date for the point-in-time backup, and then select one of the available restore points to restore the Prism Central instance and click **Next**.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3035

4. In **Installation** tab, verify the cluster IP address where Prism Central instance was hosted originally and the version of your instance, and click **Next**.
5. In **Configuration** tab, specify the networking details and click **Next**.

   > **Note:** If you are restoring the Prism Central instance from the same cluster (Prism Element web console) where the Prism Central instance was hosted, details like **vLAN**, **Subnet Mask**, **Gateway IP**, **DNS Address(es)**, **NTP Address(es)**, **Container**, and **Virtual IP** are populated automatically. You must configure these details if you are trying to restore the Prism Central instance from a different AZ or a cluster.

6. In the **Microservices** tab, specify the Prism Central service domain name, internal network, and the required input to enable Microservices Infrastructure (CMSP). Nutanix recommends using the default settings for **Subnet Mask**, **Gateway IP Address**, and **IP Address Range**.

   > **Note:** Ensure that the IP address range does not conflict with the reserved DHCP IP address pool in your network.

7. In **Summary** tab, review the information you configured in the previous steps, and click **Restore**.

Migrating a Prism Central Instance

You can use the Prism Central Backup and Restore (PCBR) capability to migrate a Prism Central instance from one cluster to another.

Before you begin

- Ensure that both the primary cluster (where the Prism Central instance is hosted) and the remote cluster (where you want to migrate the Prism Central instance) are registered to the Prism Central instance that you want to migrate.
- Read the *Supported Services for Backup and Recovery* and *Unsupported Services for Backup and Recovery* sections in Implementation Considerations and Limitations on page 556.

Procedure

1. Configure the remote cluster as the backup location for the Prism Central instance that you want to migrate.

   For more information, see Backing up Prism Central on page 558.

   The backup starts immediately and takes a couple of hours to complete. The backup progress and last backup time are visible on the Prism Central web console (go to Settings icon and navigate to **General** > **Prism Central Management** > **Prism Central Backup and Restore** widget. For more information, see Prism Central Settings (Infrastructure).

2. Log in to the Prism Central instance that you want to migrate through SSH as "nutanix" user.
3. Stop the Prism Central instance that you want to migrate using the following command and then type `I agree` as a confirmation.

   ```
   nutanix@pcvm$ cluster stop
   ```

   > **Note:** The Prism Central instance takes 10-15 minutes to stop. Ensure that a backup copy is on the remote cluster before stopping the Prism Central instance.

4. Power off the Prism Central instance.
5. Log in to the remote cluster (Prism Element web console) as an administrator.
6. Perform the restore procedure described in Restoring Prism Central (1-Click Recovery) on page 562.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3036

Disabling Prism Central Backup and Restore

About this task

The following procedure to disable Prism Central Backup and Restore is the same for continuous and point-in-time backup types.

> **Caution:** You can enable Prism Central Backup and Restore only if any one of the Nutanix clusters (Prism Element) registered to the Prism Central instance is running minimum AOS version 6.5.3.1 . For point-in-time backups, you can enable Prism Central Backup and Restore only if any one of the clusters registered to the Prism Central instance is running a minimum AOS version 6.8.

Procedure

1. Log in to the Prism Central web console.
2. Click the Settings icon and navigate to **General** > **Prism Central Management** from the **Settings** menu.
   For more information, see Prism Central Settings (Infrastructure) on page 49).
   The **Manage Prism Central** page appears. This page provides information about this Prism Central deployment.
3. Click **Remove** for the target clusters listed in the **Prism Central Backup and Restore** widget.

What to do next

When Prism Central Backup and Restore is disabled, Prism Central resources are unprotected. To ensure recovery of the Prism Central instance in case of a disaster, enable it again after completing the required tasks that require Prism Central Backup and Restore to be disabled.

Intelligent Operations

Intelligent Operations allows you to run your IT operations efficiently using intelligent operational features that include:

- Cluster activity analysis.
- Application discovery in a cluster.
- Application monitoring in a cluster.
- Resource capacity and usage planning.
- Task automation using playbooks.
- Resource and activity related reports generation for Nutanix and non-Nutanix environments

You can enable Intelligent Operations from **Admin Center** application. For more information, see Enabling Intelligent Operations in *Intelligent Operations Guide*.

Starting from Prism Central version 2023.3, NCM Intelligent Operations (formerly AIOps) now has a new user interface. The following Operations Entities have been moved from Prism Central Infrastructure app to the new user interface created for NCM Intelligent Operations:

- Analysis
- App Discovery
- Monitoring Configurations
- Operations Policies
- Planning

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3037

- Playbooks
- Reports
- Settings and Configurations

The documentation for the above-mentioned entities has been moved to the newly created *Intelligent Operations Guide*. For more information, see Intelligent Operations Guide. You can also find the Intelligent Operations Release Notes under Nutanix Cloud Manager on the documentation portal.

Large Files Upload Using Objects Lite

Objects Lite is miniaturization of Nutanix Objects where the whole objects stack runs as a container in Microservices Architecture.

The Objects Lite service is a compact version of core Nutanix Objects product, specifically designed to operate within the microservices architecture. This service enables Prism Central users to upload large objects with streaming and resumability support to other Prism Central services like images, catalog, and LCM.

This method optimizes the interaction between services and eliminates external interaction. While Objects Lite is Amazon S3-compatible, it offers a limited set of APIs specifically tailored to Prism Central services, including images and catalog.

Objects Lite Data Storage

Objects Lite uses one of the Prism Element registered to Prism Central to store its data. If no Prism Element is registered, Objects Lite waits until one becomes available. A data container named `objectsl<objects-lite-uuid>` is created for this purpose.

> **Note:** Unregistering Prism Element from Prism Central fails and you need to cleanup Objects Lite to successfully unregister Prism Element from Prism Central. In such a case, Nutanix recommends that you contact Nutanix Support.

Objects Lite Limitations

This section lists the limitations of Objects Lite.

The limitations of Objects Lite are as follows:

- User Roles: Only users with Super Admin or Prism Central Admin roles can upload objects..
- Upload-only Support: Objects Lite supports only upload operations. Download and list operations are not supported.
- Failure Handling: If an upload fails, Nutanix recommends that you upload the object again. Depending on the method used (PutObject or Multipart), you might need to upload the entire object or just the failed parts. Make sure to keep track of the successfully uploaded parts if you want to resume the `multipart` upload from the point of failure as `ListParts` API for Prism Central user is not supported.
- Concurrency Limits: Objects Lite supports up to eight parallel requests at a time. When concurrency is higher than eight, you might see the Too Many Requests error. In such cases, try again after some time.
- Temporary storage solution: Objects Lite needs to be cleaned before Prism Central Prism Element unregistration for the Prism Element hosting objects-lite’s data. Post-compliance backup retention (PCBR) events are also not supported, and all Objects Lite data is lost after a Prism Central's PCBR recovery.

Objects Lite Access

Objects Lite provides an endpoint that allows Admin and Super Admin roles to upload data directly to Objects Lite, bypassing the respective service in the data path. This endpoint is specifically designed for uploads and can be accessed using Prism Central user credentials.

The uploaded data can later be consumed by the corresponding services.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3038

Endpoint URL: The endpoint follows the format,

```
https://<pcip>:9440/api/prism/v4.0/objects/
```

> **Note:** This endpoint is Amazon S3-compatible and works with any S3 SDK or AWS CLI.

To access this endpoint, you must authenticate using your PC credentials.

For more information, seeAccessing Objects Lite Using AWS CLI- Put object on page 568.

Accessing Objects Lite Using AWS CLI- Put object

This section contains the `PutObject` AWS CLI commands that you can use to upload a file to Objects Lite.

Before you begin

Ensure that you

- Install AWS CLI.
- Configure AWS CLI with Objects Lite using the `pc-ip`, `username` and `password` attributes.

```
access key: base64(<username>:<password>)
secret key: base64(<username>:<password>)
aws configure set aws_access_key_id <access-key>
aws configure set aws_secret_access_key <secret-key>
aws configure set endpoint_url https://<pc-ip>:9440/api/prism/v4.0/objects/
```

> **Note:** The access and secret keys for Objects Lite use the `base64(<username>:<password>)` format.

About this task

Uploading a file using PutObject, Multipart Upload, or High level upload command.

Procedure

Upload the file using the `PutObject` API with AWS CLI:

```
> aws s3api put-object --bucket <bucket-name> --body <file-path> --key <object-key> --
no-verify-ssl
```

- The following list describes the Parameters in the previous command:
  - --*bucket*: The name of the bucket where the object is stored.
  - --*key*: The key (name) for the object in the bucket.
  - --*body*: The path to the file to upload.
  - --*no-verify-ssl*: Disables SSL certificate verification.

> **Note:** This command supports uploading files smaller than five GB. For larger files, consider using the multipart upload method or the high-level `aws s3 cp` command.

After the file is uploaded, the command displays the ETag of the uploaded object.

Uploading Files to Objects Lite Using AWS CLI - Multipart Upload

This section contains Multipart upload AWS CLI procedure to upload a file to Objects Lite.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3039

About this task

To upload a file using the Multipart Upload API with AWS CLI, follow these steps:

Procedure

1. Initiate multipart upload.

```
$ aws s3api create-multipart-upload --bucket <bucket-name> --key <object-key> --no-
verify-ssl
```

   This command returns an Upload ID.

2. Upload parts.

```
> aws s3api upload-part --bucket <bucket-name> --key <object-key> --part-number
 <part-number> --body <file-path> --upload-id <upload-id> --no-verify-ssl
```

   This command returns an ETag for each part.

3. Complete Multipart upload.

```
> aws s3api complete-multipart-upload --bucket <bucket-name> --key <object-key> --
upload-id <upload-id> --multipart-upload file://<parts-file> --no-verify-ssl
```

   Sample JSON file for completing the upload:

```
{
  "Parts": [
    {
      "ETag": "\"etag1\"",
      "PartNumber": 1
    },
    {
      "ETag": "\"etag2\"",
      "PartNumber": 2
    },
    {
      "ETag": "\"etag3\"",
      "PartNumber": 3
    }
  ]
}
```

   The following list describes the parameters in the previous commands:

   - --*bucket*: The name of the bucket where the object is stored.
   - --*key*: The key (name) for the object in the bucket.
   - --*part-number:* The part number for the part being uploaded.
   - --*upload-id*: The Upload ID received from `create-multipart-upload`.
   - --*multipart-upload*: The JSON file containing the list of parts and their ETags.

     Note: Track the successfully uploaded parts to resume the overall upload process in case of a failure and avoid re-uploading the parts that have already been uploaded. The `ListParts` API is not supported.

Uploading Files to Objects Lite Using AWS CLI - Highlevel upload

This section describes the AWS CLI procedure for high level upload that can be used to upload a file to Objects Lite.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3040

About this task

You can copy files from local storage to S3-compatible endpoints using the AWS S3 copy command (aws s3 cp). It simplifies the uploading process and supports automatic multipart uploads for large files. It also provides support for concurrent uploads, improving performance.

To upload a file using the high level upload command with AWS CLI, follow these steps:

Procedure

1. Configure the multipart threshold, chunk size, and concurrency.

```
$ aws configure set s3.multipart_threshold <multipart-threshold>
$ aws configure set s3.multipart_chunksize <multipart-chunksize>
$ aws configure set s3.max_concurrent_requests <max-concurrent-requests>
```

   The following list describes the parameters in the previous commands:

   - *multipart-threshold*: Size threshold for when to use multipart uploads.
   - *multipart-chunksize*: Size of each part in a multipart upload.
   - *max-concurrent-requests*: Maximum number of concurrent requests for multipart uploads.

2. Upload the file.

```
$ aws s3 cp <file-path> s3://<bucket-name>/<object-key> --no-verify-ssl
```

   Note: This command does not handle resumable uploads or retries in case of failures. In that case, consider uploading the file again.

High Availability in Prism Central

Prism Central supports high availability using the following functionalities:

- **VM high availability: Migrates and restarts the Prism Central VM (PCVM) from a failed node to another node.**

  When a node that hosts a PCVM fails, Acropolis migrates and restarts the PCVM in another node that has enough data resources and entities required to run the PCVM.

  Note: Prism Central supports VM high availability only if your deployment meets the following requirements:

  - PCVM runs pc.2024.1 or later
  - The cluster (Prism Element) runs AOS 6.8 or later
  - AHV version is 20230302.100173 or later.

  Both single VM Prism Central and three VM scale-out Prism Central deployments support high availability using the VM high availability feature in Acropolis.

  For information on high availability, see VM High Availability in Acropolis in the *Prism Element Web Console Guide*. For information on how to enable high availability in a PCVM, see Enabling High Availability for the Cluster in the *Prism Element Web Console Guide*.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3041

- **Scale-out: Scales out a single VM Prism Central deployment to a three-VM deployment with a fault tolerance of one PCVM.**

  Prism Central supports high availability by scaling out a single VM Prism Central deployment to a three-VM deployment with a fault tolerance of one PCVM. For information on how to scale out a Prism Central deployment across multiple VMs, see Expanding (Scale Out) Prism Central.

  In a scale-out Prism Central deployment, if one PCVM fails, the other two PCVMs perform the load balancing for the failed PCVM, and the Prism Central stays active. If two or all three PCVMs fail, then Prism Central is considered inactive.

  For information on the configurations, requirements, specifications, and limitations of scalability, see the *Prism Central Scalability* topic in the release notes for the Prism Central version to be installed.

Finding the Prism Central Version

About this task

You can check the version of your Prism Central instance using the Prism Central user interface or by running the following command.

```
nutanix@cvm$ ncli cluster info
```

Do the following to check the Prism Central version in the UI.

Procedure

1. Log in to Prism Central.
2. Click the user icon in the main menu and then select the **About Nutanix** option from the dropdown menu.
   An **About Nutanix** window appears that includes the AOS version number. It also includes a link to Nutanix patent information.
3. Click **Close** to close the window.

Finding the AHV Version on Prism Central

About this task

You can see the installed AHV version in Prism Central.

Procedure

To view the AHV version installed on any host in the clusters managed by Prism Central, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Hardware** > **Hosts** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
   The system displays the **List** tab by default with all the hosts across registered clusters.
3. Click the target host name for which you want to see the hypervisor version.
   The system displays the Host Details View with **Summary** tab.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3042

4. Observe the Hypervisor Version field in the **Properties** widget to view the hypervisor version.

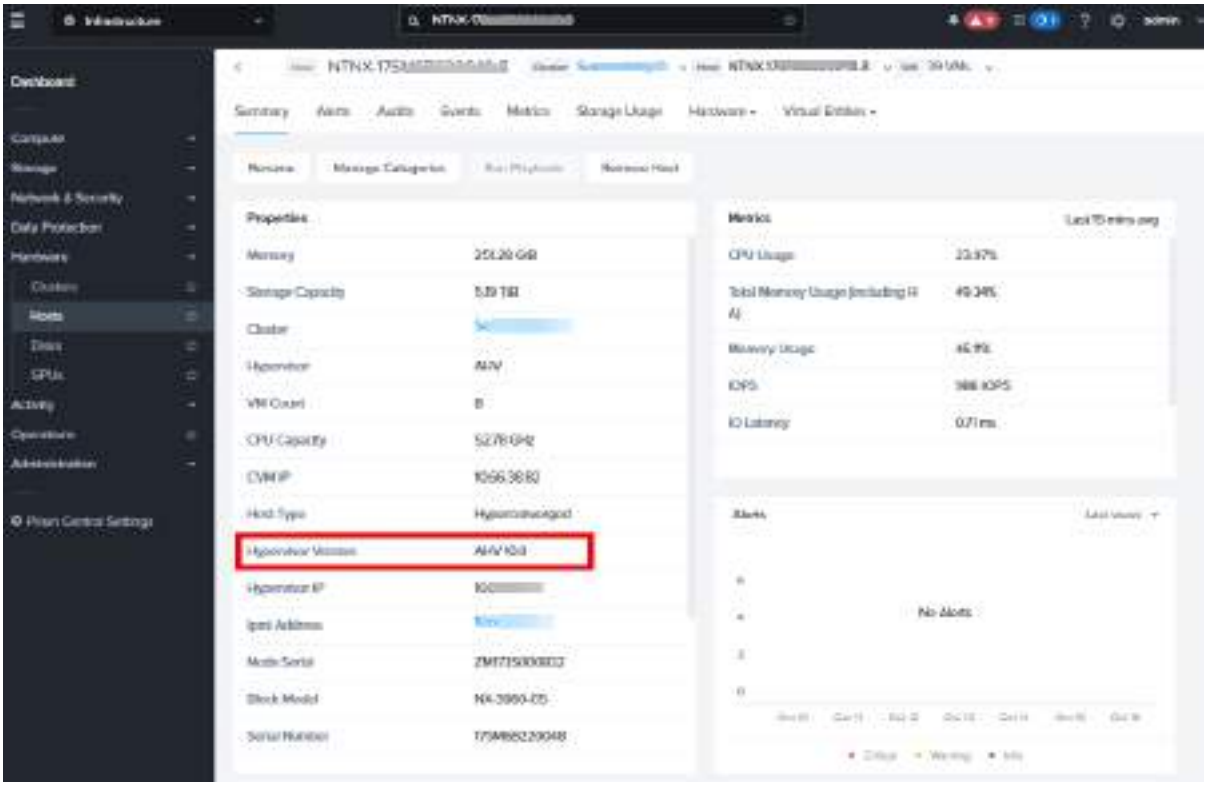


Figure 208: Hypervisor Version in Host Detail View

Finding the AOS Version Using Prism Central

To view the Nutanix AOS version running in the Prism Central, do the following:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 45, and navigate to **Hardware** > **Clusters** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 66.

   The system displays the **List** tab by default with all the registered clusters in **Nutanix** environment.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3043

3. In the **List** tab, the AOS version of the cluster is listed against the cluster name.

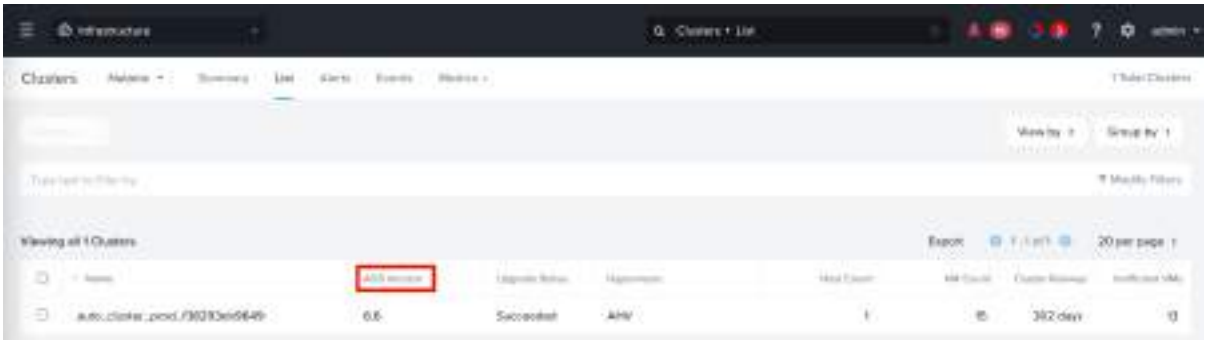


Figure 209: AOS Version in a Cluster

Expanding (Scale Out) Prism Central

Before you begin

The following requirements must be met before you can expand Prism Central or add a Prism Central VM:

- The specified gateway must be reachable.
- No duplicate IP addresses can be used.
- The container used for deployment is mounted on the hypervisor hosts.
- For Prism Central versions lower than 2023.3, the hosting cluster should be registered with Prism Central.
- When installing on an ESXi cluster:
  - vCenter and ESXi cluster must be configured properly. For more information about vCenter and ESXi configuration, see the vCenter Configuration topic in *vSphere Administration Guide for Acropolis*.
  - vCenter must be registered in Prism.
  - DRS must be enabled in vCenter.
  - vCenter is up and reachable during the deployment.

About this task

If Prism Central is just a single VM currently, you can expand it to three VMs. This increases both the capacity and resiliency of Prism Central (at the cost of maintaining two additional VMs). For information on Prism Central scalability, see the *Prism Central Scalability* topic in the release notes for the Prism Central version to be installed.

To expand this Prism Central instance across multiple VMs, do the following:

Note:

- Scaling out of Prism Central VM not registered with the hosting Prism Element is not supported if any of the portfolio products such as Self-Service or Disaster Recovery is enabled on Prism Central.
- All the scale out Prism Central VMs must run on the same cluster. For example, running two VMs in cluster_1 and one VM in cluster_2 is not supported.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3044

- If you have configured application monitoring on a single node Prism Central setup, and you scale out to 3 nodes running Prism Central version PC.2023.4, you must power off and then again power on the newly added nodes.

Procedure

1. Log in to Prism Central.
2. Click the Settings icon and then select **Prism Central Management** from the **Settings** menu. For more information, see Prism Central Settings (Infrastructure) on page 49.
   The **Manage Prism Central** page appears. This page provides information about this Prism Central instance.

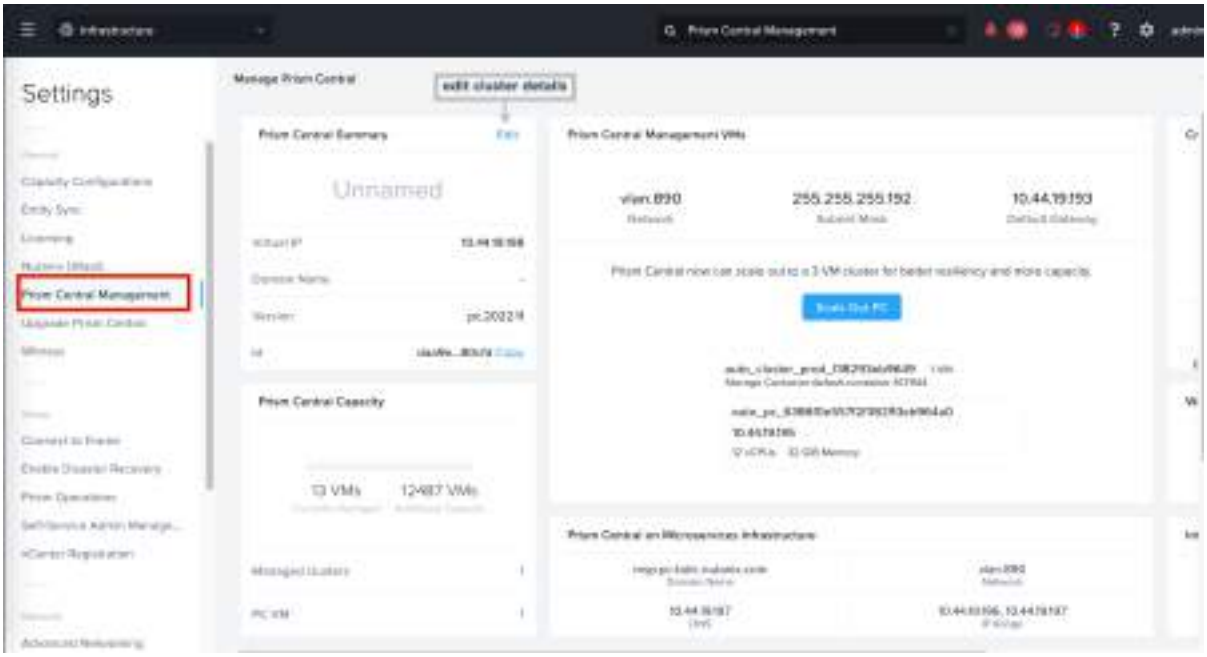


Figure 210: Manage Prism Central Page

3. To expand this Prism Central instance from one to three VMs, click **Scale Out PC** to display the **Scale Out PC** page and do the following:

> **Note:** A pop-up window appears explaining that scale out is a one-way process. Click **Continue** to display the **Scale Out PC** page. Once you scale out a Prism Central instance from a single VM to multiple VMs, you cannot revert back. Deleting any of the Prism Central VMs may result in data loss.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3046

Figure 211: Scale Out PC Page

Note: The Prism Central VM image is deployed from the target cluster. If the required image cannot be accessed, typically because there is no Internet access (such as at a dark site), a pop-up error message appears. In this case you have the option to manually download and deploy the image as follows:

1. Log on to the Nutanix customer support portal, click **Downloads** > **Prism Central**, and click the download link for the target version to save the Prism Central binary .TAR and metadata .JSON files on your local media. The binary .TAR file is from the Prism Element bundle, used for 1-click deployment.
2. Log on (using SSH) to any Controller VM in the cluster specified in the error message and copy the Prism Central binary .TAR and metadata .JSON files to the Controller VM.
3. Run the following command to deploy the Prism Central image:

   ```
   nutanix@cvm$ ncli software upload software-type=PRISM_CENTRAL_DEPLOY file-path=file_path meta-file-path=metadata_file_path
   ```

   The *file_path* is the full (absolute) path to the .TAR file, and the *metadata_file_path* is the full path to the .JSON file. After this step completes, you can continue the scale out procedure.

a. Review the **Network**, **Subnet Mask**, and **Gateway** fields, which display the network name, subnet mask value, and gateway IP address applied to this Prism Central instance.

   The values in these three fields are read-only and cannot be changed.

   Note: The scale-out process uses the IP addresses from the network configured. If you used the default network configuration being the Private Network [default] while enabling microservices infrastructure, Prism Central displays and uses Private Network [default] details in this section.

b. [optional] To specify a virtual IP address for Prism Central, click the **Add Virtual IP** link.

   This displays the **Add PC Virtual IP** window. A virtual IP can be used as a single point of access for Prism Central. Enter the IP address in the Virtual IP field, and then click **Update**.

c. Specify IP addresses for the two new Prism Central VMs.

   1. Click the pencil icon for one of the new VMs. (The VM names are set automatically.) The **IP field** opens for editing. Enter the IP address and then click the green check mark icon to save that address.

Figure 212: Edit IP Field

   2. Repeat this step for the second new VM.

   The vCPU count and memory size in the new VMs are fixed and match the current Prism Central VM values; you cannot change these values.

d. When all the parameters are correct, click **Expand**.

   This starts the process of creating the new VMs and deploying this Prism Central instance. You can monitor progress from the **Tasks** page. For more information, see Tasks View on page 452.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3048

What to do next

In some cases, especially when using NCM Self-Service (formerly known as Calm), a version mismatch with a linked product could occur after expanding Prism Central. To fix this situation, perform a life cycle manager (LCM) inventory after completing the Prism Central expansion procedure. For instructions on how to perform an LCM inventory, see the LCM documentation.

Shutting Down or Starting Up Prism Central VM

About this task

A Prism Central VM (PC VM) is managed like any other VM in a cluster through the Prism Element web console for the cluster in which the Prism Central VM is running. However, shutting down a PC VM requires extra caution.

> **Note:**
>
> Prism Central supports features that could be damaged by shutting down the PC VM abruptly. You must follow the steps carefully to avoid any issues.

Procedure

- To shut down the PC VM in single VM configuration, or to shut down all the three PC VMs in a scale out configuration, see Shutting down or starting up all the PC VMs in a Prism Central Configuration on page 578.
- To shut down a single PC VM in a scale-out Prism Central configuration, see Shutting down or starting up a single PC VM in a scale-out PC configuration on page 579.

Shutting down or starting up all the PC VMs in a Prism Central Configuration

About this task

To shut down the PC VM in single VM configuration, or to shut down all the three PC VMs in a scale out configuration, perform the following steps:

Procedure

1. SSH to the IP address of the PC VM that you want to shut down.
2. Stop the cluster.

   ```
   nutanix@pcvm$ cluster stop
   ```

3. Check the status of the services running on the cluster.

   ```
   nutanix@pcvm$ cluster status
   ```

   The command output should show the following three services still running: Zeus, Scavenger, and VipMonitor.

4. To shut down a PC VM, log on to the web console of the host and go to the VM dashboard (see VM Dashboard in Prism Element Web Console Guide). In the VM Table view, select the PC VM you want to shut down (one at a time), and then select **Power Off Actions >> Power Off** or **Power Off Actions >> Guest Shutdown** from the action links.

   Alternatively, you can SSH to the IP address of the PC VM and run the command to shut down the PC VM.

   ```
   nutanix@pcvm$ sudo shutdown -h now
   ```

   You must run this command for each PC VM that you want to shut down.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3049

5. To power on a PC VM, log on to the web console of the host and go to the VM Dashboard (see VM Dashboard). In the VM Table view, select the PC VM you want to power on (one at a time), and then select **Power On**.
6. Once all the PC VMs are powered on, check the status of the services from any one of the PC VMs.

   ```
   nutanix@pcvm$ cluster status
   ```

   In the command output, verify that all the three services (Zeus, Scavenger, and VipMonitort) are running.
7. Once all the three services start running, start the cluster from any one of the PC VMs.

   ```
   nutanix@pcvm$ cluster start
   ```

Shutting down or starting up a single PC VM in a scale-out PC configuration

About this task

To shut down or start up a single PC VM in a scale-out PC configuration, perform the following steps:

Procedure

1. SSH to the IP address of the PC VM.
2. Run the following command to gracefully stop all the services:

   ```
   nutanix@pcvm$ genesis stop all
   ```

3. Now log on to the web console of the host and go to the VM dashboard (see VM Dashboard in *Prism Element Web Console Guide*).
4. In the VM Table view, select the PC VM you want to shut down, and then select **Power Off Actions >> Power Off** or **Power Off Actions >> Guest Shutdown** from the action links.

   Alternatively, you can SSH to the IP address of the PC VM and run the command to shut down the PC VM.

   ```
   nutanix@pcvm$ sudo shutdown -h now
   ```

5. To power on a PC VM in a scale-out PC configuration, log on to the web console of the host and go to the VM Dashboard (see VM Dashboard). In the VM Table view, select the PC VM you want to power on (one at a time), and then select **Power On**.
6. Restart the genesis service:

   ```
   nutanix@pcvm$ genesis restart
   ```

7. Check the status of the services running on the cluster.

   ```
   nutanix@pcvm$ cluster status
   ```

8. Start the services in the PC VM:

   ```
   nutanix@pcvm$ cluster start
   ```

Keyboard Shortcuts in Prism Central

You can use the following keyboard shortcuts to invoke important menu options or views in Prism Central:

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3050

Table 160: Keyboard Shortcuts for Prism Central Menu Options

Shortcut Key	Menu Option/View
s	Settings Menu
f	Spotlight (search bar)
u	User Menu
h	Help menu (? menu)
p	Recent tasks

You can use the arrow keys to select a particular menu option.

IP Address Reconfiguration

You can use this procedure to reconfigure the IP address and gateway of single Prism Central instances as well as Prism Central VMs in a Scale out Prism Central (clustered PC VMs or PC cluster).

> **Note:** Reconfiguring the IP address and gateway of Prism Central VMs does not require additional steps when using Nutanix Disaster Recovery (formerly Leap).

Preparing to Reconfigure the IP Address and Gateway of PC VMs

Perform the tasks described in this topic before you start the IP address reconfiguration procedure.

About this task

You must perform the following tasks while the Prism Central VMs are still on the existing IP addresses.

Procedure

1. Coordinate Prism Central downtime, because the features and functionality of Prism Central will be unavailable for the entire duration of the IP address reconfiguration procedure.
2. Create a table to map the existing IP addresses with the new IP addresses of the Prism Central VMs for your reference.
3. Use SSH to log on to any running Prism Central VM in the PC cluster or the single PC VM if you do not have a PC cluster.
4. Verify if the PC VM or PC cluster is in a stable state.

   ```
   nutanix@pcvm$ cluster status
   ```

   This command is valid even if you only have a single PC VM and do not have a PC cluster.
5. Run the NCC health checks to make sure that the PC cluster is in a healthy state.
6. If you want to reconfigure the IP addresses of the entities in the AOS clusters (such as IP addresses of CVMs and hypervisor hosts), on which the PC is hosted, reconfigure those IP addresses first before you reconfigure the IP addresses of the PC VMs.
7. Stop the PC VM or PC cluster.

   ```
   nutanix@pcvm$ cluster stop
   ```

   This command is valid even if you only have a single PC VM and do not have a PC cluster.

   Wait to proceed until an output showing all the services as DOWN is displayed, except the Zeus and Scavenger services.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3051

Reconfiguring the IP Address and Gateway of Prism Central VMs

Before you begin

Ensure that you have completed the tasks described in Preparing to Reconfigure the IP Address and Gateway of PC VMs on page 580.

About this task

The procedure to reconfigure the IP addresses of PC VMs differs depending on whether or not IP Address Management (IPAM) is enabled in an AHV cluster. The procedure to reconfigure the IP addresses of PC VMs in an ESXi cluster is the same as the procedure of an AHV cluster in which IPAM is disabled.

For information on IPAM, see IP Address Management section in the *AHV Administration Guide*.

In this document, managed network refers to an AHV network that has IPAM enabled, and unmanaged network refers to an AHV network that does not use IPAM.

Note:

- Reconfiguration of PC VM IP addresses is not supported for Prism Central scale-out deployments used in Nutanix Cloud Clusters (NC2) on AWS or Azure environment.
- Do not reconfigure the IP address of the PC VM if any Nutanix Kubernetes Engine (NKE) or Objects are deployed on the cluster since changing the PC VM IP address is not supported for NKE or Objects after deployment.

Perform the following procedure to reconfigure the IP address of a single PC VM or PC VMs in a PC cluster.

Procedure

1. Log in as `nutanix` user and run the *external_ip_reconfig* script.

```
nutanix@pcvm$ external_ip_reconfig
```


Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3052

2. Follow the prompts to type the new netmask, gateway, and external IP addresses.

   A message similar to the following is displayed when the procedure begins:

   ```
   External IP reconfig started
   ```

   A message similar to the following is displayed if the procedure is completed successfully:

   ```
   External IP reconfig finished successfully. Restart all the CVMs and start the
    cluster.
   ```

   The message indicates that you must restart the CVMs. In this case, you are reconfiguring the IP addresses of the PC VMs, so you must restart the PC VMs and not the CVMs.

   > **Note:**
   >
   > If your PC VMs are running in a managed network of an AHV cluster, do not start the PC VMs yet but proceed to step 3.
   >
   > If your PC VMs are in an unmanaged network of an AHV cluster or are in an ESXi cluster, skip steps 3, 4, and 5, and proceed to step 6 directly.
   >
   > Perform steps 3, 4, and 5 only if the new IP address is in a different IP address range than the previous IP address range and your PC VM is in a managed network of an AHV cluster.

   A message similar to the following is displayed if the procedure fails:

   ```
   External IP reconfig Failed
   ```

   If the procedure fails, run the following command to check the log for troubleshooting purposes:

   ```
   nutanix@pcvm$ cat ~/data/logs/ip_reconfig.log
   ```

3. (Optional) Use SSH to log onto any CVM of the AOS cluster that is hosting the PC cluster or PC VM.

   > **Note:** Perform this step only if the new IP address is in a different IP address range than the previous IP address range and your PC VM is in a managed network of an AHV cluster.

4. (Optional) Update the NIC attached to the PC VM with the new IP address of the PC VM using the following command:

   > **Note:** Perform this step only if the new IP address is in a different IP address range than the previous IP address range and your PC VM is in a managed network of an AHV cluster.

   ```
   nutanix@cvm$ acli vm.nic_update pc-vm-name pc-vm-mac request_ip=true ip=pc-vm-ip
   ```

   Replace the variables with their appropriate values as follows:

   - *pc-vm-name*: Name of the Prism Central VM whose IP address you modified.
   - *pc-vm-mac*: MAC address of the Prism Central VM whose IP address you modified (press **Tab** after you type the name of the PC VM to automatically populate the MAC address).
   - *pc-vm-ip*: New IP address of the Prism Central VM.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3053

5. (Optional) Log on to the Prism Element web console and modify the IP address range in the IP pool for the PC network to work with the modified IP address of Prism Central VMs. In the Prism Element web console, perform the following:

   > **Note:** Perform this step only if the new IP address is in a different IP address range than the previous IP address range and your PC VM is in a managed network of an AHV cluster.

   a. In the **VM** dashboard, click the **Table** view.

   b. Select a **PC VM** and click **Update**.

   c. In the **Update VM** dialog box, scroll down to the **Network Adaptors (NIC)** section.

   d. In the **VLAN Name** column, note the names of the networks attached to your PC VM.

   e. Click **Close**.

   f. Click the gear icon in the top-right corner, and under **Settings**, click **Network Configuration**.

   g. In the **Network Configuration** dialog box, identify the network names you noted in step d.

   h. Select each network and click the pencil icon next to the network.

   i. Under **IP Address Pools**, modify the IP address range if the new IP address of the PC VM is in a different IP address range than the previous IP address range.

6. Restart each Prism Central VM in the PC cluster or the single PC VM if you do not have a PC cluster.

7. Once the PC VMs are powered on, use SSH to log on to each PC VM or the single PC VM if you do not have a PC cluster and verify if the output of the following verification command displays the new IP addresses:

   ```
   nutanix@pcvm$ python cluster/bin/external_ip_reconfig_verify.py
   ```

8. Start the PC cluster using the following command:

   ```
   nutanix@pcvm$ cluster start
   ```

9. Perform the steps mentioned in KB-15469.

   > **Note:** If Prism Element is not registered to Prism Central and you reconfigure the Prism Element or Prism Central IP address, ensure that the trust setup is re-established for the functioning of Microservices (CMSP) infrastructure. For more information, see KB 12603.

10. Perform the following verification steps:

    a. Log on to the Prism Element web console of every cluster attached to the PC VM whose IP address you changed.

    b. On the **Home** page, verify if the **PC Registration** status is displayed as **OK**. This might take a few minutes after the PC VM or PC cluster is powered on.

What to do next

If you need to change the IP address of the Prism Element cluster hosting the Prism Central VMs, you must first complete the steps for changing the IP address of the PC VM and restart the PC VM. Wait till all the services in Prism Central are restarted and then run the following command on Prism Element to ensure that the new IP address of Prism Central is now associated with the Prism Element cluster:

```
ncli multicluster get-cluster-state
```

If the new IP address of the PC VM is not reflected in the command output of the above command, contact Nutanix Support.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3054

Logging Out of Prism Central

Procedure

To log off from Prism Central, select **Sign Out** from the user menu that appears on the far right side of the Prism Central landing page. You are logged out immediately after selecting the option (no prompt or message).

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3055

CUSTOMER SUPPORT SERVICES

Nutanix provides customer support services in several ways.

- Nutanix customer support can monitor your clusters and provide assistance when problems occur through the Pulse mechanism. For more information, see Pulse Health Monitoring information in *Prism Central Admin Center Guide*.
- Nutanix customer support maintains a portal that you can access to request assistance, download various product updates, and view documentation. For more information, see Accessing the Nutanix Support Portal (Prism Central) on page 590.
- If you need help, you can create a support ticket directly from Prism Central. For more information, see Creating a Support Case on page 586.
- Nutanix technical support can remotely assist with problems in a Prism Central (PC) VM by logging into the faulty PCVM through an SSH connection. For more information, see Configuring Remote Connection Using CLI on page 585.

Configuring Remote Connection Using CLI

You can enable a remote support connection tunnel for a maximum of 72 hours using CLI.

About this task

If you face an issue in your Prism Central (PC) VM and the Nutanix Support team needs access to it to troubleshoot the issue, you can open a support tunnel for the Nutanix Support team to give remote access to your VM. The Nutanix Support team ensures that the connection to your PCVM through the support tunnel is secure and compliant by consolidating connectivity, authentication, authorization, audit, and recorded sessions.

Use the following procedure to enable the remote support connection tunnel.

Procedure

1. SSH into CVM or PCVM .
2. Start ncli.

```
nutanix@cvm$ ncli

<ncli>
```

3. Run the cluster start-remote-support with the duration parameter set as required.

   The duration parameter must be set in minutes even if you need a duration of hours.

```
ncli> cluster start-remote-support duration=<minutes>
```

   Add duration that you want to enable the remote support connection tunnel for, in minutes. For example, if you want to keep the connection open for 24 hours, enter `duration=1440`.

> **Note:** You can keep the remote support connection tunnel between 0-72 hours.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3056

Creating a Support Case

About this task

Nutanix customer support maintains a portal where you can get assistance by opening a support case and viewing the status of your open cases (see Accessing the Nutanix Support Portal (Prism Central) on page 590). However, you can also create a support case directly from Prism Central. To create a support case or view information about your open cases, do the following:

> **Note:** A support portal connection is required before you can create a case (see Prism Licensing on page 59). In addition, at least one cluster must be registered with Prism Central. Also, this feature is available only to customers who get support directly from Nutanix (such as NX and SX model customers), not customers who get initial support from third parties.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3057

Procedure

1. Click the Help icon in the main menu and select **Create Support Case** from the dropdown menu.

   The **Create new support case** page appears. One of the following appears on this page:

   - If there are no open cases currently, a blank page with fields for creating a case appears.
   - If you have one or more open support cases, summary information about those cases appears (see Viewing Case Status on page 589). To create a case from this page, click the **Create new support case** button (upper right). The blank page with fields for creating a case will appear.

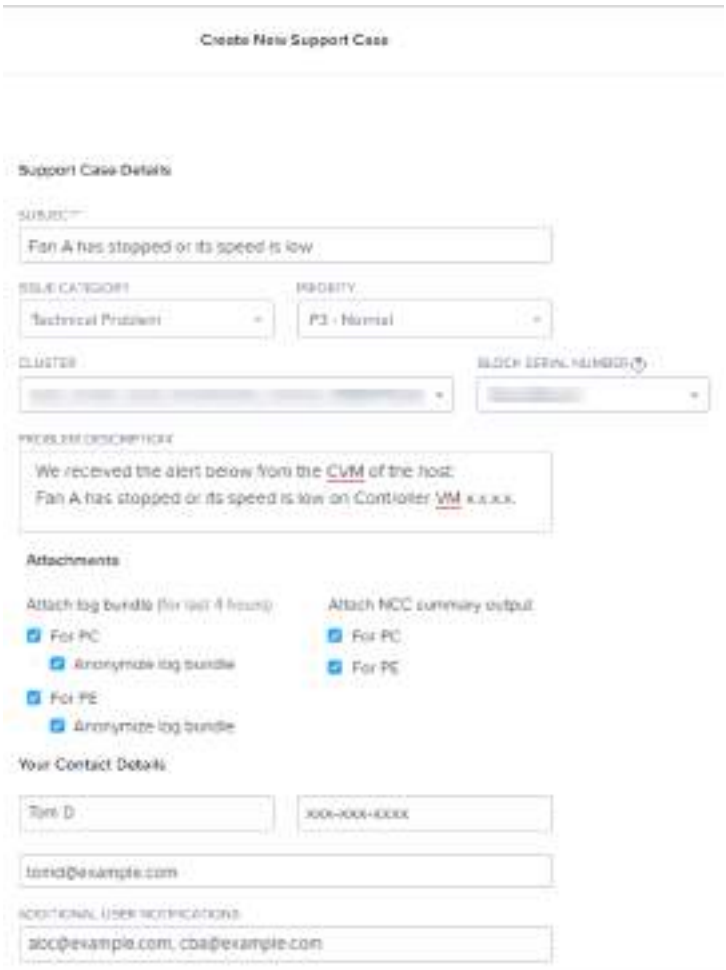


Figure 213: Create New Support Case Page

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3058

2. Do the following in the indicated fields:

   a. **Subject**: Enter a title that briefly describes the issue.

   b. **Issue Category**: Select the type of issue from the dropdown menu.

      The types are **Technical Problem**, **Question**, **Comment/Feedback**, **Scheduled Upgrade/ Maintenance**, **RFE** (request for enhancement), **Licensing**, **Non Technical issue**, and **Technical Problem - Foundation**.

   c. **Priority**: Select the priority for this issue from the dropdown menu.

      There are four priority levels based on the severity of the problem plus a request for enhancement option. Select the appropriate priority based on the following descriptions.

      - **P1 - Emergency**. System is not available and productivity has been halted. Product is unusable in its current state.
      - **P2 - Critical**. System is available but experiencing issues which have a direct impact on productivity. Major inconvenience.
      - **P3 - Normal**. System is having an occasional issue that has been identified as needing to be resolved, but the issue has not greatly affected productivity. Minor inconvenience.
      - **P4 - Low**. Questions about documentation, processes, or procedures. General requests about information.
      - **RFE - Request for Enhancement**. Feature requests for the product which would improve the experience or functionality for the customer.

   d. **Cluster**: Select the target cluster from the dropdown menu.

   e. **Block Serial Number**: Select the serial number of the asset (node) in question from the dropdown menu.

      If you need more information, see the "Installed Base" page on the Nutanix support portal for a list of your assets and the corresponding serial numbers.

   f. **Tell Us More**: Enter a description of your issue in the text box.

      Include any relevant details that might help Nutanix customer support analyze and resolve your issue.

   g. **Attach log bundle (for last 4 hours)**: Check this box to attach log files from the last four hours to the case. If you want the attached logs to be anonymized (personally identifiable information removed), check the **Anonymize log bundle** box.

      - **For PC**: Check this box to attach Prism Central log files from the last four hours to the case. If you want the attached logs to be anonymized (personally identifiable information removed), check the **Anonymize log bundle** box.
      - **For PE**: Check this box to attach Prism Element log files from the last four hours to the case. If you want the attached logs to be anonymized (personally identifiable information removed), check the **Anonymize log bundle** box.

      > **Note:** If the target cluster is not connected to the Internet, such as in a dark site, a log bundle or NCC summary report (following step) cannot be attached to the case through this method.

   h. **Attach NCC summary output**

      - **For PC**: When this box is checked, NCC is run, and the summary output of Prism Central is attached. This ensures that the NCC (health checks) results reflect the current state.
      - **For PE**: When this box is checked, NCC is run, and the summary output of Prism Element is attached. This ensures that the NCC (health checks) results reflect the current state.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3059

i. **Your Contact Details**: Enter your name, phone number, and e-mail address in the indicated fields. Case updates are sent to your e-mail address. You can also have the case updates sent to (up to two) additional users by entering their e-mail addresses in the **Additional User Notification** field.

3. When the entered information is completed, click **Submit**.

   This submits the case to Nutanix customer support for review and response. The speed of response reflects the priority of the issue, where P1 and P2 issues have a higher priority and more rapid response than less critical issues, but Nutanix customer support strives to handle all cases as quickly as possible.

   A Prism Central task is started to create the case. If you selected to attach a log bundle and/or NCC summary output, a task is started for each selected item. The tasks run asynchronously, and you can check the progress (case creation, log collection, and health check tasks) through the tasks dashboard (see Tasks View on page 452). If a task encounters a problem, you can hover the cursor over the "Failed" status to see a brief explanation. Automatically generated comments (preceded by "Prism Central Automated Note:") are added to the case when the log/health checks collection starts and when the upload completes. When the tasks complete, the output (log bundle and NCC summary report) appear as attachments in the case summary (see Viewing Case Status on page 589).

Figure 214: Tasks Dashboard for Prism Central (create case tasks)

Figure 215: Tasks Dashboard for Prism Element (create case tasks)

Viewing Case Status

You can view information about open support cases directly from Prism Central by clicking the Help icon in the main menu and selecting **Create Support Case** from the dropdown menu. This opens the **Create new support case** page, which displays summary information about open cases (if any). When you have one or more open cases, this page displays the following sections:

- **Open Cases** column (on the left). There is an entry (line) for each open case that includes the case name and number; click the desired case entry to displays summary information about that case in the main section of the page.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3060

- Main section (in the middle). This section displays the creation date, description, attachments (if any), and other information related to the selected case. This is an abridged version of the full case details available from the Nutanix support portal (see below).
- **Key Insights** column (on the right). This section includes the following fields:
  - **Status**: Displays the current status of the case.
  - **Created By**: Displays the name of the user who created the case.
  - **Type**: Displays the type (category) of issue the user specified when creating the case.
  - **Case number**: Displays the number assigned to this case.
  - **Serial Number**: Displays the serial number of the asset (node) in question.
  - **Access Portal**: Includes a link to the Nutanix support portal. Clicking the **View Details in Portal** link opens the details page for that case in the support portal in a new tab or window. The details page in the support portal provides the full details and history of that case should you desire more information, and you can submit additional material to the case such as screen shots or other relevant information.

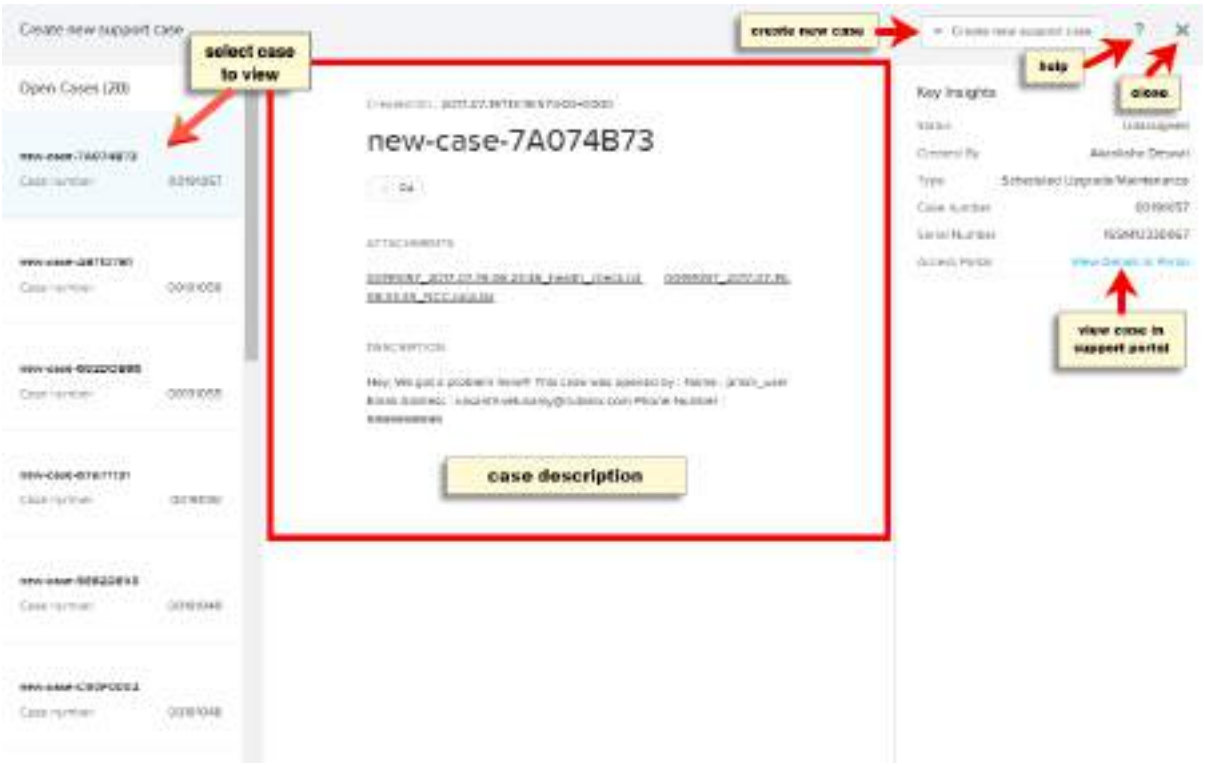


Figure 216: Create New Support Case Page (open cases)

Accessing the Nutanix Support Portal (Prism Central)

About this task

Nutanix provides a variety of support services and materials through its support portal.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3061

Procedure

1. To access the Nutanix support portal from Prism Central, select **Support Portal** from the User icon dropdown menu of the main menu.

   The login screen for the Nutanix support portal appears in a new tab or window.

2. Enter your support account user name and password.
   The Nutanix support portal home page appears.

3. Select the desired service from the screen options.

   You can select an option from one of the main menu dropdown menus or search for a topic at the top of the screen, click one of the icons (Documentation, Open Case, View Cases, Downloads) in the middle, or view one of the selections at the bottom such as an announcement or KB article. The following table lists the menu options.

   Note: Some options have restricted access and are not available to all users.

Table 161: Main Menu Options

Category	Option	Description
Documentation	Software Documentation	Displays a page from which you can view the Nutanix software manuals.
	Hardware Replacement Documentation	Displays a page from which you can view the Nutanix hardware replacement manuals.
	Knowledge Base	Displays a page from which you can view the knowledge base (KB) articles.
	Solutions Documentation	Displays a page from which you can view documents that describe how to implement the Nutanix platform to solve a variety of business applications.
	EOL Information	Displays a page from which you can view the end of life policy and bulletins.
	Field Advisories	Displays a page from which you can view field advisories.
	Training	Provides a link to the separate Nutanix training portal.
	Security Advisories	Displays a page from which you can view security advisories.
	AOS Upgrade Paths	Displays a page where you can see the supported AOS release upgrade paths.
	Compatibility Matrix	Displays a page from which you can view a compatibility matrix broken down (filtered) by hardware model, AOS version, hypervisor type and version, and feature version (NCC, Foundation, BMC/ BIOS).
	Webinar Recordings	Displays a page with links to a selection of Nutanix training webinars.
Support	Open Case	Displays a form to create a support case.
	View Cases	Displays a page from which you can view your current support cases.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3062

Category	Option	Description
	.NEXT Forums	Provides a link to the (separate) Nutanix Next Community forum.
	Terms & Conditions	Displays a page from which you can view various warranty and terms and conditions documents.
Downloads	AOS (NOS)	Displays a page from which you can download AOS releases.
	Acropolis File Services (AFS)	Displays a page from which you can download the Acropolis File Services.
	Acropolis Container Services (ACS)	Displays a page from which you can download the Acropolis Container Services.
	Hypervisor Details	Displays a page from which you can download Acropolis hypervisor versions. You can also download supporting files used when manually upgrading a hypervisor version (AHV, ESXi, or Hyper-V).
	Prism Central	Displays a page from which you can download the Prism Central installation bundle. There are separate bundles for installing on AHV, ESXi, or Hyper-V.
	Phoenix	Displays a page from which you can download Phoenix ISO files.
	Foundation	Displays a page from which you can download Foundation releases.
My Products	Installed Base	Displays a table of your installed Nutanix appliances, including the model type and serial number, location, and support coverage.
	Licenses	Displays a table of your product licenses along with options to add or upgrade licenses for your clusters.

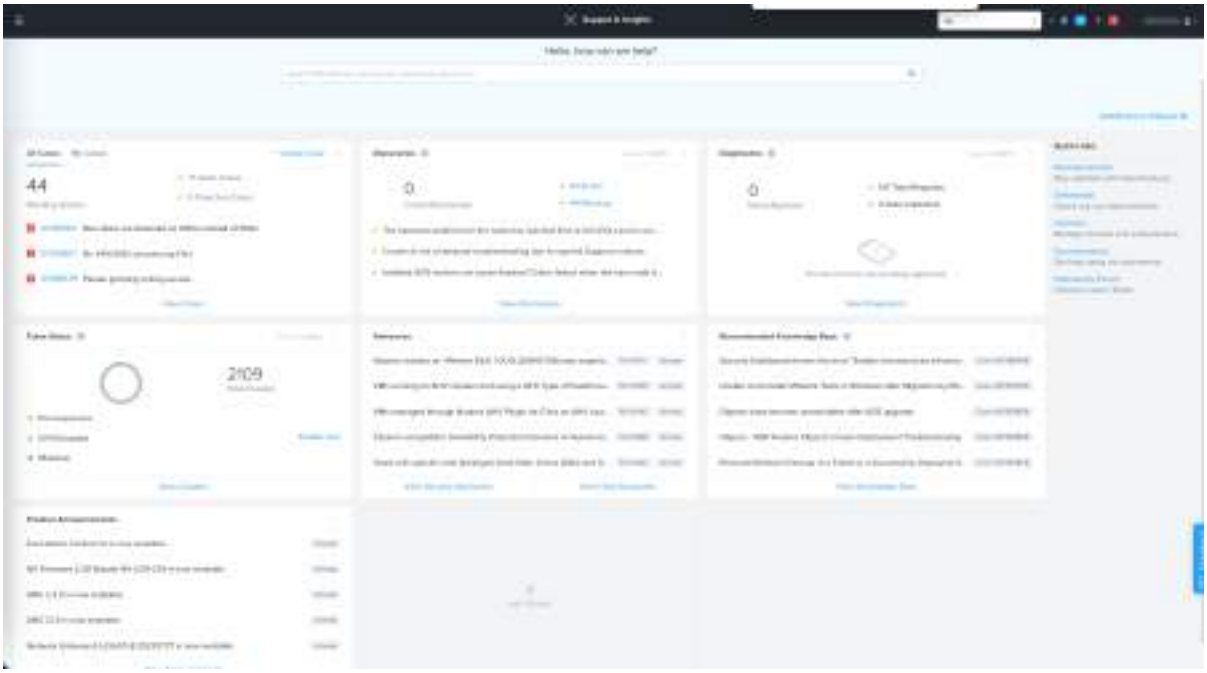


Figure 217: Nutanix Support Portal

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3063

Accessing the REST API Explorer

About this task

Nutanix provides a utility with the web console to help you get started with the REST API. The Explorer displays the parameters and format for the API calls that can be included in scripts. Sample API calls can be made to show the type of output you should expect to receive. Only an admin user can access the REST API Explorer.

The v3 API can be viewed in the REST API Explorer.

Procedure

1. Log on to Prism Central, click the User icon in the upper-right corner of the web console, and click **REST API Explorer**.

   The REST API Explorer displays a list of the objects that can be managed by the API.

2. Find the object you want to explore and click the name of the object to expand and show the detailed view of the operations that can be run on this object.

   For example, click **alerts**. All the API calls for **alerts** are displayed.

   a. Click **GET** to show the details for this API call.

   b. Click **Try it out!** to test the API call when used with your cluster.

   c. Similarly, you can explore other API calls.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3064

HELP RESOURCES

There are several information sources that you can access at any time when you need help:

- Prism Central help documentation (see Accessing Online Help (Prism Central) on page 594).
- Nutanix customer support portal (see Accessing the Nutanix Support Portal (Prism Central) on page 590).
- Nutanix community forum (see Accessing the Nutanix Next Community on page 595).
- Glossary of terms (see Nutanix Glossary).

Accessing Online Help (Prism Central)

About this task

Prism Central includes online help documentation that you can access at any time.

Procedure

1. To open the online help, choose one of the following from the Help icon dropdown menu of the main menu:

   » Select **Help with this page** to display help documentation that describes the current screen.

   > **Note:** In a task window click the Help icon in the upper right to display the help documentation for that window.

   » Select **Online Documentation** to display the **Help Organization** page.

   A context-sensitive help page or the **Help Organization** page appears in a new tab or window. (These pages are located on the Nutanix support portal.) The **Help Organization** page provides descriptions of the major help topics with links to the entry page for each major topic. The display includes a breadcrumb at the top to navigate through the help pages.

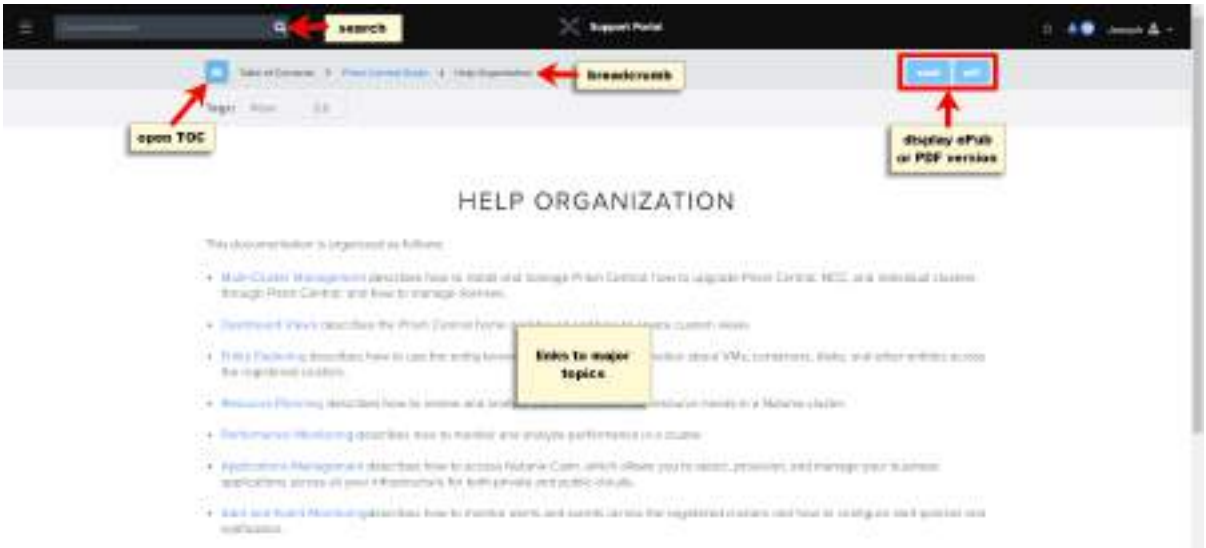


Figure 218: Help Organization Page

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3065

2. To select a topic from the table of contents, click the Navigation icon.

   A table of contents pane appears on the left. Click a topic in the table of contents to display that topic.

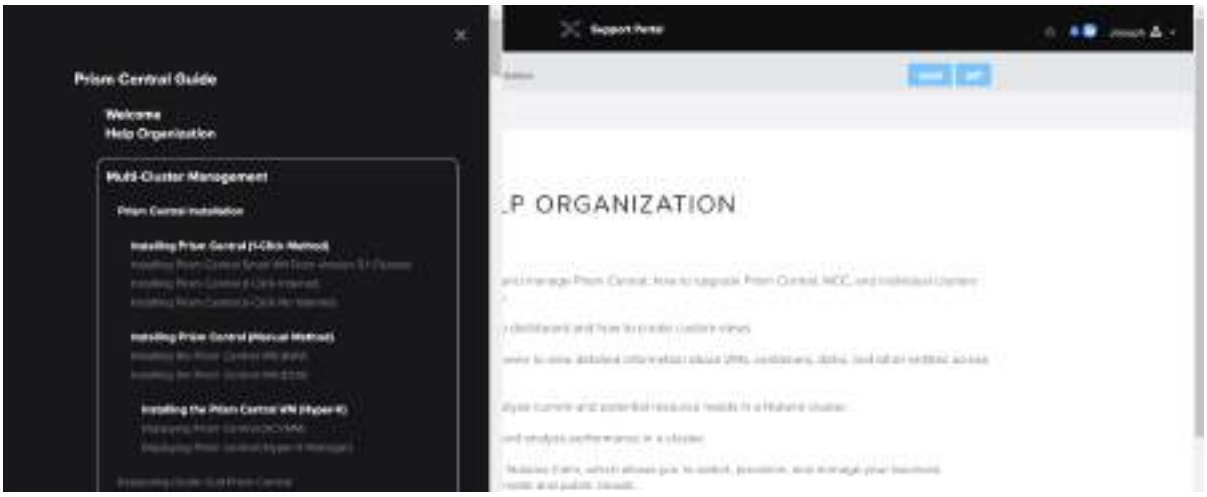


Figure 219: Table of Contents Pane

3. To display all the help contents as a single document, click **epub** or **pdf** in the upper right.

   You can view the *Prism Central Infrastructure Guide* in either ePUB or PDF format by selecting the appropriate option. If your browser does not support the selected format, you can download the PDF or ePUB file.

4. To search for a topic, click the magnifying glass icon in the main menu bar and enter a search string in the field.

   This searches not only the help contents, but also all the documentation, knowledge base articles, and solution briefs. Matching results appear below the search field. Click a topic from the search results to display that topic.

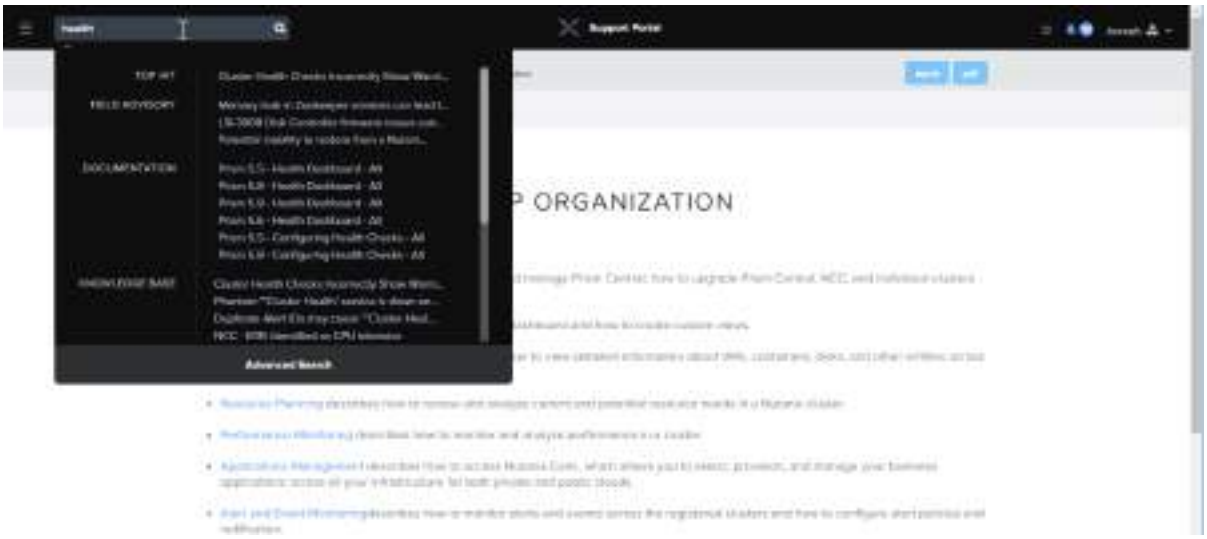


Figure 220: Search Results Example

Accessing the Nutanix Next Community

Nutanix maintains a community forum for customers and partners to facilitate a peer-to-peer exchange of ideas, tips, and information about Nutanix technologies and the rapidly changing landscape of data center IT.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3066

Procedure

- To access the Nutanix next community forum from Prism Central, select **Nutanix Next Community** from the Help icon dropdown menu of the main menu (see Prism Central Landing Page on page 41).

  The Nutanix Next Community main page appears in a new tab or window. From this page you can search existing posts, ask questions, and provide comments.

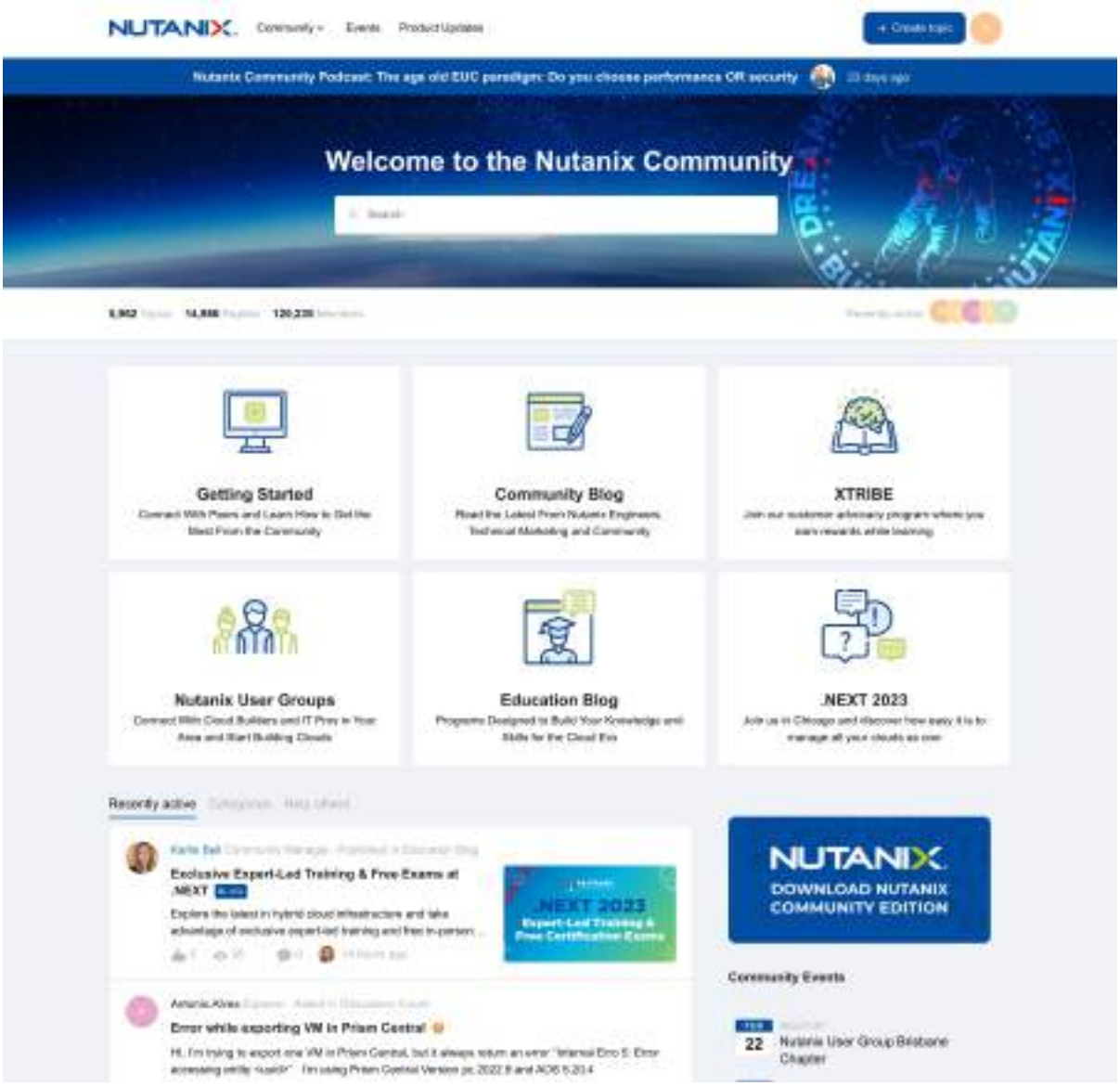


Figure 221: Next Community Screen

Glossary

For terms used in this guide, see Nutanix Glossary.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3067

COPYRIGHT

Copyright 2025 Nutanix, Inc.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Nutanix and the Nutanix logo are registered trademarks of Nutanix, Inc. in the United States and/or other jurisdictions. All other brand and product names mentioned herein are for identification purposes only and may be trademarks of their respective holders.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3068

HPE JUNIPER networking

Data sheet

QFX5120 ETHERNET SWITCH

HPE

Product overview

The QFX5120 Switch delivers rich, low latency Layer 2/Layer 3 features and advanced EVPN-VXLAN capabilities, making it an ideal data center top-of-rack and distribution switch for campus enterprise deployments.

Featuring L3 gateway capabilities for routing between virtualized and bare-metal servers, the QFX5120 is designed for extremely agile data centers that require support for overlay/underlay network architectures. Native 25GbE with 100GbE uplink ports on the QFX5120-48Y and QFX5120-48YM, 10GbE/1GbE copper with 100GbE uplink ports on the QFX5120-48T, and 32 100GbE ports on the QFX5120-32C make the QFX5120 family ideal for spine- and-leaf network deployments.

Product description

The Juniper Networks QFX5120 Switch delivers high scale, high availability, and high performance for data center and campus deployments. The QFX5120 Switch is a versatile routing and switching platform addressing higher server access speed and campus distribution use cases while offering high-density 1GbE/10GbE/25GbE and 100GbE uplinks for collapsed spine data center or campus distribution deployments

Product options

The QFX5120 Switch includes four compact 1 U platforms — the QFX5120-48Y, the QFX5120-48YM, the QFX5120-48T, and the QFX5120-32C — that provide wire-speed packet performance, very low latency, and a rich set of Junos operating system features.

QFX5120-48Y

The QFX5120-48Y is a 25GbE/100GbE data center leaf and campus distribution switch featuring:

— 48 25GbE (SFP28)/10GbE (SFP+)/1GbE (SFP) downlink ports

— Eight 100GbE (QSFP28)/40GbE (QSFP+) uplink ports

— Up to 2/4 Tbps (uni/bidirectional) of L2 and L3 performance, with latency as low as 800 nanoseconds

— A 2.2 GHz quad-core Intel® CPU with 16 GB memory and 50 GB SSD storage

Using breakout cables, each of the eight 100GbE QSFP28 ports can be broken into four 25GbE SFP28 ports, while each 40GbE quad small form-factor pluggable plus (QSFP+) transceiver ports can be broken into four 10GbE small form-factor pluggable plus (SFP+) transceiver ports, increasing the total number of supported 25GbE and 10GbE ports per switch to 80.

QFX5120-48YM

The QFX5120-48YM is a 10GbE/25GbE/100GbE data center leaf and campus distribution switch featuring:

— 48 25GbE (SFP28)/10GbE (SFP+)/1GbE (SFP) downlink ports

— Eight 100GbE (QSFP28)/40GbE (QSFP+) uplink ports

— Up to 2/4 Tbps (uni/bidirectional) of L2 and L3 performance, with latency as low as 800 nanoseconds

— Media Access Control Security (MACsec) AES-256 support across all ports

— A 2.9 GHz quad-core Intel CPU with 16 GB memory and 100 GB SSD storage

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3070

When using breakout cables, two of the 100GbE QSFP28 ports (ports 50 and 52) can be broken into four 25GbE SFP28 or four 10GbE SFP+ ports, increasing the maximum number of 10GbE/ 25GbE ports supported to 56. When using breakouts, the total number of all ports on the switch, including 6x100GbE ports and 56x10/25GbE, is 62.

QFX5120-48T

The QFX5120-48T is a 10GbE/100GbE data center leaf and campus distribution switch featuring:

— 48 dual-speed 1GbE/10GbE RJ-45 copper downlink ports

— Six dual-speed 100GbE (QSFP28)/40GbE (QSFP+) uplink ports

— Up to 1.08/2.16 Tbps (uni/bidirectional) of L2 and L3 performance, with latency as low as 800 nanoseconds

— A 2.2 GHz quad-core Intel CPU with 16 GB memory and 100 GB SSD storage

Using breakout cables, 40GbE QSFP+ ports 50 and 51 can be channelized into four 10GbE SFP+ ports each, increasing the total number of 10GbE ports per switch to 56.

QFX5120-32C

The QFX5120-32C is a compact 100GbE data center leaf-and- spine and campus distribution switch featuring:

— 32 100GbE (QSFP28) or 40GbE (QSFP+) uplink ports

— A 2.2 GHz quad-core Intel CPU with 16 GB memory and 64 GB SSD storage

— Up to 3.2/6.4 Tbps (uni/bidirectional) L2 and L3 performance, with latency as low as 800 nanoseconds

Using breakout cables, 100GbE QSFP28 ports 0-30 can be channelized into four 25GbE SFP28 ports*, and the 40GbE QSFP+ ports 0-30 can be channelized into four 10GbE SFP+ ports, increasing the total number of 25GbE per switch to 124 and the total number of 10GbE ports per switch to 126 (including SFP+ ports 32 and 33). Port 31 does not support 4x10G or 4x25G channelization options. Only 100GbE, 40GbE, and 2x50GbE channelization options are supported on port 31.

In addition, all QFX5120 switch models include:

— Support for VXLAN as an L2 or L3 gateway

— Advanced Junos OS features such as Ethernet VPN-Virtual Extensible LAN (EVPN-VXLAN), BGP add-path, L3 VPN, and MPLS

— Feature-rich automation capabilities with support for Python and zero-touch provisioning (ZTP)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3071

Junos OS

The high performance QFX5120 Switch runs Junos OS, HPE Juniper Networking's powerful and robust network operating system that powers all HPE Juniper Networking switches, routers, and firewalls. Key Junos OS features that enhance the functionality and capabilities of the QFX5120 include:

— Software modularity, with process modules running independently in their own protected memory space and with the ability to do process restarts

— Uninterrupted routing and forwarding, with features such as nonstop active routing (NSR) and nonstop bridging (NSB)

— Commit and rollback functionality that ensures error-free network configurations

— A powerful set of scripts for on-box problem detection, reporting, and resolution

Data center deployments

Data centers demand high-speed, low-latency, storage- and I/O-converged networking solutions that maximize performance for physical servers, virtual servers, and storage. The QFX5120 Switch addresses these issues with low-latency, lossless, high-density 10GbE, 25GbE, and 100GbE interfaces on a compact 1 U platform. In addition, the QFX5120 offers EVPN-VXLAN L2 and L3 gateway support, making it an ideal solution for either edge routed or centrally routed overlay deployments in the data center. The QFX5120 also supports flexible back-to-front and front-to-back airflow cooling options, ensuring consistency with server designs for hot-aisle or cold-aisle deployments.

Data center server access

The QFX5120-48Y and QFX5120-48YM support tri-speed 1GbE/10GbE/25GbE, making them a perfect fit for top-of-rack deployments. The 48 ports of native 10GbE/25GbE for server connectivity, plus up to eight 40GbE or 100GbE ports for uplink connectivity, provide very low oversubscription of 1.5:1 from access to aggregation.

The QFX5120-48T supports dual-speed 1GbE/10GbE, also making it a perfect fit for top-of-rack deployments. The 48 native 10GbE RJ-45 copper ports for server connectivity, plus up to six 40GbE or 100GbE ports for uplink connectivity, provide an unsubscribed (0.8:1) access-to-aggregation ratio.

The QFX5120-32C can also be used for high-density 25GbE server connectivity, with an option to break out the 100GbE ports into four 25GbE ports.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3072

In Figure 1, the QFX5120 is deployed as a leaf acting as an edge-routed gateway. In this topology, the VXLAN tunnel encapsulation and decapsulation take place on the QFX5120 leaf switches, while Juniper Networks QFX5200-32C or Juniper Networks QFX5210-64C spine switches are used for IP transit. Juniper Networks QFX5110-32Q switches can also be used in the spine to build a 40GbE fabric.

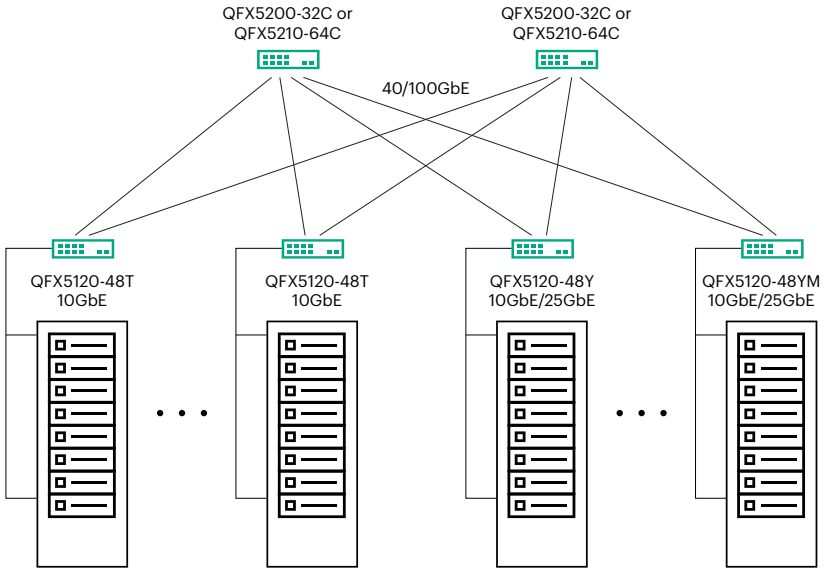


Figure 1: Edge-routed bridging at the leaf with QFX5120 as leaf switches and QFX5200-32C/QFX5210-64C as spine switches

In Figure 2, the QFX5120-48YM leaf and Juniper Networks QFX10008 Switch spine are deployed as EVPN-VXLAN switches acting as centrally routed gateways or distributed edge-routed gateways. If centrally routed bridging is used, the VXLAN tunnel encapsulation and decapsulation occur on the spine switches for inter-IRB (integrated routing and bridging) symmetric routing purposes. If edge-routed bridging is used, the IP first hop gateways are distributed at the leaf-level QFX5120-48YM switches using Type 5 symmetric inter-IRB routing. When using a QFX10000-30C-M MACsec line card installed in a spine QFX10008 Switch working with a leaf QFX5120-48YM switch, the leaf-to-spine architecture offers end-to-end MACsec AES-256 capabilities.

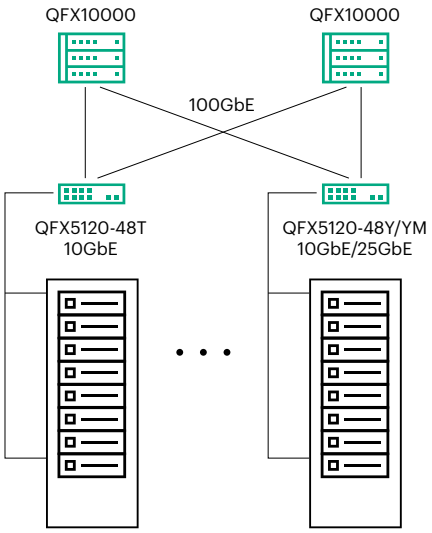


Figure 2: QFX5120-48T and QFX5120-48Y/48YM as leaf and QFX10000 as spine switches

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3073

Data center spine

The QFX5120-32C, with 32 ports of 100GbE, can serve as the spine in small to medium-sized enterprise data centers. The QFX5120-32C can be deployed in a three-stage IP Clos with EVPN-VXLAN overlay to support as many as 1500 server access ports. The QFX5120-48Y/QFX5120-48YM and QFX5120-32C can also be used as a collapsed spine data center deployment, offering Ethernet segment identifier-link aggregation group (ESI-LAG) connectivity to the rest of the network infrastructure blocks.

All QFX5120 switches can operate in both cut-through and store- and forward modes, delivering sustained wire-speed switching with sub-microsecond latency and low jitter for any packet size (including jumbo frames) in either mode. With features such as multichassis link aggregation (MC-LAG), the QFX5120 supports active/active server dual-homing and can use full bisectional bandwidth from server to switch.

Equipped with Junos OS, the QFX5120 supports the most advanced and robust routing capabilities in the industry, OSPF for both IPv4 and IPv6, as well as advanced routing capabilities such as IS-IS and BGP. With additional capabilities such as 64-way equal-cost multipath (ECMP) and BGP add path, the QFX5120 is an ideal building block for deploying the most robust L3 underlay for SDN.

Campus deployments

HPE Juniper Networking campus fabrics provide a single, standards-based Ethernet VPN-Virtual Extensible LAN (EVPN-VXLAN) solution that can be deployed in any campus, whether a two-tier network with a collapsed core distribution or a campus-wide system that involves multiple buildings with separate distribution and core layers.

The QFX5120-48Y and QFX5120-48YM are ideal as campus distribution switches with 10GbE/25GbE downlinks and 40GbE/ 100GbE uplinks supporting technologies like MC-LAG and EVPN multihoming.

The QFX5120-32C is ideal as a campus core switch with 32 ports of 100GbE and support for technologies like campus fabric core-distribution.

The QFX5120-48T supports dual-speed 1GbE/10GbE, also making it a perfect fit for top-of-rack deployments in campus environments for server connectivity.

HPE Juniper Networking campus fabrics support the following validated architectures:

— **MC-LAG and EVPN Multihoming (Collapsed Core/ Distribution)**: A pair of interconnected QFX5120 switches can be deployed to provide EVPN multihoming (ESI-LAG) or multichassis link aggregation (MC-LAG) in a collapsed core/ distribution configuration. This eliminates the need for Spanning Tree Protocol (STP) across the campus network by providing multihoming capabilities from the access to the distribution layer, while distribution to the core is an L3 IP fabric. ESI-LAG also supports horizontal scaling with more than two devices in the distribution layer and can extend EVPN to the core.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3074

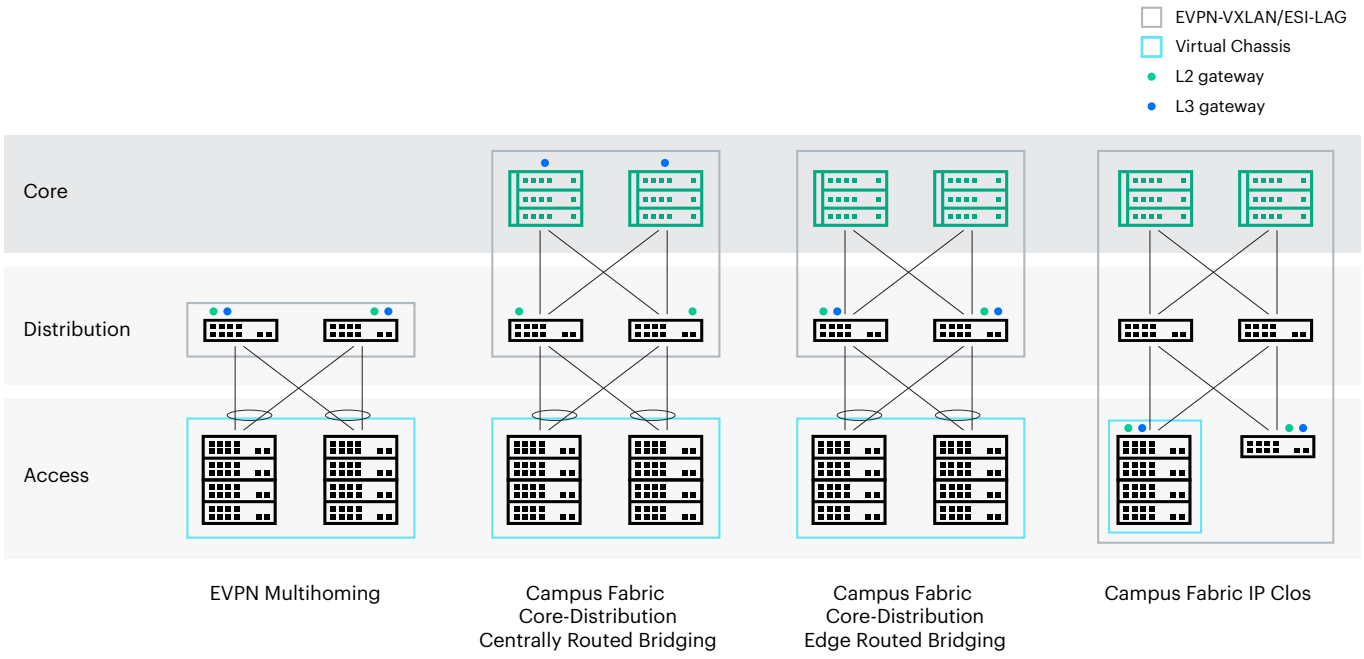


Figure 3: QFX5120 as distribution and core in EVPN multihoming and campus fabric architectures

— **Campus fabric core-distribution**: A pair of interconnected QFX5120 switches can provide EVPN L2 and L3 VXLAN gateway support. This eliminates the need for STP across the campus network by providing a multihoming capability from the access to the distribution layer, while distribution to the core is an L3 IP fabric using EVPN technology. The IP fabric can also extend to connect multiple enterprise buildings, while VXLAN allows stretching of L2 across buildings. An IP Clos network between the distribution and the core layers can exist in two modes, both of which are supported by the QFX5120:

- **Centrally routed bridging overlay**: An IRB interface placed at a central location in the fabric (in this case, a core device)
- **Edge routed bridging overlay**: An IRB interface placed at the edge of the fabric (in this case, a distribution device)

— **Campus fabric IP Clos**: The Campus Fabric IP Clos architecture pushes VXLAN Layer 2/3 gateway functionality to the access layer. In this architecture, the QFX5120 switch acts as an IP fabric distribution switch.

Features and benefits

— **Automation**: The QFX5120 supports a number of network automation and plug-and-play operational features, including ZTP and event scripts, automatic rollback, and Python scripting.

— **Flexible forwarding table**: The QFX5120 includes a unified forwarding table, which allows the hardware table to be carved into configurable partitions of L2 media access control (MAC), L3 host, and longest prefix match (LPM) tables. In a pure L2 environment, the QFX5120 supports 291,000 MAC addresses. In L3 mode, the QFX5120 table can support 211,000 host entries. In LPM mode, it can support 351,000 prefixes. Junos OS provides configurable options through a CLI that can optimize the QFX5120 for various deployment scenarios.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3075

— **Intelligent buffer management**: The QFX5120 features a total of 32 MB of shared buffers. While 25% of the total buffer space is dedicated, the rest is shared among all ports and is user configurable. The intelligent buffer mechanism in the QFX5120 effectively absorbs traffic bursts while providing deterministic performance, significantly increasing performance over static allocation.

— **MPLS**: A broad set of MPLS features, including L3 VPN, IPv6 provider edge router (6PE), RSVP traffic engineering, and LDP, allow standards-based network segmentation and virtualization, enabling the QFX5120 to be deployed as a low latency MPLS label-switching router (LSR).

— **VXLAN overlays**: The QFX5120 switch is capable of both L2 and L3 gateway services. Customers can deploy overlay networks to provide L2 adjacencies for applications over L3 fabrics. The overlay networks use VXLAN in the data plane and EVPN or Open vSwitch Database (OVSDB) for programming the overlays.

— **MACsec and hop-by-hop encryption**: The QFX5120-48YM supports IEEE 802.1AE MACsec AES-256, providing link-layer data confidentiality, data integrity, and data origin authentication. The MACsec feature enables the QFX5120-48YM to support 2/4 Tbps (uni/bidirectional) of hardware-based traffic encryption on all 100GbE, 40GbE, 25GbE, 10GbE, and 1GbE ports. Defined by IEEE 802.1AE, MACsec provides secure, encrypted communication at the link layer that is capable of identifying and preventing threats from denial-of-service (DoS) and intrusion attacks, as well as man-in-the-middle, masquerading, passive wiretapping, and playback attacks launched from behind the firewall. When MACsec is deployed on switch ports, all traffic is encrypted on the wire, but traffic inside the switch is not. This allows the switch to apply network capabilities such as quality of service (QoS) and sFlow® to each packet without compromising the security of packets on the wire.

In addition, Ethernet-based WAN networks can use MACsec to provide link security over long haul connections. MACsec is transparent to Layer 3 and higher layer protocols and is not limited to IP traffic; it works with any type of wired or wireless traffic carried over Ethernet links.

— **Virtual chassis**: The QFX5120 supports HPE Juniper Networking's unique virtual chassis technology, which enables interconnected switches to operate as a single, logical device with a single IP address. This technology allows campus enterprises to eliminate STP and efficiently utilize network links. QFX5120-48Y (starting with Junos 19.3), QFX5120-32C (staring with Junos 20.3), QFX5120-48T (starting with Junos 20.2), and QFX5120-48YM (starting with Junos 23.1) support virtual chassis feature.

QFX5120-48T, QFX5120-48Y, and QFX5120-32C switch models support HiGig protocol for forming a virtual chassis. However, the QFX5120-48YM switch model supports only HGoE protocol for virtual chassis formation.

Management, monitoring, and analytics

Data center fabric management: Apstra Data Center Director (formerly Juniper Apstra) provides operators with the power of intent-based network design to help ensure changes required to enable data center services can be delivered rapidly, accurately, and consistently. Operators can further benefit from the built-in assurance and analytics capabilities to resolve day 2 operations issues quickly.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3076

Data Center Director Key Features

— Automated deployment and zero-touch deployment

— Continuous fabric validation

— Fabric lifecycle management

— Troubleshooting using advanced telemetry

For more information, see Apstra Data Center Director

Campus fabric management: Campus and branch cloud

Juniper Wired Assurance brings cloud management and Marvis AI to campus fabrics. It sets a new standard moving away from traditional network management towards AI operations, while delivering better experiences to connected devices.

— Automated deployment and Zero Touch Deployment

— Anomaly detection

— Root cause analysis

For more information on Wired Assurance, see juniper.net/us/en/products/cloud-services/wiredassurance.html

Paragon Insights (formerly HealthBot)

Combining the power of telemetry, programmability, advanced algorithms, and machine learning, Juniper Paragon Insights (formerly HealthBot) delivers the following features and benefits for enhanced monitoring and analytics:

— Key performance indicator collection and visualization

— Anomaly detection

— Root cause analysis

— Automated remediation

— Multivendor support

— Customizable playbooks

— JTI telemetry

For more information on Paragon Insights, see juniper.net/content/dam/www/assets/datasheets/us/en/network-automation/paragon-insights-datasheetpdf.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3077

Junos telemetry interface

The QFX5120 switch supports Junos telemetry interface (JTI), a modern telemetry streaming tool designed for performance monitoring in complex, dynamic data centers. Streaming data to a performance management system enables network administrators to measure trends in link and node utilization and troubleshoot such issues as network congestion in real time. JTI delivers the following features:

— Application visibility and performance management by provisioning sensors to collect and stream data and analyze application and workload flow paths through the network

— Capacity planning and optimization by proactively detecting hotspots and monitoring latency and microbursts

— Troubleshooting and root cause analysis via high-frequency monitoring and correlation of overlay and underlay networks

QFX5120 switch specifications

Hardware

Switching capacity

— QFX5120-48Y: 2/4 Tbps (uni/bidirectional)/2 Bpps

— QFX5120-48YM: 2/4 Tbps (uni/bidirectional)/2 Bpps

— QFX5120-48T: 1.08/2.16 Tbps (uni/bidirectional)/1 Bpps

— QFX5120-32C: 3.2/6.4 Tbps (uni/bidirectional)/2 Bpps

— Switching mode (all models): Cut-through and store-and-forward

— Switch chip (all models): Broadcom Trident3

Weight

— QFX5120-48Y: 23.7 lb (10.75 kg)

— QFX5120-48YM: 23.37 lb (10.60 kg)

— QFX5120-48T: 24.25 lb (11 kg)

— QFX5120-32C: 21.12 lb (9.58 kg)

Dimensions (H x W x D)

— QFX5120-48Y: 1.72 x 17.36 x 20.48 in. (4.37 x 44.09 x 52.02 cm)

— QFX5120-48YM: 1.72 x 17.36 x 20.48 in. (4.37 x 44.09 x 52.02 cm)

— QFX5120-48T: 1.72 x 17.36 x 20.48 in. (4.37 x 44.09 x 52.02 cm)

— QFX5120-32C: 1.7 x 17.26 x 20.27 in. (4.32 x 43.84 x 51.5 cm)

Power consumption

— QFX5120-48Y

  • Max power draw*: 283W

  • Typical power draw**: 155W

— QFX5120-48YM

  • Max power draw*: 446W, 460W with MACsec

  • Typical power draw**: 280W, 291W with MACsec

— QFX5120-48T

  • Max power draw*: 251W

  • Typical power draw**: 202W

— QFX5120-32C

  • Max power draw**: 365W

  • Typical power draw**: 173W

* Max power consumption measured at 40°C ambient temperature with SR optics at 100% load with IMIX traffic.

** Typical power consumption is measured at 25°C ambient temperature with DACs at 50% load with IMIX traffic, excluding transceivers.

Power consumption is subject to operating conditions and unit-to-unit variations.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3078

Airflow

— Front-to-back (airflow out) for hot aisle deployment

— Back-to-front (airflow in) for cold aisle deployment

Interface options

— QFX5120-48Y

- 2 management ports: 2 x RJ-45 ports
- 1GbE SFP: 48
- 10GbE SFP+: 48/80 (with breakout cable)
- 25GbE SFP: 48/80 (with breakout cable)
- 40GbE QSFP+: 8 (each QSFP+ port can be configured as a 4 x 10GbE interface or as a 40 Gbps port)
- 100GbE QSFP28: 8 (each QSFP28 port can be configured as a 4 x 25GbE interface or as a 100 Gbps port)
- SFP GbE optical and copper module
- SFP+ 10GbE optical modules
- SFP+ direct attach copper (DAC) cables: 1/3/5 m twinax copper and 1/3/5/7 m active twinax copper
- SFP28 DAC cables: 1/3 m twinax copper
- SFP28 optics: Short reach (SR), long reach (LR)
- QSFP+ to SFP+: 10GbE direct attach breakout copper (1/3 m twinax copper cable)

— QFX5120-48YM

- 2 management ports: 2 x RJ-45 ports
- 1GbE SFP: 48
- 10GbE SFP+: 48/56 (total of 56 ports with breakout cable on port 50 and 52)
- 25GbE SFP: 48/56 (total of 56 ports with breakout cable on port 50 and 52)
- 40GbE QSFP+: 8 (QSFP+ port 50 and 52 can be configured as a 4 x 10GbE interface or as a 40 Gbps port)
- 100GbE QSFP28: 8 (QSFP28 port 50 and 52 can be configured as a 4 x 25GbE interface or as a 100 Gbps port)
- SFP GbE optical
- SFP+ 10GbE optical modules
- SFP+ DAC cables: 1/3/5 m twinax copper and 1/3/5/7 m active twinax copper
- SFP28 DAC cables: 1/3 m twinax copper
- SFP28 optics: Short reach (SR), long reach (LR)
- QSFP+ to SFP+: 10GbE direct attach breakout copper (1/3 m twinax copper cable)

— QFX5120-48T

- 1 management port: 1 x RJ-45 port
- 1GbE RJ45 (copper): 48 (each port is dual speed supporting 1GbE/10GbE)
- 40GbE QSFP+: 6 (ports 50 and 51 can be configured as a 4 x 10GbE interface or as 40 Gbps interfaces)
- 100GbE QSFP28: 6 (ports 50 and 51 can be configured as a 4 x 25GbE interface or as 100 Gbps interfaces)

— QFX5120-32C

- 1 RJ-45 in-band management port
- 10GbE SFP+: 2 native ports plus 124 (with 4 x 10GbE breakout cable)
- 25GbE SFP: 124 (with breakout cable)
- 40GbE QSFP+: 32 (ports 0-31 can be configured as a 4 x 10GbE interface)
- 100GbE QSFP28: 32 (ports 0-31 can be configured as a 4 x 25GbE interface)
- SFP+ 10GbE optical modules
- SFP+ DAC cables: 1/3/5 m twinax copper and 1/3/5/7 m active twinax copper
- SFP28 DAC cables: 1/3 m twinax copper
- SFP28 optics: SR, LR
- QSFP+ to SFP+: 10GbE direct attach breakout copper (1/3 m twinax copper cable)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3079

Common to all models

— 1 USB 2.0 port

— 1 RS-232 console port

— Supported transceiver and direct attach cable

  • QSFP+ DAC cables: 1/3 m twinax copper

  • QSFP+ optics: SR4, LX4, ESR4, ER4, LR4

  • QSFP28 optics: SR4, ER4, PSM4, CWDM4, LR4

— Versatile four post mounting options for 19-in server rack or datacom rack

Airflow

— Redundant (N+1) and hot-pluggable fan modules for front-to- back and back-to-front airflow

— Redundant variable-speed fans to reduce power draw

Power supply and fan modules

— Dual redundant (1+1) and hot-pluggable 650W AC/DC power supplies

— 100-240V single phase AC power

— -48 to -60V DC power supply

— Redundant 4+1 (QFX5120-48Y/YM and QFX5120-48T) or 5+1 (QFX5120-32C) and hot-pluggable fan modules for front- to-back or back-to-front airflow

Performance scale (Unidimensional)

— MAC addresses per system: 288,000

— VLAN IDs: 4094

— Number of link aggregation groups (LAGs):

  • 80 (QFX5120-48Y/YM, QFX5120-32C)

  • 64 (QFX5120-48T)

— Number of ports per LAG: 64

— IPv4 unicast routes: 2,000,000 prefixes (RIB); 351,000 prefixes (FIB); 211,000 host routes; 64 ECMP paths

— IPv4 multicast routes: 106,000

— IPv6 unicast routes: 500,000 prefixes (RIB); 172,000 prefixes (FIB); 106,000 host routes

— IPv6 multicast routes: 52,000

— Address Resolution Protocol (ARP) entries: 64,000

— Jumbo frame: 9216 bytes

— Spanning Tree Protocol (STP)

— Multiple Spanning Tree Protocol (MSTP) instances: 64

— VLAN Spanning Tree Protocol (VSTP) instances: 509

— Traffic mirroring

  • Mirroring destination ports per switch: 4

  • Maximum number of mirroring sessions: 4

  • Mirroring destination VLANs per switch: 4

— 100,000 L2 IGMP snooping*

— Virtual Routing and Forwarding (VRF) instances : 2000

*Scale number may vary depending on the test scenarios and other factors.

Software features supported

Layer 2 features

— STP — IEEE 802.1D (802.1D-2004)

— Rapid Spanning Tree Protocol (RSTP) (IEEE 802.1w); MSTP (IEEE 802.1s)

— Bridge protocol data unit (BPDU) protect

— Loop protect

— Root protect

— RSTP and VSTP running concurrently

— VLAN — IEEE 802.1Q VLAN trunking

— Routed VLAN interface (RVI)

— Port-based VLAN

— Private VLAN (PVLAN)

— VLAN translation

— Static MAC address assignment for interface

— Per VLAN MAC learning (limit)

— MAC learning disable

— Link Aggregation and Link Aggregation Control Protocol (LACP) (IEEE 802.3ad)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3080

— MACsec with AES256 (QFX5120-48YM only)

— Virtual chassis — up to 2 members on QFX5120-48Y, QFX5120-32C and QFX5120-48T, and up to 4 members on QFX5120-48YM

Link aggregation

— MC-LAG

— LAG load sharing algorithm — bridged or routed (unicast or multicast) traffic

— IP: Session Initiation Protocol (SIP), Dynamic Internet Protocol (DIP), TCP/UDP source port, TCP/UDP destination port

— Layer 2 and non-IP: MAC SA, MAC DA, Ethertype, VLAN ID, source port

Layer 3 features (IPv4)

— Static routing

— Routing protocols (RIP, OSPF, IS-IS, BGP)

— Virtual Router Redundancy Protocol (VRRP)

— Virtual router

— Dynamic Host Configuration Protocol (DHCP) relay

— Proxy Address Resolution Protocol (ARP)

EVPN-VXLAN features

— MAC virtual routing and forwarding (MAC-VRF) multiple EVPN instances (EVI) with service-types VLAN-based, VLAN-aware, VLAN-bundle

— Symmetric inter-IRB routing with anycast gateway and EVPN type-5 instances

— Proxy IGMPv2 — EVPN route types 6/7/8

— ARP/ND proxy/suppression

— ESI-LAG A/A multihoming using Enterprise and SP-style interfaces

— Enhanced Ethernet loop detection

— Filter-based forwarding on IRB.VGA

— EVPN advanced route policing

— VLAN-id overlapping using SP-style interfaces

— VLAN rewrite support in EVPN-VXLAN enterprise-style

— (EP-style) interfaces — VLAN-id overlap in EP-style interfaces

— OISM — draft-ietf-bess-evpn-irb-mcast

— VLAN rewrite support in EVPN-VXLAN enterprise-style

Multicast features

— Internet Group Management Protocol (IGMP): v1, v2, v3

— IGMP snooping: v1, v2, and v3 (Layer 2 only)

— IGMP filter

— Protocol Independent Multicast-Sparse Mode (PIM-SM), PIM- Source-Specific Multicast (PIM-SSM), PIM-Dense Mode (PIM- DM) in pure IP fabric use case

— Multicast Source Discovery Protocol (MSDP)

Security and filters

— Secure interface login and password

— RADIUS

— TACACS+

— Ingress and egress filters: Allow and deny, port filters, VLAN filters, and routed filters, including management port filters

— Filter actions: Logging, system logging, reject, mirror to an interface, counters, assign forwarding class, permit, drop, police, mark

— SSH v1, v2

— Static ARP support in pure IP fabric

— Storm control, port error disable, and auto-recovery

— Source MAC address filtering on the port

— DHCP snooping in pure IP fabric use case

Quality of service (QoS)

— L2 and L3 QoS: Classification, rewrite, queuing

— Rate limiting:

  • Ingress policing: Single-rate two-color policer, two-rate three-color policer

  • Egress policing: Policer, policer mark down action

  • Egress shaping: Per queue on each port

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3081

— 10 hardware queues per port (8 unicast and 2 multicast)

— Strict-priority queue (SPQ), shaped-deficit weighted round- robin (SDWRR), weighted random early detection (WRED), weighted tail drop

— 802.1p remarking

— Layer 2 classification criteria: Interface, MAC address, Ethertype, 802.1p, VLAN

— Congestion avoidance capabilities: WRED

— Trust IEEE 802.1p (ingress)

— Remarking of bridged packets

— Default inner to outer DiffServ code point (DSCP) copy for EVPN-VXLAN

IP storage

— Priority-based flow control (PFC) — IEEE 802.1Qbb, DCBX

— PFC using DSCP and explicit congestion notification (ECN) for ROCEv2

High availability

— Bidirectional Forwarding Detection (BFD)

— Uplink failure detection

MPLS

— Static label-switched paths (LSPs)

— RSVP-based signaling of LSPs

— LDP-based signaling of LSPs

— LDP tunneling (LDP over RSVP)

— MPLS class of service (CoS)

— MPLS LSR support

— IPv6 tunneling (6PE) (via IPv4 MPLS backbone)

— IPv4 L3 VPN (RFC 2547, RFC 4364)

Management and analytics platforms

— Apstra Data Center Director

— Juniper Wired Assurance for Campus

— Junos Space Network Director for Campus

— Paragon Insights

Device management and operations

— Role-based CLI management and access

— CLI via console, telnet, or SSH

— Extended ping and traceroute

— Junos OS configuration rescue and rollback

— Image rollback

— SNMP v1/v2/v3

— Junos XML management protocol

— sFlow v5

— IPFIX

— Beacon LED for port and system

— Inband Flow Analyzer (IFA)

— ZTP

— OpenStack Neutron Plug-in

— Python

— Junos OS event, commit, and OP scripts

— JTI

Traffic mirroring

— Port-based

— LAG port

— VLAN-based

— Filter-based

— Mirror to local

— Mirror to remote destinations (L2 over VLAN)

Standards compliance IEEE standard

IEEE 802.1D

— IEEE 802.1w

— IEEE 802.1

— IEEE 802.1Q

— IEEE 802.1p

— IEEE 802.1ad

— IEEE 802.3ad

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3082

— IEEE 802.1AB

— IEEE 802.3x

— IEEE 802.1Qbb

— IEEE 802.1Qaz

T11 standards

— INCITS T11 FC-BB-5

Supported RFCs

— RFC 768 UDP

— RFC 1350 Trivial File Transfer Protocol (TFTP) Revision 2

— RFC 791 IP

— RFC 792 ICMP

— RFC 793 TCP

— RFC 826 ARP

— RFC 854 Telnet client and server

— RFC 894 IP over Ethernet

— RFC 903 RARP

— RFC 906 TFTP Bootstrap

— RFC 951 1542 BOOTP

— RFC 1058 Routing Information Protocol

— RFC 1112 IGMP v1

— RFC 1122 Host requirements

— RFC 1142 OSI IS-IS Intra-domain Routing Protocol

— RFC 1256 IPv4 ICMP Router Discovery Protocol (IRDP)

— RFC 1492 TACACS+

— RFC 1519 Classless Interdomain Routing (CIDR)

— RFC 1587 OSPF not-so-stubby area (NSSA) Option

— RFC 1591 Domain Name System (DNS)

— RFC 1745 BGP4/IDRP for IP — OSPF Interaction

— RFC 1772 Application of the Border Gateway Protocol in the Internet

— RFC 1812 Requirements for IP Version 4 Routers

— RFC 1997 BGP Communities Attribute

— RFC 7348 VXLAN — Virtual extensible Local Area Network

— RFC 8365 NVO — Network Virtualization Overlay Solution Using Ethernet VPN (EVPN-VXLAN)

— OISM - EVPN Optimized Inter-Subnet Multicast (OISM) Forwarding - draft-ietf-bess-evpn-irb-mcast

— IGMP and MLD Proxy for EVPN - draft-ietf-bess-evpn-igmp- mld-proxy

— RFC 2030 SNTP, Simple Network Time Protocol

— RFC 2068 HTTP server

— RFC 2131 BOOTP/DHCP relay agent and Dynamic Host

— RFC 2138 RADIUS Authentication

— RFC 2139 RADIUS Accounting

— RFC 2154 OSPF with Digital Signatures (Password, MD-5)

— RFC 2236 IGMP v2

— RFC 2267 Network ingress filtering

— RFC 2328 OSPF v2 (edge mode)

— RFC 2338 VRRP

— RFC 2362 PIM-SM (edge mode)

— RFC 2370 OSPF Opaque LSA Option

— RFC 2385 Protection of BGP Sessions via the TCP MD5 Signature Option

— RFC 2439 BGP Route Flap Damping

— RFC 2453 RIP v2

— RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers

— RFC 2597 Assured Forwarding PHB (per-hop behavior) Group

— RFC 2598 An Expedited Forwarding PHB

— RFC 2697 A Single Rate Three Color Marker

— RFC 2698 A Two Rate Three Color Marker

— RFC 2796 BGP Route Reflection — An Alternative to Full Mesh IBGP

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3083

— RFC 2918 Route Refresh Capability for BGP-4

— RFC 3065 Autonomous System Confederations for BGP

— RFC 3376 IGMP v3 (source-specific multicast include mode only)

— RFC 3392 Capabilities Advertisement with BGP-4

— RFC 3446 Anycast RP

— RFC 3569 SSM

— RFC 3618 MSDP

— RFC 3623 Graceful OSPF Restart

— RFC 4271 Border Gateway Protocol 4 (BGP-4)

— RFC 4360 BGP Extended Communities Attribute

— RFC 4456 BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)

— RFC 4486 Subcodes for BGP Cease Notification Message

— RFC 4724 Graceful Restart Mechanism for BGP

— RFC 5549 - Advertising IPv4 Network Layer Reachability Information with an IPv6 Next Hop

— RFC 4812 OSPF Restart Signaling

— RFC 4893 BGP Support for Four-octet AS Number Space

— RFC 5176 Dynamic Authorization Extensions to RADIUS

— RFC 5396 Textual Representation of Autonomous System (AS) Numbers

— RFC 5668 4-Octet AS Specific BGP Extended Community

— RFC 5880 Bidirectional Forwarding Detection (BFD) Dynamic Host Configuration Protocol (DHCP) server

Supported MIBs

— RFC 1155 SMI

— RFC 1157 SNMPv1

— RFC 1212, RFC 1213, RFC 1215 MIB-II, Ethernet-Like MIB and TRAPs

— RFC 1850 OSPFv2 MIB

— RFC 1901 Introduction to Community-based SNMPv2

— RFC 2011 SNMPv2 for Internet Protocol using SMIv2

— RFC 2012 SNMPv2 for the Transmission Control Protocol using SMIv2

— RFC 2013 SNMPv2 for the User Datagram Protocol using SMIv2

— RFC 2233 The Interfaces Group MIB using SMIv2

— RFC 2287 System Application Packages MIB

— RFC 2570 Introduction to Version 3 of the Internet-standard Network Management Framework

— RFC 2571 An Architecture for describing SNMP Management Frameworks (read-only access)

— RFC 2572 Message Processing and Dispatching for the SNMP (read-only access)

— RFC 2576 Coexistence between SNMP Version 1, Version 2, and Version 3

— RFC 2578 SNMP Structure of Management Information MIB

— RFC 2579 SNMP Textual Conventions for SMIv2

— RFC 2580 Conformance Statements for SMIv2

— RFC 2665 Ethernet-like Interface MIB

— RFC 2787 VRRP MIB

— RFC 2790 Host Resources MIB

— RFC 2819 RMON MIB

— RFC 2863 Interface Group MIB

— RFC 2932 IPv4 Multicast MIB

— RFC 3410 Introduction and Applicability Statements for Internet Standard Management Framework

— RFC 3411 An Architecture for Describing SNMP Management Frameworks

— RFC 3412 Message Processing and Dispatching for the SNMP

— RFC 3413 Simple Network Management Protocol (SNMP) Applications (all MIBs are supported except the Proxy MIB)

— RFC 3414 User-based Security Model (USM) for version 3 of SNMPv3

— RFC 3415 View-based Access Control Model (VACM) for the SNMP

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3084

— RFC 3416 Version 2 of the Protocol Operations for the SNMP

— RFC 3417 Transport Mappings for the SNMP

— RFC 3418 Management Information Base (MIB) for the SNMP

— RFC 3584 Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework

— RFC 3826 The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model

— RFC 4188 Definitions of Managed Objects for Bridges

— RFC 4318 Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol

— RFC 4363b Q-Bridge VLAN MIB

Approvals

Safety

— CAN/CSA-C22.2 No. 62368-1-14 Information Technology Equipment — Safety

— UL 62368-1 Information Technology Equipment — Safety

— EN 62368-1: 2014 Information Technology Equipment — Safety

— IEC 62368-1: 2014 2nd Edition Information Technology Equipment — Safety (All country deviations): CB Scheme

— IEC 60950-1:2005/A2:2013 Information Technology Equipment — Safety (All country deviations): CB Scheme

EMC

— EN 300 386 V1.6.1 (2012-09) Electromagnetic compatibility and radio spectrum matters (ERM) Telecommunication network equipment

— EN 300 386 V2.1.1 (2016-07) Telecommunication network equipment; EMC requirements; Harmonized Standard covering the essential requirements of the Directive 2014/30/EU

— EN 55032:2012 (CISPR 32:2012) Electromagnetic compatibility of multimedia equipment — Emission requirements

— EN 55024:2010 (CISPR 24:2010) Information technology equipment — immunity characteristics — limits and methods of measurement

— IEC/EN 61000 Immunity Test

— AS/NZS CISPR 32:2015 Australia/New Zealand Radiated and Conducted Emissions

— FCC 47 CFR Part 15 USA Radiated and Conducted Emissions

— ICES-003 Canada Radiated and Conducted Emissions

— VCCI-CISPR 32:2016 Japanese Radiated and Conducted Emissions

— BSMI CNS 13438 Taiwan Radiated and Conducted Emissions (at 10 meters)

— KN32/KN35 Korea Radiated Emission and Immunity Characteristics (at 10 meters)

— KN61000 Korea Immunity Test

— TEC/SD/DD/EMC-221/05/OCT-16 India EMC standard

Environmental compliance

Restriction of Hazardous Substances (ROHS) 6/6

80 Plus Silver PSU Efficiency

Recycled material

Waste Electronics and Electrical Equipment (WEEE)

Registration, Evaluation, Authorization and Restriction of Chemicals (REACH)

China Restriction of Hazardous Substances (ROHS)

Telco

— Common Language Equipment Identifier (CLEI) code

Environmental ranges

— Operating temperature: 32° to 104°F (0° to 40°C)

— Storage temperature: -40° to 158°F (-40° to 70°C)

— Operating altitude: Up to 6000 ft (1829 m)

— Relative humidity operating: 5% to 90% (noncondensing)

— Relative humidity nonoperating: 0% to 95% (noncondensing)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3085

Installation and implementation service

Juniper Professional Services offers a Data Center Switching QuickStart program to ensure that the solution is operational and that you have a complete understanding of areas such as configuration and ongoing operations. The QuickStart service provides an on-site consultant who works with your team to quickly develop the initial configuration and deployment of a small HPE Juniper Networking data center switching environment. A knowledge transfer session, which is intended as a review of local implementation and configuration options, is also included, but is not intended as a substitute for formalized training.

Ordering information

Product	Description
Switch hardware	
QFX5120-48Y-AFI2	QFX5120-48Y, 48x25GbE+8x100GbE, 1 U, AC airflow in
QFX5120-48Y-AFO2	QFX5120-48Y, 48x25GbE+8x100GbE, 1 U, AC airflow out
QFX5120-48Y-DC-AFI2I	QFX5120-48Y, 48x25GbE+8x100GbE, 1 U, DC airflow in
QFX5120-48Y-DC-AFO2	QFX5120-48Y, 48x25GbE+8x100GbE, 1 U, DC airflow out
QFX5120-48YM-AFI	48x25GbE+8x100GbE MACsec AES256 switch, AC, back-to- front air flow
QFX5120-48YM-AFO	48x25GbE+8x100GbE MACsec AES256 switch, AC, front-to- back air flow
QFX5120-48YM-DC-AI	48x25GbE+8x100GbE MACsec AES256 switch, DC, back-to- front air flow, DC power
QFX5120-48YM-DC-AO	48x25GbE+8x100GbE MACsec AES256 switch, AC, front-to- back air flow, DC power
QFX5120-48T-AFI	QFX5120-48T, 48x10GbE+6x100GbE, 1 U, AC airflow in
QFX5120-48T-AFO	QFX5120-48T, 48x10GbE+6x100GbE, 1 U, AC airflow out
QFX5120-48T-DC-AFI	QFX5120-48T, 48x10GbE+6x100GbE, 1 U, DC airflow in
QFX5120-48T-DC-AFO	QFX5120-48T, 48x10GbE+6x100GbE, 1 U, DC airflow out
QFX5120-32C-AFI	QFX5120-32C, 32x100GbE, 1 U, AC airflow in
QFX5120-32C-AFO	QFX5120-32C, 32x100GbE, 1 U, AC airflow out
QFX5120-32C-DC-AFI	QFX5120-32C, 32x100GbE, 1 U, DC airflow in
QFX5120-32C-DC-AFO	QFX5120-32C, 32x100GbE, 1 U, DC airflow out
QFX520048Y-APSU-AO	AC Power supply unit, front-to-back airflow for QFX5120-32C- AFO
QFX520048Y-APSU-AI	AC Power supply unit, back-to-front airflow for QFX5120-32C- AFI
QFX520048Y-DPSU-AO	DC Power supply unit, front-to-back airflow for QFX5120-32C- DC-AFO
QFX520048Y-DPSU-AI	DC Power supply unit, back-to-front airflow for QFX5120-32C- DC-AFI
JPSU-650W-AC-AO	AC Power supply unit, front-to-back airflow for QFX5120-48T- AFO and QFX5120-48Y-AFO2
JPSU-650W-AC-AI	AC Power supply unit, back-to-front airflow for QFX5120-48T- AFI and QFX5120-48Y-AFI2

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3086

Ordering Information (continued)

Product	Description
JPSU-650W-DC-AFO	DC Power supply unit, front-to-back airflow for QFX5120-48T- DC-AFO and QFX5120-48Y-DC-AFO2
JPSU-650W-DC-AFI	DC Power supply unit, back-to-front airflow for QFX5120-48T- DC-AFI and QFX5120-48Y-DC-AFI2
JPSU-850W-AC-AFO	AC Power supply unit, front-to-back airflow for QFX5120-48YM-AFO
JPSU-850W-AC-AFI	AC Power supply unit, back-to-front airflow for QFX5120-48YM-AFI
JPSU-850W-DC-AFO	DC Power supply unit, front-to-back airflow for QFX5120-48YM-DC-AO
JPSU-850W-DC-AFI	DC Power supply unit, back-to-front airflow for QFX5120-48YM-DC-AI
QFX520048Y-FAN-AO	front-to-back airflow fan model for QFX5120-32C models
QFX520048Y-FAN-AI	back-to-front airflow fan model for QFX5120-32C models
QFX5110-FANAFO	Front-to-back airflow fan model for QFX5120-48T, QFX5120-48Y, and QFX5120-48YM models
QFX5110-FANAFI	Back-to-front airflow fan model for QFX5120-48T, QFX5120-48Y, and QFX5120-48YM models
QFX512032C-RMK	4 post rack mount kit for QFX5120-32C models
QFX5K-2PST-RMK	2 post rack mount kit for QFX5120-32C models
QFX512032C-RMK-E	Toolless RMK for QFX5130-32C model (Default RMK)
EX-4PST-RMK	4 post rack mount kit for QFX5120-48T, QFX5120-48Y, and QFX5120-48YM models
EX-RMK	2 post rack mount kit for QFX5120-48T, QFX5120-48Y, and QFX5120-48YM models
JNP-4PST-RMK-1U-E	Toolless RMK for QFX5120-48T, QFX5120-48Y, and QFX5120-48YM models (Default RMK)
MACsec encryption licenses	
S-QFX5KC1-MACSEC-1	Class C1 QFX5000, MACsec AES 256 Encryption Sub Software, Term: 1 Yr
S-QFX5KC1-MACSEC-3	Class C1 QFX5000, MACsec AES 256 Encryption Sub Software, Term: 3 Yrs
S-QFX5KC1-MACSEC-5	Class C1 QFX5000, MACsec AES 256 Encryption Sub Software, Term: 5 Yrs
S-QFX5KC1-MACSEC-P	Class C1 QFX5000, MACsec AES 256 Encryption Software, Perpetual
Flex software licenses	
S-QFX5K-C1-A1-3	Flex Sub Software, Class 1 QFX5000 line, Adv 1, Term: 3 Yrs
S-QFX5K-C1-A1-5	Flex Sub Software, Class 1 QFX5000 line, Adv 1, Term: 5 Yrs
S-QFX5K-C1-A1-P	Flex Software, Class 1 QFX5000 line, Adv 1, Perpetual
S-QFX5K-C1-A2-3	Flex Sub Software, Class 1 QFX5000 line, Adv 2, Term: 3 Yrs
S-QFX5K-C1-A2-5	Flex Sub Software, Class 1 QFX5000 line, Adv 2, Term: 5 Yrs
S-QFX5K-C1-A2-P	Flex Software, Class 1 QFX5000 line, Adv 2, Perpetual
S-QFX5K-C1-P1-3	Flex Sub Software, Class 1 QFX5000 line, Prem 1, Term: 3 Yrs

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3087

Ordering information (continued)

Product	Description
S-QFX5K-C1-P1-5	Flex Sub Software, Class 1 QFX5000 line, Prem 1, Term: 5 Yrs
S-QFX5K-C1-P1-P	Flex Software, Class 1 QFX5000 line, Prem 1, Perpetual
S-QFX5K-C2-A1-3	Flex Sub Software, Class 2 QFX5000 line, Adv 1, Term: 3 Yrs
S-QFX5K-C2-A1-5	Flex Sub Software, Class 2 QFX5000 line, Adv 1, Term: 5 Yrs
S-QFX5K-C2-A1-P	Flex Software, Class 2 QFX5000 line, Adv 1, Perpetual
S-QFX5K-C2-A2-3	Flex Sub Software, Class 2 QFX5000 line, Adv 2, Term: 3 Yrs
S-QFX5K-C2-A2-5	Flex Sub Software, Class 2 QFX5000 line, Adv 2, Term: 5 Yrs
S-QFX5K-C2-A2-P	Flex Software, Class 2 QFX5000 line, Adv 2, Perpetual
S-QFX5K-C2-P1-3	Flex Sub Software, Class 2 QFX5000 line, Prem 1, Term: 3 Yrs
S-QFX5K-C2-P1-5	Flex Sub Software, Class 2 QFX5000 line, Prem 1, Term: 5 Yrs
S-QFX5K-C2-P1-P	Flex Software, Class 2 QFX5000 line, Prem 1, Perpetual
Services licenses	
SVC-COR-QFX51-48M	Juniper Care Core Support for QFX5120-48YM Switches
SVC-ND-QFX51-48M	Juniper Care Next Day Support for QFX5120-48YM
SVC-COR-QFX5KC1-MS	Juniper Care Core Support for S-QFX5KC1-MACSEC-P
Advanced Telemetry Feature (ATF) licenses	
S-QFX5K-C1-ATF-P	SW, QFX5K, Class 1, ATF License SKU, Perpetual, SVC Customer Support to be purchased separately
S-QFX5K-C2-ATF-P	SW, QFX5K, Class 2, ATF License SKU, Perpetual, SVC Customer Support to be purchased separately

Note: An ATF license is needed on each Inband Flow Analyzer (IFA) terminating node. For definition of IFA terminating node and models supported, please refer to our Monitoring, Sampling, and Services Interfaces User Guide.

Optics and transceivers

Up-to-date information on supported optics for the QFX5120 switches can be found in the Hardware Compatibility Tool: QFX5120-32C, QFX5120-48T, QFX5120-48YM, and QFX5120-48Y.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3088

About HPE

HPE is a leader in essential enterprise technology, bringing together the power of AI, cloud, and networking to help organizations achieve more. As pioneers of possibility, our innovation and expertise advance the way people live and work. We empower our customers across industries to optimize operational performance, transform data into foresight, and maximize their impact. Unlock your boldest ambitions, with HPE. Discover more at HPE.com.

Visit HPE.com

Chat now

© Copyright 2025 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Intel is a trademark of Intel Corporation or its subsidiaries in the U.S. and/or other countries. sFlow is a registered trademark of InMon Corp. All third-party marks are property of their respective owners.

a00150810ENW, Rev. 1

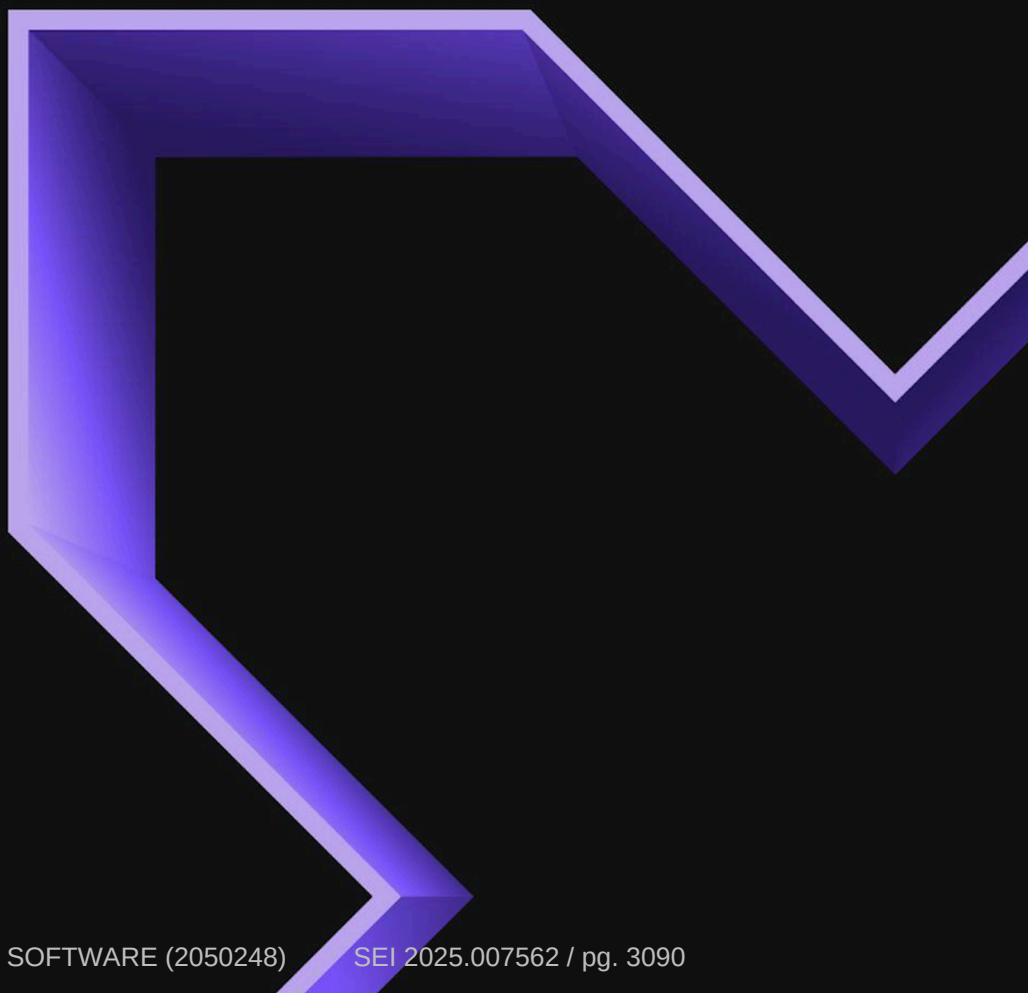
HEWLETT PACKARD ENTERPRISE

hpe.com

v1.1 | November 2024 | RA-2147

REFERENCE ARCHITECTURE

Nutanix for Enterprise Edge Computing



NUTANIX

Legal

© 2024 Nutanix, Inc. All rights reserved. Nutanix, the Enterprise Cloud Platform, the Nutanix logo and the other Nutanix products, features, and/or programs mentioned herein are registered trademarks or trademarks of Nutanix, Inc. in the United States and other countries. All other brand and product names mentioned herein are for identification purposes only and are the property of their respective holder(s), and Nutanix may not be associated with, or sponsored or endorsed by such holder(s). This document is provided for informational purposes only and is presented "as is" with no warranties of any kind, whether implied, statutory or otherwise.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

Contents

1. Executive Summary 5

2. Introduction 6
Purpose 6
Audience 6

3. Nutanix Cloud Platform Overview 7
Physical Layer 7
Hypervisors 9
Management 9
Business Continuity and Disaster Recovery 9
Automation 11
Security and Compliance 11

4. High-Level Design Considerations 12
Choosing an Enterprise Edge Architecture 12
Choosing a Hypervisor 20
System Availability 20
System Recoverability 22
Performance and Scalability 25
Manageability 26
Choosing a Control Plane 27
Choosing the Right Licensing and Support 27
Choosing Hardware 29
High-Level Design Recommendations 30

5. Detailed Technical Design 32
Required Software Versions 32
Physical Layer Design 33
Virtualization Layer Design 49
Management Layer Design 51
Security Layer Design 54
Automation Layer Design 58
Operations Design 61
BCDR Design 62

6. Optional Nutanix Products and Services..... 71

7. Conclusion..... 72

8. Appendix..... 73
Best Practices for Enterprise Edge Sites..... 73
References..... 85

About Nutanix..... 87

List of Figures..... 88

1. Executive Summary

Each organization defines edge computing differently; we define edge computing as workloads (applications and services) hosted and contained outside the core enterprise datacenter. These workloads fall into three categories:

1. Internet of Things (IoT) edge
   a. End users: developers, data scientists
   b. Roles: data acquisition, inferencing, modeling
   c. Typical use cases: manufacturing, transportation, robotics
2. Enterprise edge
   a. End user: enterprise IT
   b. Roles: localized applications, service hosting, remote office
   c. Typical use cases: file server, remote desktops, latency sensitive applications, business continuity planning (BCP)
3. Telco edge
   a. End user: the enterprise (operated and managed by the service provider)
   b. Typical use cases: multi-access edge computing, carrier-grade network function virtualization (NFV) services

This reference architecture focuses on the Nutanix Cloud Platform as a solution for enterprise edge workloads.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3094

2. Introduction

Purpose

We created this reference architecture to assist architects through the design process of implementing enterprise edge sites. After reading this document, architects should understand Nutanix best practices for enterprise edge sites and the implications and justifications of the design choices they make.

Audience

This reference architecture is part of the Nutanix Solutions Library. We wrote it for IT decision makers and architects responsible for deploying enterprise edge applications and services. Readers of this document should already be familiar with Nutanix.

This document often refers readers to the Nutanix Hybrid Cloud Reference Architecture.

Unless otherwise stated, the solution described in this document is valid on AOS versions 5.20 and later.

Document Version History

Version Number	Published	Notes
1.0	July 2022	Original publication.
1.1	November 2024	Updated AOS release cycle descriptions.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3095

3. Nutanix Cloud Platform Overview

Physical Layer

Nutanix converges compute, storage, storage networking, and virtualization, reducing complexity and replacing the separate servers, storage systems, and storage area networks (SANs) found in conventional datacenter architectures. Each node in a Nutanix cluster includes compute, memory, and storage, and nodes are grouped into clusters. AOS software running on each node pools storage across nodes and distributes operating functions across all nodes in the cluster for performance, scalability, and resilience.

Hardware

The Nutanix Cloud Platform provides significant flexibility when it comes to hardware platform selection. Available options include:

- Nutanix NX appliances
- Original equipment manufacturer (OEM) appliances from leading vendors such as Dell, Lenovo, HPE, and Fujitsu
- Other third-party servers from a wide range of vendors

The Nutanix Hardware Compatibility Lists contain the most up-to-date information on supported systems.

Compute

The process for sizing systems to meet compute needs in a Nutanix environment is similar to that of other architectures. However, you must ensure that your design provides enough compute (CPU and RAM) to support the CVM.

Storage

Nutanix nodes offer a range of storage configurations:

- Hybrid nodes combine flash SSDs for performance and HDDs for capacity.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3096

- All-flash nodes use traditional flash SSDs.
- NVMe nodes use NVMe SSDs.

You can mix different node types in the same cluster.

Nutanix AOS storage exhibits data avoidance and efficiency using techniques such as thin provisioning, intelligent cloning, compression, deduplication, and erasure coding. These techniques accelerate application performance and optimize storage capacity. They are intelligent and adaptive, requiring little or no fine-tuning in most cases, which reduces operating expenses and frees your IT staff to focus on growth and innovation. Unlike traditional storage architectures, the Nutanix web-scale design ensures that data efficiency techniques scale as the cluster grows.

For more information, see the Data Efficiency tech note.

Networking

The distributed storage architecture relies on the performance and resilience of the physical network. A good design provides high performance while maintaining simplicity. For more details on networking, see the Physical Networking best practice guide and the AHV Networking best practice guide.

Cluster Design

A Nutanix cluster is the management boundary of the storage provided to a group of workloads. A Nutanix deployment can have either single clusters with mixed workloads or dedicated clusters for each workload type in a block-and-pod design. Designs with dedicated clusters can include the following cluster types:

Management clusters

Designed to run VMs that support datacenter management services, such as Nutanix Prism Central, VMware vCenter, and Active Directory (AD) domain controllers, and other management workloads, such as DNS, DHCP, NTP, and syslog.

Edge clusters

Reside at an edge or remote and branch office (ROBO) deployment to run VMs or ROBO workloads. These clusters are typically distinguished from normal workload

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3097

clusters by their small size and limited external bandwidth and can contain a variety of node types and sizes.

Hypervisors

This solution covers two enterprise-grade hypervisors: Nutanix AHV and VMware ESXi (vSphere). Both fulfill a similar set of requirements and use cases. Nutanix AHV is included at no additional cost with every Nutanix node. For more information on AHV, see the Nutanix AHV Virtualization tech note and the AHV best practice guide. For information on VMware vSphere on Nutanix, see the VMware vSphere best practice guide.

Note: Nutanix also supports Microsoft Hyper-V; however, this document only covers AHV and ESXi.

Management

Nutanix Prism is the centralized management solution for Nutanix environments. Prism combines multiple aspects of datacenter management into a single consumer-grade design that provides complete infrastructure and virtualization management, operational insights, and troubleshooting.

For more detailed information about Prism, see the Prism software documentation and the Prism tech note.

Business Continuity and Disaster Recovery

We built Nutanix with resilience in mind, so the platform includes redundancy for power and other hardware components and enables you to protect entire datacenters. Nutanix provides native business continuity, including backup and restore and disaster recovery, at the hardware, node, data, VM, and datacenter or site levels.

For more detailed information about Nutanix business continuity and disaster recovery (BCDR), read the Data Protection and Disaster Recovery best practices guide, the Disaster Recovery with Nutanix Cloud Clusters (NC2) on AWS tech note, the Nutanix Disaster Recovery (previously Leap) software documentation, and the Nutanix Mine software documentation.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3098

Snapshots and Clones

An individual cluster can create a snapshot of a vDisk or an entire VM. Nutanix snapshots are redirect-on-write, where the pointers that indicate which physical disk extent maps to a virtual disk are updated only as data changes.

Snapshots can be application-consistent or crash-consistent. AOS can trigger an application-consistent snapshot in Nutanix Guest Tools or VMware tools, depending on which hypervisor you use.

For ESXi-triggered clones, AOS supports offloading the clone using vStorage API for Array Integration (VAAI). The VM must be turned off and the clone must reside on the same datastore as the primary VM in order to trigger offloading.

> **Note:** Nutanix snapshots are a vital element of a data protection strategy; however, they aren't a substitute for a full backup methodology.

Replication Options

You can also replicate Nutanix snapshots to multiple destination clusters to provide multiple redundant copies if needed. Configure these arrangements as part of the snapshot schedule by specifying each remote site that should receive a copy and how many copies it should retain.

> **Note:** One-to-many relationships are allowed (Site A to Site B, Site A to Site C, Site A to Site N), but cascading relationships (Site A to Site B to Site N) aren't supported.

Protection Domains

With Prism Element, you can group VMs into protection domains. During a failover event, all the entities in the protection domain are activated at the remote site as a group. The RPO you choose for these entities determines whether the system uses traditional asynchronous snapshots or lightweight snapshots for this process.

You can also create a consistency group for all VMs and volume groups in a protection domain. Consistency groups enable you to snapshot all members of the group in a crash-consistent manner.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3099

Automation

Automation and orchestration are critical to IT success. By simplifying infrastructure management across the entire lifecycle, automating operations, and enabling self-service, Nutanix helps you deploy datacenter infrastructure that delivers a high degree of scalability, availability, and flexibility with Prism (centralized automation management), Nutanix Cloud Manager (NCM) Self-Service (previously Calm; application orchestration), and simplified test and development automation.

Security and Compliance

Nutanix takes a security-first approach that includes a secure platform, extensive automation, and a robust partner ecosystem. Security Configuration Management Automation (SCMA) monitors the health of storage and VMs, automatically healing any deviations from the baseline, and data-at-rest encryption (DaRE) features add to our robust security capabilities. We also provide additional configuration options if you need to add an extra layer of security to fulfill business or technical requirements.

For more detailed information on Nutanix security and compliance features, see the following documents, separated by category:

- Networking: Flow Network Security tech note
- Information: Information Security tech note
- Cloud: Nutanix DRaaS Security tech note
- Database: Nutanix Era Security tech note

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3100

4. High-Level Design Considerations

There are several high-level design decisions you must make before proceeding to the detailed technical design.

Choosing an Enterprise Edge Architecture

First, you need to know what availability you need and what failures the design must protect against. These are key input requirements.

You also need to be familiar with the regions and availability zones as defined in the High-Level Design Considerations section of the Nutanix Hybrid Cloud Reference Architecture. Briefly, a region holds one or more availability zones. Each availability zone contains one or more datacenters or edge locations.

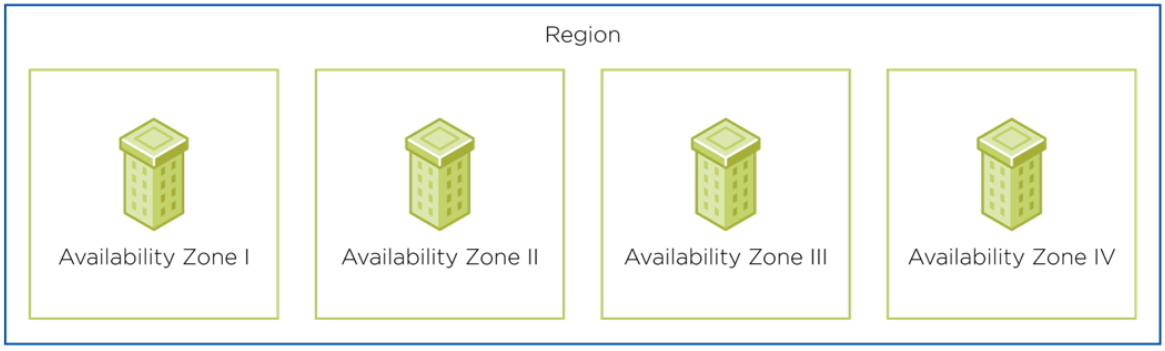


Figure 1: Availability Zones in a Region

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3101

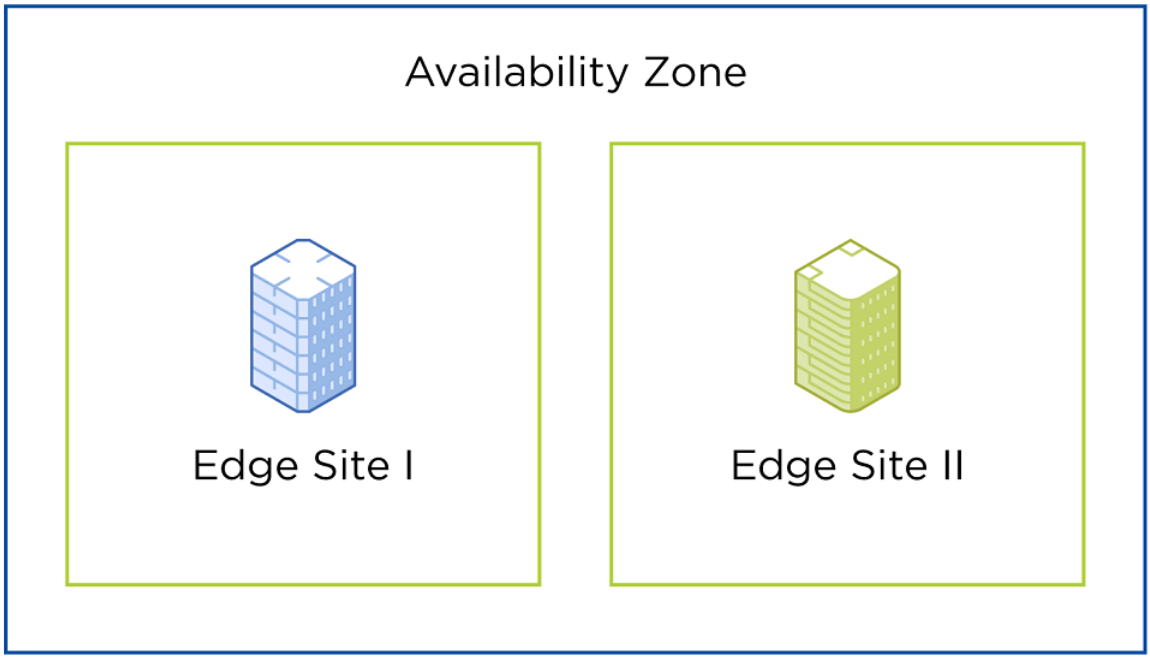


Figure 2: Edge Sites in an Availability Zone

Because an enterprise edge deployment can cover many locations often distributed across multiple geographies, we suggest that you logically group the manageability, replication, and BCDR components of your edge sites into a single region with multiple availability zones. This logical grouping provides design advantages for the control plane, scalability and performance, and BCDR.

> **Note:** If your enterprise edge deployment has a small number of sites and single locations, you may not need this grouping.

When choosing an enterprise edge architecture, keep the following things in mind:

- Latency requirements can vary depending on the deployment and the resources being consumed. For example, witness VMs hosted in the cloud can tolerate up to 500 ms of latency per 100 instances, while Prism Central can only tolerate 150 ms of latency per Prism Element instance that it manages.
- Bandwidth requirements vary based on desired recovery point objectives (RPOs), replication mediums, and the resources being consumed.
- A scaled-out Prism Central instance can manage 400 clusters and up to 2,000 nodes.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3102

- You need accurate NTP access.
- You must consider whether you want a WAN-restricted topology or open internet access.
- You need to review your BCDR requirements, planned versus unplanned downtime, and environmental risk.
- You can replicate data to more than one location using different replication types if needed. For example, you might use NearSync replication between sites located in the same availability zone and asynchronous replication to a datacenter in another region.

Edge Operating Models

Nutanix supports the following enterprise edge operating models, independent of the operating model of the core datacenter:

- Single site, active
  - › Applications are active in the edge site.
  - › Backups are stored in the same edge site that the applications run in.
  - › Long-time archiving is stored offsite.
  - › This model provides limited protection against datacenter failure.
- Single site, multiple failure domains, active-active
  - › Applications are active in one or more failure domains during normal production.
  - › Failure domains can be in different locations in the site (for example, opposite ends of a campus).
  - › Failure domains can provide disaster avoidance and disaster recovery for each other.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3103

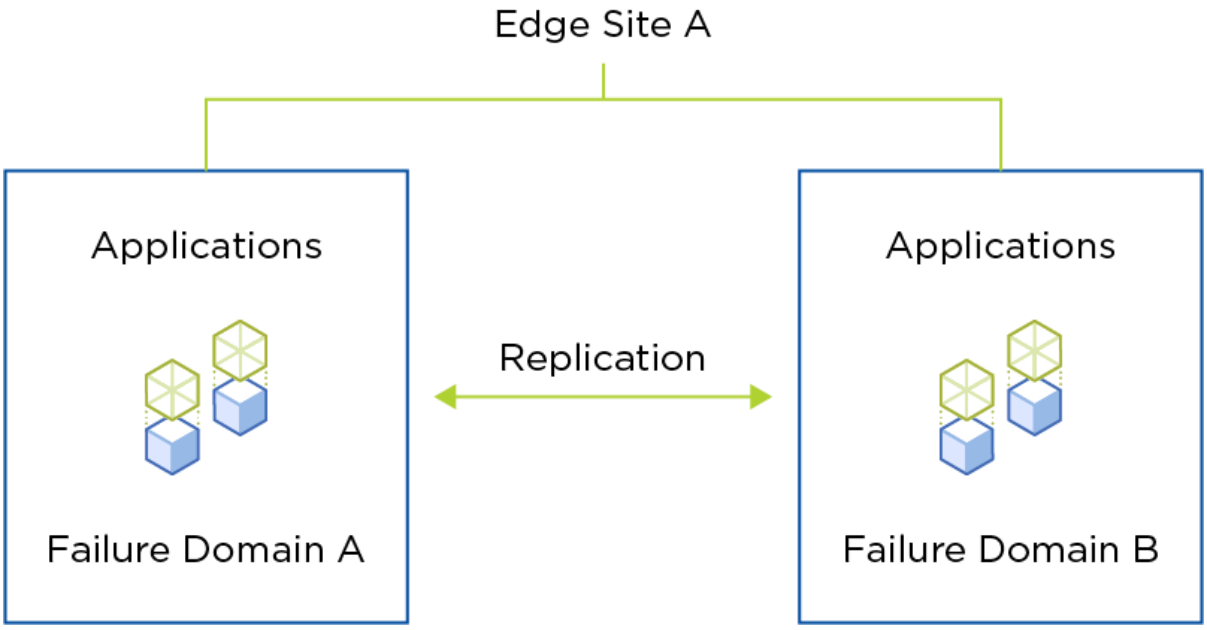


Figure 3: Single Site, Multiple Availability Domains, Active-Active

- Multiple sites, active-passive
  - › Edge-based applications typically run at the edge site during normal production.
  - › Usually the central datacenter (passive site) provides disaster avoidance and disaster recovery for the active enterprise edge site.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3104

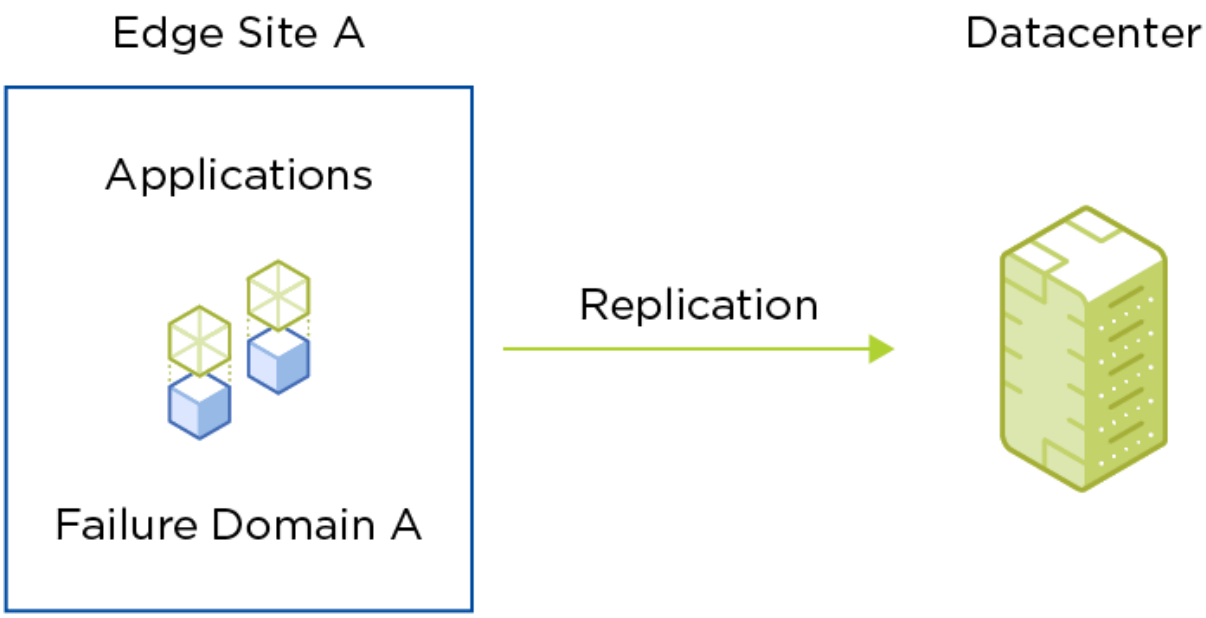


Figure 4: Single Site, Multiple Availability Domains, Active-Passive

- Multiple sites, fan-in or central datacenter
  - › Multiple enterprise edge sites replicate data to the datacenter.
  - › The datacenter acts as disaster recovery for the edge sites.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3105

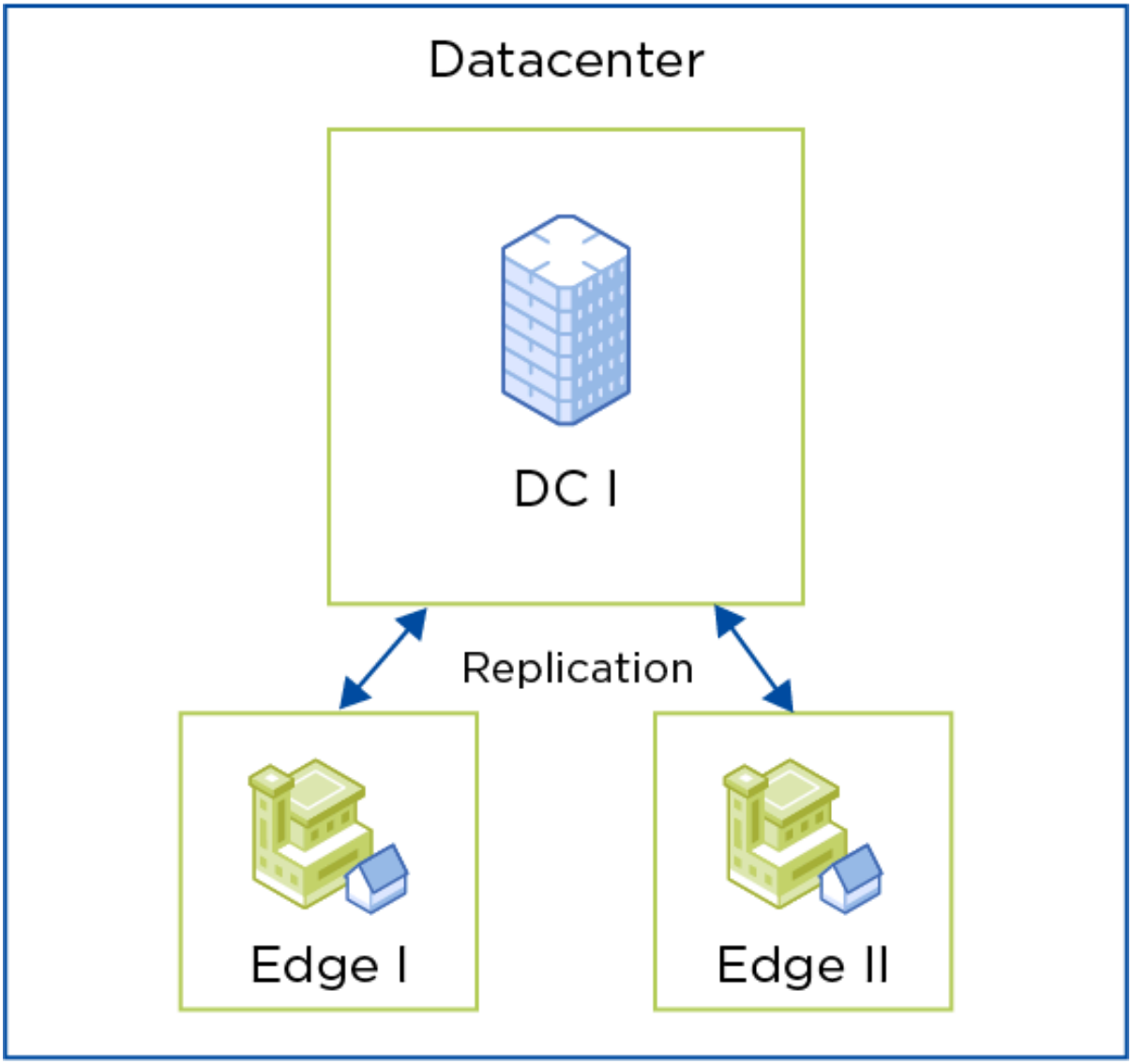


Figure 5: Multiple Sites, Fan-In or Central Datacenter

© 2024 Nutanix, Inc. All rights reserved

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3106

- Multiple sites, chain structure
  - › The datacenter provides disaster recovery for the closest edge site or sites.
  - › This model is often used by organizations with multiple datacenters or regions.
  - › The first-tier edge sites connected to the datacenter acts as disaster recovery sites for the next tier of edge sites. Some organizations call these locations regional datacenters.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3107

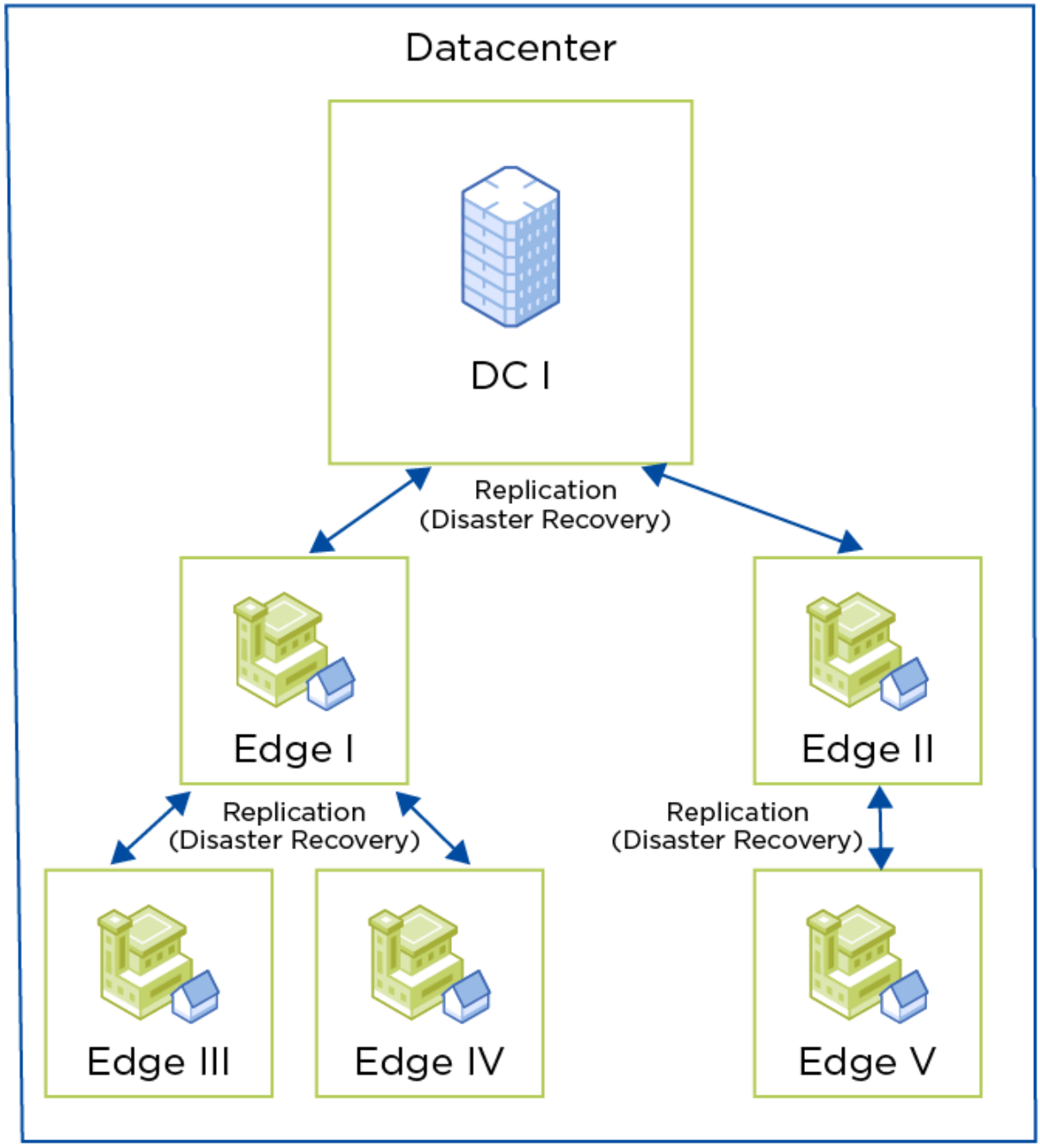


Figure 6: Multiple Sites, Chain Structure

© 2024 Nutanix, Inc. All rights reserved |

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3108

Choosing a Hypervisor

Nutanix supports multiple hypervisors: Nutanix AHV, VMware vSphere, and Microsoft Hyper-V. This design covers the deployment of either Nutanix AHV or VMware vSphere.

Nutanix AHV is included with AOS and delivers high performance, flexible migrations, integrated networking, security hardening, automated data protection and disaster recovery, and rich analytics. AHV is a lean virtualization solution with robust, integrated management features. VMware vSphere is a proven virtualization platform used by many organizations. It has a robust ecosystem but is a complex platform with many design choices and settings to tune that often requires the purchase of additional licenses.

System Availability

When evaluating availability requirements, start by building a dependency map of the applications and services hosted at the enterprise edge coupled with the service-level agreement (SLA; measured in 9s of availability) that the Nutanix system needs to support. Next, categorize availability events as planned or unplanned to enable you to plan for unforeseen events.

Single-Node Clusters

Let's say, for example, that an edge site has a single node in the Nutanix cluster (ROBO1) that hosts compute and storage. During write operations, the cluster mirrors data across the internal drives. In the event of a drive loss, the cluster enters a read-only state until the drive failure has been addressed, meaning that any hardware failure renders the system, application, and service offline.

You could address the availability constraints of the single-node cluster in the following ways:

Replicate data to a neighboring node: Deploy and maintain two separate single-node clusters that each serve as a replication partner to the other and independent failure domains.

Replicate data to the central datacenter or cloud.

The advantages of the single-node cluster are:

- It's an operationally well-understood and simplified model.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3109

- It has lower capex.
- It offers 1 GbE support.

The disadvantages of the single-node cluster are:

- It can support fewer VMs.
- You can't easily expand the cluster; it requires additional planning.
- It doesn't support storage optimization features.
- Without standard operating procedures (SOPs), RPOs and RTOs can be negatively affected.
- Planned outages such as patches and updates can require downtime.

Two-Node Clusters

A two-node cluster (ROBO2) improves system availability. In this design, two Nutanix nodes replicate data synchronously (RPO 0) while supporting VM high availability and migration features like automatic restart and migration, dramatically decreasing the RTO.

Two-node clusters offer reliability for smaller sites that must be cost effective and run with tight margins. These clusters only use a witness in failure scenarios to coordinate rebuilding data and automatic upgrades. You can deploy the witness offsite up to 500 ms away for asynchronous replication and 200 ms away for Metro Availability. Multiple clusters can use the same witness for two-node and metro clusters.

The advantages of the two-node cluster are:

- It aggregates system resources (compute and storage).
- It reduces the RPO and RTO.
- It automatically recovers resources.
- There's minimal impact from planned outages such as patches and updates.
- It supports asynchronous replication with lower RPOs to a neighboring cluster.

The disadvantages of the two-node cluster are:

- You can't easily expand the cluster; it requires additional planning.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3110

- It relies heavily on the availability of a witness VM.
- Staff needs familiarity with SOPs for node patching and upgrading.
- It doesn't support storage optimization features.

Three-Node or Greater Clusters

Clusters with three or more nodes (ROBO3) follow the traditional datacenter deployment strategy and have the same levels of availability and platform-specific features to optimize compute and storage resources. Clusters with three or more nodes address availability concerns by providing advanced clustering and data distribution, which result in lower RTOs for planned versus unplanned system outages.

The advantages of clusters with three or more nodes are:

- They support all Nutanix features and functionalities.
- Their clustering and data distribution yield a lower RTO.
- They have zero down time for patches, upgrades, and cluster expansion operations.

The disadvantages of clusters with three or more nodes are:

- They have a higher capex due to the additional nodes.
- For optimum performance, they require a 10 GbE network connection for all nodes. However, 1 GbE is sufficient for clusters with up to eight members.
- They use additional compute resources.
- They have increased power and cooling requirements.

System Recoverability

System recoverability defines how you recover the service or application hosted at the edge when the primary copy has been compromised or lost.

Nutanix has several recoverability options for customers who want to protect and back up their data against defined SLAs. The following figure and table illustrate four common recoverability strategies that you can use regardless of the edge strategy you deployed.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3111

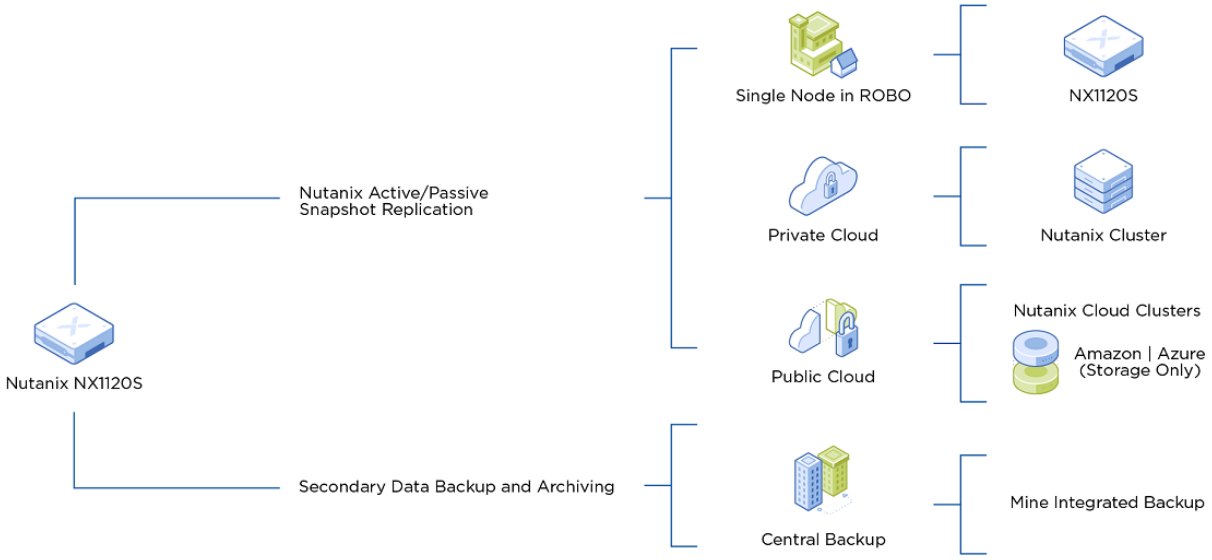


Figure 7: Overview of Nutanix Recoverability Options

Table: Replication Options with Nutanix

Destination	Strategy	Description	RPO	Recovery Method
Single-node ROBO	Asynchronous replication	Used when the source and the destination are single-node clusters.	6 hours	VM
Private cloud	Near-synchronous (NearSync) replication	Used when there are at least three nodes in a cluster on both the primary and the remote site.	1–15 minutes	VM
Private cloud	Asynchronous replication	Used when replicating to a cluster of at least three nodes in the primary datacenter.	60 minutes	VM

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3112

Destination	Strategy	Description	RPO	Recovery Method
Public cloud	Nutanix Cloud Clusters (NC2; asynchronous)	Used when customers need to host Nutanix on AWS, GCP, or the Nutanix public cloud; allows customers to use the same replication strategies as the private cloud.	60 minutes	VM
Public cloud	Amazon S3 / EBS, Azure Blob	Uses the Cloud Connect feature to replicate VMs to AWS S3 (EBS for metadata) or Azure Blob Storage. With this option, customers can't turn on VMs because they're just using a storage target or service in the public cloud.	60 minutes	VM
Central backup	Nutanix Mine (secondary data backup and archiving)	Used when customers need a dedicated, turnkey solution that supports backup and archiving using integrated solutions from Veeam and HYCU.	60 minutes	VM- or file-level backup

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3113

For more information on NearSync requirements and limitations, see Requirements of Data Protection with NearSync Replication. For more information on single-node clusters, consult Single-node Clusters. To understand more about the Cloud Connect feature and protection domains, see Asynchronous Replication Using Cloud Connect (On-Prem to Cloud).

Performance and Scalability

When you build an enterprise edge solution, you need to carefully define your performance and scalability requirements because node deployment strategy can adversely affect the scalability of the solution. For example, with ROBO1, you're limited to a single node and can't expand your deployment by adding additional nodes or take advantage of data distribution across multiple compute nodes. ROBO2 has similar constraints.

> **Note:** If you need to be able to scale your edge solution beyond two nodes or add storage-only nodes to the cluster, you should implement a three-node cluster.

Regardless of whether your sites are classified as small (fewer than 10 VMs) or large (more than 50 VMs), you need to standardize the resources the edge sites provide and consume from the core datacenter. To accomplish this standardization, consider the four key elements of edge sites:

1. Devices and applications
   a. Create a dependency map of physical devices and applications that your infrastructure interfaces with or provides services for.
   b. Understand whether you plan to scale your devices and applications linearly over time.
   c. Establish whether the device or application should have a dedicated cluster or share a mixed cluster with other applications and services.
2. Clusters
   a. Define the maximum size of the clusters in your edge sites and the maximum number of edge sites in your organization.
   b. Reference the configuration maximums of Nutanix components and third-party components used in your design.
   c. Define the services that edge sites should provide (file sharing, NFV).

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3114

3. Network
   a. Choose the optimal network layout, considering how sites receive and send public versus private traffic and connect to the core datacenter.
   b. Use minimal bandwidth and a latency standardized for connectivity to the core datacenter.
4. Cloud
   a. Determine your cloud deployment model (hybrid, private, public).
   b. Determine which additional cloud resources you need, such as additional storage to cover replication from additional edge sites.
   c. Determine how much additional bandwidth you need in order to add additional edge sites to the cloud.

Manageability

The deployment model you use for the enterprise edge solution influences overall manageability.

Dedicated or Mixed Clusters

Typically, in enterprise edge sites organizations deploy between 5 and 10 VMs. In this instance, a mixed workload cluster makes the most sense. However, with larger deployments (for example, large distribution centers) that serve many mission-critical applications and have many regulatory compliance requirements, the complexity of sizing and operating the mixed environment increases dramatically.

When you operate edge sites at a large scale, your architecture, design choices, and requirements start to look more like those of a traditional datacenter. For these cases, we encourage you to review the Will You Deploy Dedicated or Mixed Clusters? section of the Nutanix Hybrid Cloud Reference Architecture.

Storage-Only Nodes in Clusters

Storage-only nodes add storage capacity and I/O performance to a cluster. Storage-only nodes can be any node type, but they're typically configured with just enough CPU and memory resources to run the CVM because no application VMs run on them. These nodes are members of the AOS cluster but aren't visible to the hypervisor cluster for nonstorage functions, so the hypervisor can't schedule other VMs to run on them.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3115

Note: You can only add storage-only nodes to clusters with three or more nodes.

Note: We recommend deploying storage-only nodes in pairs.

Choosing a Control Plane

When working with larger edge deployments geographically dispersed across multiple regions, we expect the organization to face control plane proliferation, so you must give additional thought to the operational administration of the clusters. In this design:

- The primary control plane is Prism Central.
- If you use ESXi, you also need VMware vCenter.

Each of these control planes has a maximum size that dictates the number of VMs, nodes, and clusters a single instance can manage. For AOS 5.20 (the minimum version required for these solutions), Prism Central (scaled-out configuration) can manage a maximum of:

- 25,000 VMs
- 400 clusters
- 2,000 nodes

These limits are quickly realized when you work with multiple sites and auxiliary solutions, especially when sharing a Prism Central instance with the core datacenter infrastructure. At very large scale (multiple sites, geographically dispersed), it makes sense to deploy an additional Prism Central instance in the management cluster in your core datacenter to manage the edge sites or to deploy a Prism Central instance specific to the region it manages.

Choosing the Right Licensing and Support

When evaluating the different Nutanix platform options available, there are two key decision points:

- Your software and support licensing types
- Your platform vendor

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3116

Software and Support Licensing

Nutanix nodes are primarily available in two different purchasing or licensing options: appliances or software-only.

Appliances:

- Available directly from Nutanix or through our OEM relationships.
- Appliance-based licensing is referred to as life-of-device licensing, meaning it's only applicable to the appliance it was purchased with.
- The manufacturer of the appliance takes all support calls for software and hardware issues. For example, if you choose a Dell appliance, Dell takes all support calls and escalates to Nutanix for software support as needed. With a Nutanix NX appliance, all support calls go directly to Nutanix.

Software-only:

- Decouples software and support licensing from the underlying hardware, which enables:
  - License portability. You can use the same license even when the underlying hardware changes, as with a hardware vendor change or a node refresh.

    Note: Licenses are portable for like-for-like hardware replacements. If the hardware specification of the nodes changes, you might need to purchase additional licenses.

  - Deployment on additional supported hardware platforms, based on our qualified list of platforms, which you can find on the Hardware Compatibility Lists page.
  - Direct software support from Nutanix while the server vendor provides hardware support.
- Another type of software-only licensing is the core licensing option, which is best for customers who prefer the benefits of the software-only model but want hardware from a specific OEM server vendor. Core licensing enables customers to purchase software-only licenses and buy hardware from any of the appliance vendors. For example, XC-Core uses Dell XC OEM appliances but decouples software and hardware support.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3117

Vendor Considerations

When it comes to selecting a hardware vendor, there are many factors to evaluate:

- Brand loyalty
- Support quality
- Hardware quality
- Operational experience
- Configuration options
- Physical form factor

Choosing Hardware

Most edge workloads can successfully run on any of the Nutanix and OEM models available, but some models and configurations may be a better fit than others. Once you know the requirements of your workloads, you can use Sizer (a Nutanix product that calculates node and cluster configuration based on inputs) to determine the best configuration for your clusters.

The following sections provide considerations for hardware model selection and performance.

Model Types

The various Nutanix and OEM appliance models and servers give you the flexibility to identify and use the right solution to meet financial, space, and performance requirements for different projects.

Servers for this solution fall under the edge category, which are similar to the servers used for general workloads and EUC but may offer fewer options for CPU and storage because they're optimized for edge-specific use cases.

Performance Considerations

Nutanix and AOS meet the performance demands of different workloads without continuous performance tuning. However, different cluster design and configuration options still yield performance benefits. Selecting the appropriate node model and

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3118

configuration to meet application and solutions requirements is an important design decision. The primary design considerations for performance are:

- Number of drives: The number of HDDs or SSDs in a node can dramatically affect its performance characteristics.
  - › Write-heavy workloads benefit from additional storage devices to provide performance and consistency.
  - › Workloads like VDI typically have minimal capacity requirements but higher IOPS demands. It's common to use nodes with partially populated storage bays and as few as two flash devices per node, providing the right amount of storage capacity while still exceeding performance demands.
- All flash: All-flash clusters only use SSDs and provide higher IOPS and a more consistent I/O profile than HDDs.
- NVMe: New flash technology allows NVMe devices to deliver higher levels of I/O than SSDs with lower latencies.
  - › To realize the full benefits of NVMe, nodes are typically configured with remote direct memory access (RDMA). RDMA allows one node to write directly to the memory of another node by allowing a VM running in the user space to directly access a NIC, which avoids TCP and kernel overhead resulting in CPU savings and performance gains.
- Size of flash tier: In hybrid configurations containing SSD and HDD devices, the bulk of the performance comes from the flash tier. The flash tier in hybrid clusters should be sized to meet or exceed the size of the working set for all applications running on the cluster. There's no penalty for having too much flash in a cluster but not having enough can result in inconsistent performance.

High-Level Design Recommendations

To summarize, for edge computing on Nutanix solutions, we recommend the following:

- Logically group the manageability, replication, and BCDR components of your edge sites in a single region or availability zone.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3119

- Use Prism Central as the primary control plane.
  - › If you use ESXi, you also need VMware vCenter.
- Use the simplified block-and-pod architecture detailed in the Block and Pod Architecture section of the Nutanix Hybrid Cloud Reference Architecture.
  - › If you're building a large-scale site (more than four blocks with the expectation of additional blocks in the future) with the characteristics of a datacenter, see the Nutanix Hybrid Cloud Reference Architecture.
- Build clusters with one or three nodes.
  - › If you need to be able to scale your edge solution beyond two nodes or add storage-only nodes to the cluster, you should implement a three-node cluster.
- If you use them, deploy storage-only nodes in pairs.
  - › You can only use storage-only nodes in clusters with three or more nodes.
- Define an SOP that stipulates how to scale one- or two-node clusters in your design, as this step isn't a function of the core AOS and doesn't have a workflow.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3120

5. Detailed Technical Design

This section provides technical guidelines for each layer of the design stack.

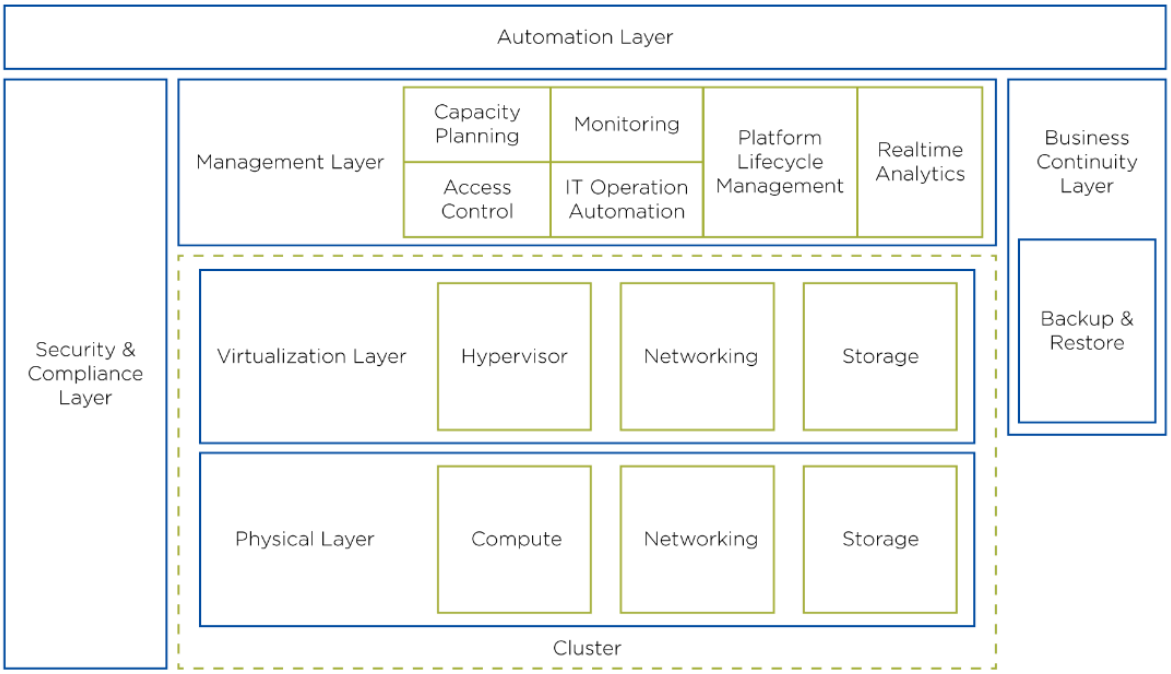


Figure 8: Overview of the Technical Design

Required Software Versions

We used the versions in the following table for this design.

Table: Software Versions

Name	Version	Reasoning
Prism Central	pc.2020.7	Use the latest version available.
Nutanix AOS	5.20	Use the latest version available.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3121

Name	Version	Reasoning
Nutanix AHV	5.15	Use the latest version available.
VMware vSphere	6.7 or 7.0	Use either major release.
VMware vCenter	6.7 or 7.0	Recommended for vSphere deployments.

Physical Layer Design

This section guides you through the process of designing all physical aspects of your Nutanix edge deployment.

Choosing the Cluster Size

When designing a Nutanix cluster, it's important to consider hardware vendor recommendations, security, and operational requirements that may dictate the optimal cluster size. The following table provides a comprehensive list of the design considerations that pertain to cluster size.

Table: Cluster Size Design Considerations

Area	Limiting Factor	Considerations
Operations and manageability	Maintenance window	Define and validate your maintenance window and make sure the cluster upgrade process fits in the window. Example: If you have a maintenance window of 12 hours and a full single node upgrade takes at least 45 minutes, your maximum cluster size is 12–15 nodes.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3122

Area	Limiting Factor	Considerations
Security and compliance	Security zones in an organization or business unit	Collect all relevant security and compliance requirements. Example: You have multiple security zones: internet perimeter, prod, test and dev, and inner perimeter. Every security zone has different cluster sizes: internet-facing perimeter clusters usually have fewer nodes and workloads to minimize impact of a security breach or DDoS attack. Less-critical test and dev clusters may also have more relaxed change management policies and can therefore have many hosts.
Vendor recommendations and limitations	Hypervisor limitations, management plane limitations, and vendor recommendations	Each product has limitations and vendor recommendations. Don't cross boundaries set by the vendor. Check the vendor's limitations and recommendations table.
Business continuity	RPO, RTO, and backup window	Collect BCDR requirements, RPO, RTO, backup and restore time window, and backup system performance statistics. Example: RPO: 24 hours, RTO: 48 hours. Ensure you can recover and restore from backup and restart workloads within 48 hours. A cluster where total storage capacity exceeds the technical capabilities of the backup system could fail to meet desired RTO.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3123

Area	Limiting Factor	Considerations
Workload considerations	Application architecture, application licensing, and application criticality	Verify application architecture with the application team or vendor, including HA, disaster recovery, scale-in vs. scale-out, and performance requirements. For example: Application has its own HA or disaster recovery. If the application can provide native HA or disaster recovery, the RPO and RTO considerations described in the Business continuity row of this table may not apply. Consider the licensing model for each application and its implications. For example: Oracle or MS SQL licensing models are based on physical core count. Design clusters for database performance and capacity requirements to avoid cluster oversizing and minimize license costs.
Networking	Total available network switch ports and available network switch ports per rack	You need to know the available physical ports per rack and rack row when choosing cluster size and number of clusters. For example: A configuration with 96 × 10 Gbps ports available per rack, 48 × 1 Gbps ports available per rack, 2 × 10 Gbps uplinks per Nutanix host, and 1 × 1 Gbps uplink for out-of-band management can have at most 48 nodes per rack (total capacity of the top-of-rack switches).

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3124

Area	Limiting Factor	Considerations
Datacenter facility	Available server rooms, total power and cooling, power and cooling per rack, total available rack units, available rack units per rack, and floor weight capacity	Power and cooling are two of the most important factors limiting Nutanix cluster size and node density. Don't exceed any hard limits when designing your cluster layout. When calculating power consumption and thermal dissipation, use the maximum values provided by vendor. A typical datacenter rack is 42RU. Some datacenters have racks up to 58RU.
One- and two-node clusters	Planned vs. unplanned downtime and scalability	You need to know how to handle planned vs. unplanned events, and you need a plan for scaling beyond one node.

AHV deployments have the following limits:

- A scaled-out implementation of Prism Central on AHV can manage up to 400 clusters, 2,000 nodes, or 25,000 VMs (whichever limit is hit first).

  Note: One- and two-node AHV clusters are only available for ROBO deployments.

VMware vSphere deployments have the following limits:

- A scaled-out implementation of Prism Central on ESXi can manage up to 400 clusters, 2,000 nodes, or 25,000 VMs (whichever limit is hit first).
- VMware vCenter can support 2,000 hosts and 25,000 VMs (turned on).
- A single VMware ESXi cluster can support a minimum of 2 nodes and a maximum of 48.

  › The maximum number of nodes in a Nutanix cluster with ESXi is limited by the hypervisor version. For more details, refer to official VMware vSphere Documentation.

  Note: Two-node ESXi clusters are only available for ROBO deployments.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3125

Failure Domain Considerations

Failure domains are the physical or logical parts of a computing environment or location that are adversely affected when a device or service experiences an issue or outage. The device or services affected greatly influence the size of the failure domain and its potential impact. For example, a router generally has a bigger failure domain than a wireless access point because more endpoints rely on a single router than a single access point. Identifying possible failure domains and keeping them small where possible reduces the chance of widespread disruption.

Building redundancy within and across failure domains helps mitigate the risks of failure. Nutanix clusters are resilient to a drive, node, block, and rack failures because they use redundancy factor 2 by default, allowing Nutanix clusters to self-heal.

Management Plane–Level Failure Domain

One of the most important failure domains is the management plane. The more workload domains a single management plane manages, the bigger the impact of a failure. When deploying the management plane, consider the following risk mitigations to reduce the impact of a failure:

- At a minimum, design to meet the availability requirements of the managed workload or service with the highest uptime requirement.
- Confine workload domain to a single edge site and defined security zone.
- Ensure that the API gateway is always available because other third-party integrations (such as the backup vendor integration) may rely on it.
- Configure built-in RBAC to restrict access to management platform resources.
- Design your management plane to reside in the region or location where your edge clusters reside.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3126

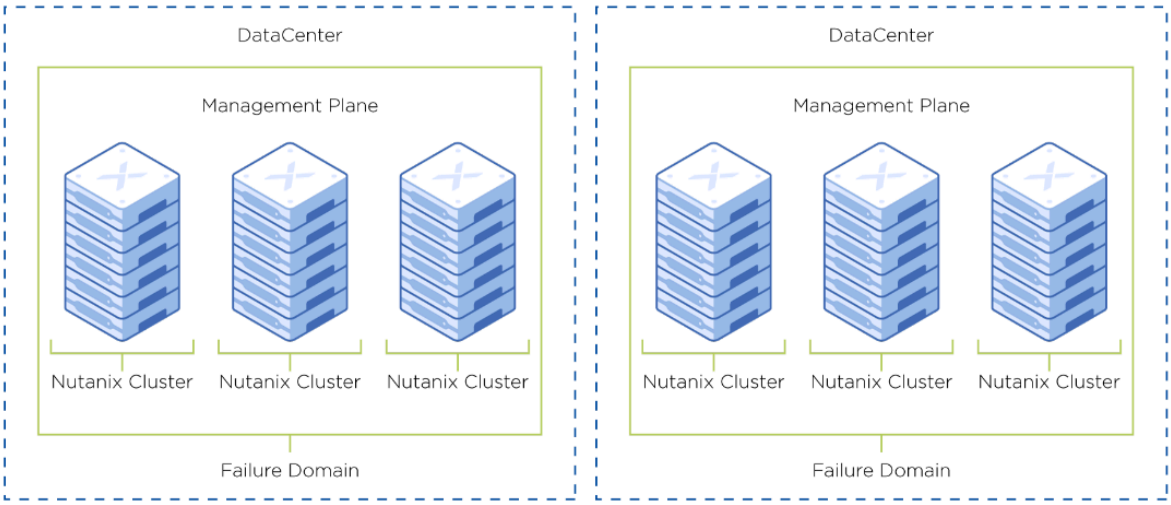


Figure 9: Management Plane Failure Domains

Cluster-Level Failure Domain

Nutanix clusters are another important failure domain. Large clusters result in larger failure domains and potentially higher business impacts, since they typically host considerably more workloads. To mitigate the risk of data unavailability or service disruption, design for redundancy at the cluster level to protect data and services and apply the following mitigations:

- Use redundant power.
- Use redundant top-of-rack switches.
- Ensure redundant upstream connectivity to top-of-rack switches from each Nutanix node.
- Ensure redundant connectivity from edge to central datacenter.
- Use Nutanix scale-out architecture and data protection capabilities to replicate data to a second Nutanix cluster if one cluster fails.
- Deploy the application across multiple clusters.
- For smaller edge sites (fewer than five VMs) with cost constraints, consider implementing two single-node clusters because they operate as independent failure domains without the complexities of managing two-node clusters.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3127

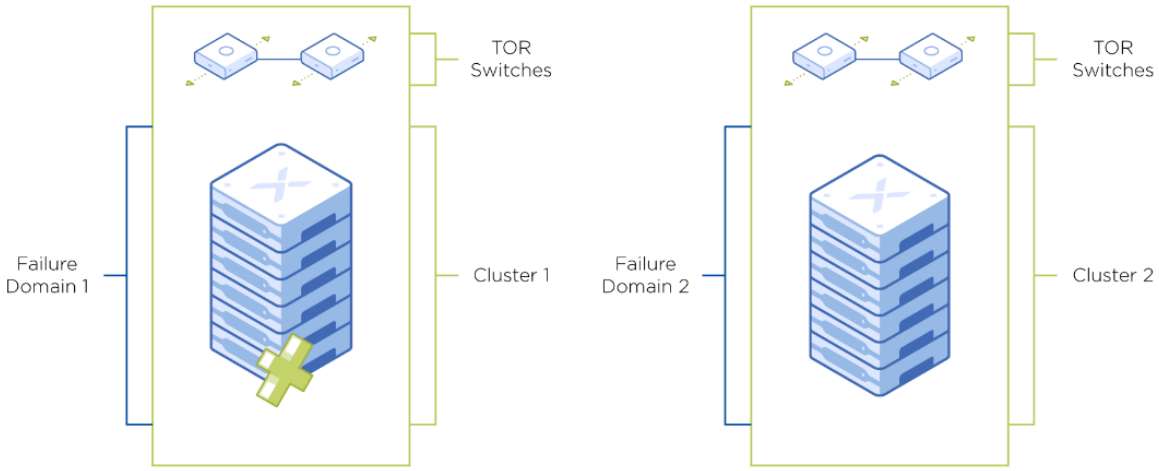


Figure 10: Nutanix Cluster Failure Domains

Rack and Server Room Failure Domains

Edge deployments can have a dedicated server room or a single wiring closet, but both represent a failure domain. Configure your deployment with the following mitigations:

- Use redundant power.
- Use independent cooling.
- Provide a redundant server room in a separate fire zone.
- Place the applications in multiple server rooms. For example, have AD domain controllers in separate server rooms.

If your edge site runs mission-critical workloads, consider mitigating risk by:

- Deploying stretched clusters across two server rooms in the edge site, representing a single failure domain with member nodes distributed across both rooms.
- Deploying two independent clusters across two server rooms in the edge site, representing two independent failure domains

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3128

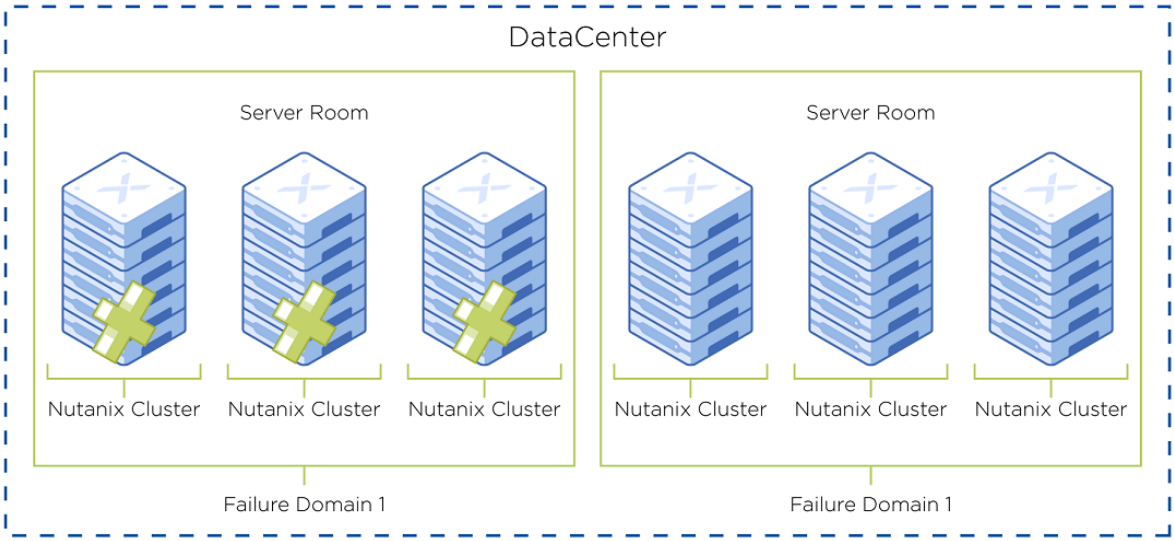


Figure 11: Server Room Failure Domains

Datacenter Failure Domains

Edge sites can lack the IT personnel necessary to assist during a failure scenario and keep the mean time to repair (MTTR) short. You should design your system with the following mitigations:

- Use redundant power.
- Use an independent and redundant cooling system for each datacenter room.
- Ensure redundant networking connectivity from different providers between datacenter buildings.
- Ensure redundant internet connectivity from different providers.
- Where possible, use multiple buildings and server rooms in separate buildings or campuses so that the failure of a single server room doesn't affect production. Distribute multicomponent services equally across datacenter server rooms.
- Ensure strict SLA compliance and keep well-documented resources and processes to help keep MTTR short.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3129

Designing Workload Domains

This design uses a single workload domain at each edge site. Each workload domain consists of a set of Nutanix nodes managed by the same management instance (Prism Central or VMware vCenter) and connected to the same network domain.

A single workload domain can include different hardware and software combinations and have all ESXi or AHV nodes or mix ESXi (running VMs) and AHV (not running VMs) nodes in a single cluster. Single workload domains at edge sites provide the following advantages:

- Efficient space usage
- Default redundancy level
- Simple consumption
- Decreased capex and opex

Note: Using a single workload domain increases the negative effect of a domain failure.

Note: If your edge site runs multiple workloads with different requirements or constraints, consider using multiple workload domains. Refer to the Designing Workload Domains section in the Nutanix Hybrid Cloud Reference Architecture.

Networking for Edge Sites

A Nutanix cluster can tolerate multiple simultaneous failures and protect the cluster's read and write storage capabilities. However, this level of resilience requires a highly available, redundant network connecting a cluster's nodes. Even with intelligent data placement, if network connectivity between more than the allowed number of nodes breaks down, VMs on the cluster could experience write failures and enter read-only mode.

Consult the Physical Networking best practice guide to learn more about general networking guidelines and design requirements and recommendations.

Physical Switches

Edge sites operating as datacenters require datacenter switches with large buffers (10 Gbps or faster), which are critical in a large AOS cluster that sustains critical growth or hosts storage-intensive applications. In this case, see the Physical Switches section of the Nutanix Hybrid Cloud Reference Architecture.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3130

In smaller edge clusters or ROBO deployments that have fewer than eight nodes or don't host write-intensive applications, the switch may not experience buffer contention, and you can relax these switch restrictions. The following switches don't meet high-performance datacenter switch requirements but are acceptable for these smaller edge clusters:

- Arista 7050
- Arista 7150S
- Cisco Catalyst 9000
- Cisco Catalyst 3000
- HPE FM2072

There are some switch types you should never use for any Nutanix deployment:

- Cisco Nexus 2000 (Fabric Extender)
- 10 Gbps expansion cards in a 1 Gbps access switch

Although Nutanix recommends an out-of-band management switch network separate from the primary network in traditional datacenter deployments, for enterprise edge sites these recommendations can be relaxed since the nodes typically have between one and three nodes. Configure IPMI, iLO, or iDRAC server-facing ports in the management network as access ports and don't use VLAN trunking for these ports. Restrict access to this critical management network.

Network Topology

In small edge sites running a handful of VMs, a simple network topology consisting of a pair of top-of-rack switches interconnected to a firewall and router is the simplest option. This simplified setup can address the requirements of a deployment with between one and three nodes.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3131

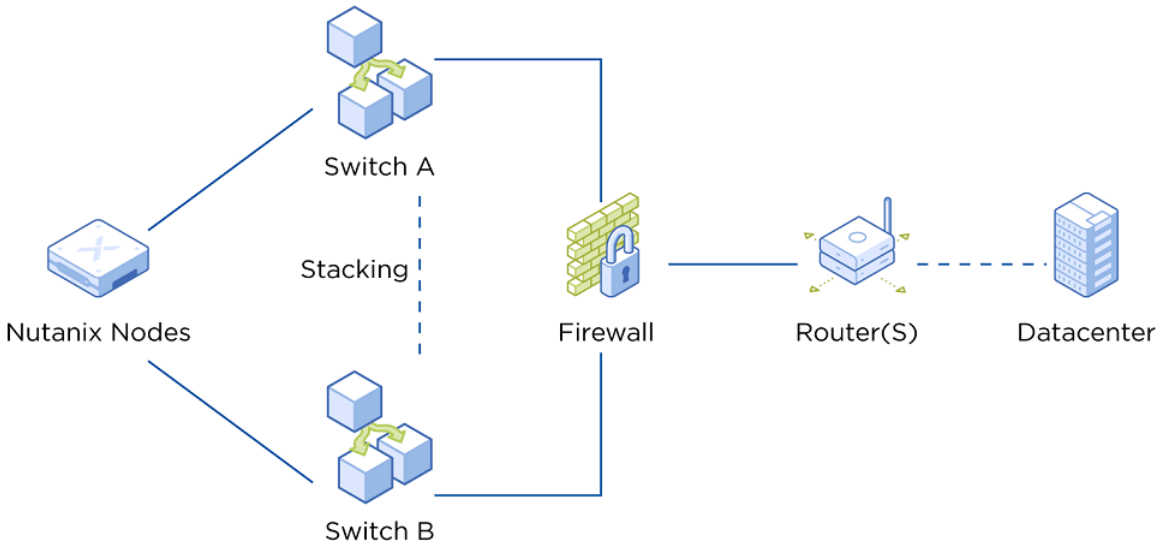


Figure 12: Small Edge Site Network Topology

For medium and larger deployments with multiple racks, Nutanix recommends using a leaf-spine topology because it's easy to scale, achieves high performance with low latency, and provides resilience. A leaf-spine topology requires at least two spine switches and two leaf switches. Every leaf connects to every spine using uplink ports.

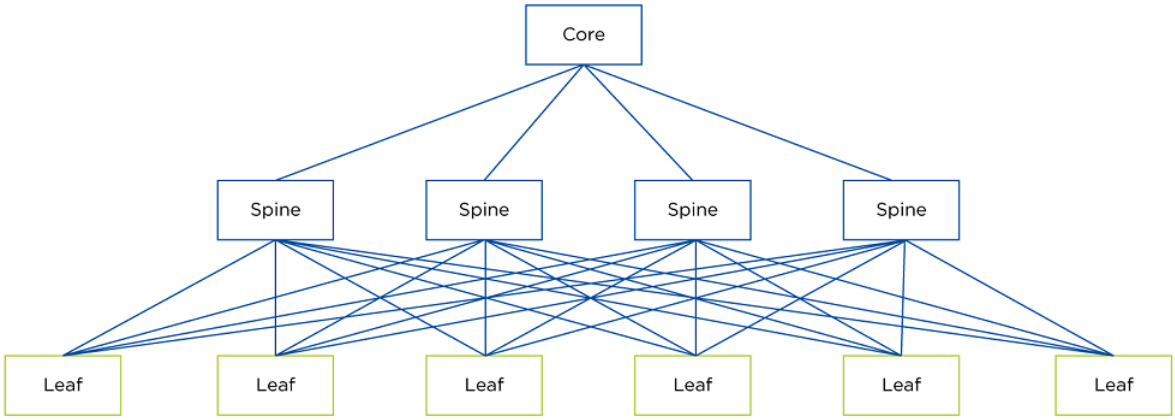


Figure 13: Leaf-Spine Topology for Medium and Larger Edge Sites

Note: If you're considering implementing a leaf-spine network topology, review the Network Topology section in the Nutanix Hybrid Cloud Reference Architecture for specific guidelines and recommendations.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3132

The following list details Nutanix best practices and requirements for edge site network topology:

- Ensure that every Nutanix node in a cluster is in the same layer 2 broadcast domain and shares the same IP subnet.
- You can populate nodes designed exclusively for edge or ROBO with 1 Gbps networking for one- and two-node clusters with latency spikes of approximately 6 to 8 ms.
  - › Limit your cluster size to at most eight nodes if you plan on using 1 Gbps.
- Ensure that when there are two or more nodes in a cluster, each layer of the network topology is highly available and tolerates individual device failures.
  - › Avoid configurations or technologies that don't maintain system availability during single-device outages or upgrades, such as stacked switches.
- Ensure that there are no more than three switches between any two Nutanix nodes in the same cluster.
- Don't use WAN or remote links between Nutanix nodes in the same Nutanix cluster.
- Separate Nutanix CVM and hypervisor hosts in a dedicated VLAN that doesn't include any VM traffic.
- Don't place Nutanix nodes in the same Nutanix cluster if the stretched layer 2 network spans multiple edge sites, buildings, datacenters, or availability zones or if there's a remote link between the two locations.
  - › Using a stretched layer 2 network over a layer 3 network is only acceptable when the Nutanix cluster is in the same switch fabric or aggregation layer, such as when a layer 2 network stretches between two racks in the same datacenter.
- Don't use features like block or rack awareness to stretch a Nutanix cluster between different physical sites.
- Configure adequate uplinks between switches or interswitch links for east-west storage traffic to minimize port-to-port oversubscription. For example, use multiple 40 Gbps uplinks (or interswitch links).
- Connect hosts using redundant links.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3133

- Configure switch ports facing Nutanix servers as spanning tree portfast or edge to skip the listening and learning phases and prevent cluster outages caused by changes to spanning tree topology.
- Configure the CVM and hypervisor VLAN as native, or untagged, on server-facing switch ports. Newly added nodes use untagged traffic for discovery and work out of the box, reducing manual server configuration.
- Use tagged VLANs on the switch ports for all guest workloads to keep the workloads separate from each other and from the CVM and hypervisor network.
- Reduce network oversubscription to ensure as close to a one-to-one ratio as possible. Dropped network packets or a congested network immediately affect storage performance.

Broadcast Domains

Nutanix recommends a traditional layer 2 network design to ensure that CVMs and hosts can communicate in the same broadcast domain even if they're in separate racks. The CVM and host must be in the same broadcast domain and IP subnet.

> **Note:** If you choose a layer 3 network design, refer to the Broadcast Domains section of the Nutanix Hybrid Cloud Reference Architecture.

Network Scalability

Because edge sites are typically small, they contain a simplified core, aggregation, and access layer switch design. In this scenario, to scale, you simply add additional access layer switches, taking into consideration the oversubscription ratios in the design.

If you used a leaf-spine network topology, see the Scaling the Network section of the Nutanix Hybrid Cloud Reference Architecture.

Connectivity to the Core Datacenter

There are multiple ways to establish connectivity from the edge to the core datacenter, including traditional VPNs and direct connect methods. Evaluating the various advantages and disadvantages of each method is beyond the scope of this document; however, keep in mind the latency and bandwidth requirements for edge sites:

- Witness VMs hosted in the cloud can sustain up to 500 ms of latency per 100 instances they manage.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3134

- Prism Central requires at least1.5 Mbps and a maximum latency of 150 ms to run CRUD operations, collect statistics, and perform updates.
- Scheduled replications have no set bandwidth requirements.

AHV Networking

AHV uses Open vSwitch (OVS) for all VM networking. The virtual switch is referred to as a bridge and uses a br prefix in the name. AHV also includes a Linux bridge called virbr0. The virbr0 Linux bridge carries management traffic between the CVM and AHV host. All other storage, host, and workload network traffic flows through the br0 OVS bridge or additional brN bridges if configured.

Read the AHV Networking best practice guide for in-depth guidance on any settings not covered here.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3135

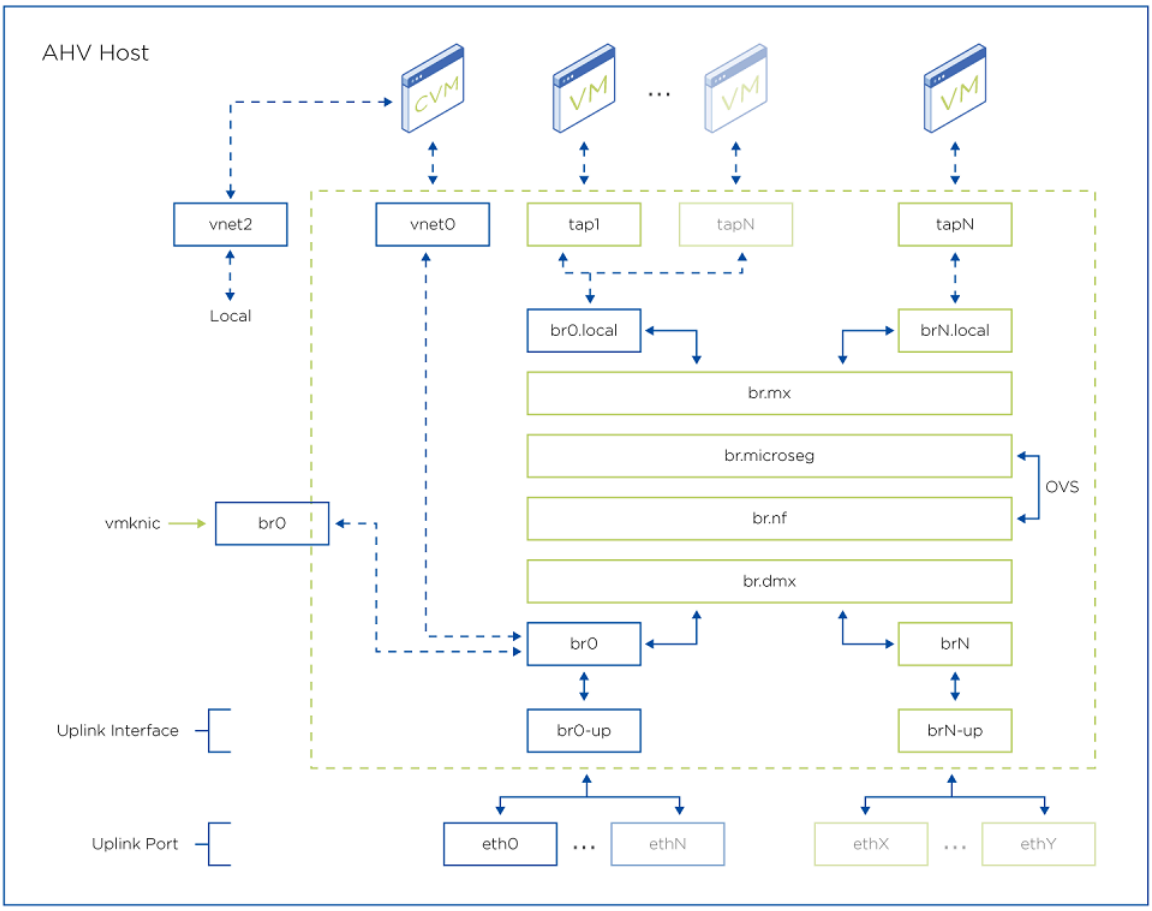


Figure 14: AHV Networking

The following list details the Nutanix best practices and requirements for edge site AHV networking:

- Use only the default bridge, br0, with at least two of the fastest network uplink adapters of the same speed to simplify the design.
  - › Converge the management, storage, and workload traffic on this single pair of uplink adapters.
- Only add additional brN bridges when you need a connection to a separate physical network. For example, if the top-of-rack switch has two pairs of switches—one pair for storage and management and another pair for workload traffic—it makes sense to create another bridge, br1, and place the workloads on this bridge.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3136

- Don't modify the configuration of any bridges inside the AHV host unless following an official Nutanix guide.
- To keep network configuration simple and reduce risk, use the standard 1,500-byte MTU in the hosts, CVMs, and workload VMs. Nutanix doesn't recommend jumbo frames unless specifically required by high-performance Nutanix Volumes iSCSI workloads or specific workload requirements.
  - When switching from 1,500-byte frames to 9,000-byte frames, performance improvements are generally not significant unless the workload uses the maximum network bandwidth for read traffic. For more information on when to use jumbo frames, see the Nutanix Volumes best practice guide and AHV Networking best practice guide.
- Connect at least one 10 Gbps or faster NIC to each tor switch to maintain high availability if one switch is lost.
- Use NICs from the same vendor within a bond to ensure compatibility and prevent undesired failover behavior.
- Use VLANs to separate logical networks. Physical hosts have a limited number of network ports and each port adds complexity. You can separate traffic logically without numerous physical ports.
- To simplify the design, use active-backup uplink load balancing.

vSphere Networking

VMware vSphere networking follows many of the same design decisions as AHV networking. Nutanix hosts with vSphere ESXi use two virtual switches (vSwitches), named vSwitchNutanix and vSwitch0. vSwitchNutanix is the internal, standard vSwitch used for management and storage traffic between the CVM and the hypervisor. vSwitch0 is also a standard vSwitch by default, used for communication between CVMs and workload traffic.

The critical design choices for vSphere networking are covered here, and you can refer to the VMware vSphere Networking best practice guide for more details.

The following list details the Nutanix best practices and requirements for edge site vSphere networking:

- Don't modify vSwitchNutanix.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3137

- Convert vSwitch0 to the virtual distributed switch (VDS) following the instructions in Migrate from a Standard Switch to a Distributed Switch. Converting to the VDS allows you to centrally manage networking for all hosts, instead of configuring each host network individually. The VDS also enables advanced networking functions such as load-based teaming, LACP, and traffic shaping.
- To simplify the design, connect at least two of the fastest adapters of the same speed to vSwitch0 and use the **Route Based on Physical NIC Load** load balancing method to ensure that traffic is balanced between uplink adapters.
  - › Connect these adapters to two separate top-of-rack switches to ensure redundancy.
- Connect at least one 10 Gbps or faster NIC to each top-of-rack switch to maintain high availability if one switch is lost.
- Don't add more vSwitches unless you need to connect to another physical network to meet security or workload requirements.
- All CVM storage, hypervisor host, and workload traffic should flow through vSwitch0, using VLANs to separate the workload traffic and all other traffic.
- Use the default 1,500-byte frame size on all uplinks unless there is a specific performance or application requirement that justifies 9,000-byte jumbo frames.

Virtualization Layer Design

This section describes technical design considerations for Nutanix AHV and VMware ESXi.

Nutanix AHV

AHV delivers virtualization capabilities for the most demanding workloads, and provides an open platform for server virtualization, network virtualization, security, and application mobility. When combined with comprehensive operational insights and virtualization management from Prism and Prism Central, AHV provides a complete datacenter solution.

Nutanix AHV has built-in VM high availability (VMHA) and a resource contention avoidance engine called Acropolis Dynamic Scheduling (ADS). ADS is always on and doesn't require any manual tuning. There are two main levels of VMHA for AHV: best

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3138

effort (no node or memory reservations required) and guarantee (some memory reserved on each node to enable failover). Use the guarantee level for VMHA in production environments and best effort in test and development environments. For additional information, see the Virtual Machine High Availability tech note.

Like VMware's Enhanced vMotion Capability (EVC), which allows VMs to move between different processor generations, AHV determines the lowest processor generation in the cluster and constrains all QEMU domains to that level. This feature enables you to mix processor generations in an AHV cluster and to live-migrate between hosts.

VMware vSphere

If you use vSphere in your enterprise edge deployment, deploy a highly available vCenter instance with an embedded Platform Services Controller to manage the ESXi-based Nutanix clusters. Nutanix upgrade automation features, such as one-click upgrades and LCM, require the advanced control features that vCenter provides. You also need vCenter Server to create and manage the VMware vSphere cluster responsible for the Distributed Resource Scheduler (DRS) and HA, and Prism Central to manage the Nutanix components.

> **Note:** If you're using the disaster recovery runbook automation feature, you need to deploy separate vCenter and Prism Central instances in each region or availability zone.

EVC allows VMs to move between different processor generations in a cluster. EVC mode is a manually configured option, unlike the corresponding feature in AHV. Enable EVC at cluster installation to help ensure that future node additions are seamless. Set EVC mode to the highest compatibility level the cluster processors support.

VMware HA and DRS are core features you should use in your edge site design. Nutanix best practices specify a few HA and DRS configuration changes from the default:

- Enable HA to automatically restart VMs in case of node failure.
- Enable DRS with the default automation level so that it can move VMs as needed to ensure optimal performance.

  > **Note:** Moving VMs may temporarily affect Nutanix data locality.

- Configure **DAS.IGNOREINSUFFICIENTHBDATASTORE** if one Nutanix container is presented to the ESXi hosts to eliminate false positives when a cluster uses a single datastore.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3139

- Disable automation level, HA, and DRS for all CVMs. HA doesn't need to reserve resources for CVMs because they're bound to a single node and can't be restarted elsewhere in the cluster.
- Set Host failures cluster tolerates to **1** for replication factor 2 and **2** for replication factor 3. These settings ensure that the proper resources are automatically reserved for the cluster.
- Set the host isolation response to **Power off and restart VMs** to ensure that VMs are moved to a healthy host and continue to function.
- Set the host isolation response to **Leave powered on** for CVMs. You don't want CVMs to be turned off if there's a transient network disruption.
- Disable Storage I/O Control. If Storage I/O Control is enabled, it can cause storage unavailability, unnecessary lock files, and complications with Metro Availability.

Management Layer Design

Prism Central

There are two deployment architectures for Prism Central that you can use and scale depending on the size and goals of the design:

1. Single-VM Prism Central: One instance in each region or availability. Required if you use the disaster recovery runbook automation feature, which requires that the source and target sites have separate Prism Central instances controlling them. Requires additional cluster resources to run the required VMs.
2. Scaled-out Prism Central cluster: Three-VM cluster. Increases management plane availability and the total number of objects you can manage. Requires additional cluster resources to run the required VMs.

We recommend deploying the scaled-out Prism Central instance for edge sites to simplify capacity planning, platform lifecycle management, and virtual networking management, and to reduce management overhead.

VMware vCenter Server

You can deploy vCenter in many different sizes, and the size ultimately determines how large an environment you can support in terms of VMs, hosts, and clusters. Refer to the

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3140

official VMware documentation for the version you're deploying to determine the proper size for your design.

You can deploy vCenter as a single VM or as a vCenter High Availability (vCenter HA) instance. vCenter HA doesn't increase the size of the environment it can manage because a single virtual appliance is active at any time. The size of the environment that can be managed is based on the size of the VMs deployed.

We recommend deploying one instance of vCenter HA for all workloads and configuring it with Platform Services Controller embedded.

Dependent Infrastructure

There are a variety of other infrastructure services that are necessary for a successful Nutanix deployment, such as NTP, DNS, and AD. You may already have these infrastructure services deployed and available for use when you deploy your Nutanix environment, but if you don't, you need to deploy them as part of the new environment.

NTP

If clock times drift too far apart, some products may have trouble communicating across layers of the solution. Network Time Protocol (NTP) synchronizes computer clock times including network, storage, compute, and software.

The following list details the Nutanix best practices and requirements for NTP for edge sites:

- Configure at least three NTP servers (NTP standard recommendation is five to detect rogue time sources) and ensure that they're accessible at all solution layers, including AOS, AHV, and Prism Central, plus vCenter and ESXi if you're using vSphere.
- Use the same NTP servers for all infrastructure components.
- Don't use an AD domain controller as an NTP source.
- If you're in a dark site with no internet connectivity, use a switch or GPS time source.
- Configure NTP sources specific to the region where the edge clusters reside.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3141

DNS

Domain Name System (DNS) is a directory service that translates domain names of the form domainname.ext to IP addresses. DNS ensures that all layers can resolve names and communicate.

We recommend configuring at least two DNS servers and making them accessible at all layers (AOS, Prism Central, ESXi, vCenter, and network switches) to ensure that components can reliably resolve addresses at all times. We also recommend configuring DNS sources specific to the region where the edge clusters reside.

Active Directory

Active Directory (AD) often serves as the authoritative directory for all applications and infrastructure in an organization. For this design, all the consoles and element managers use RBAC and use AD as the directory service for user and group accounts. Where possible, use AD groups to assign privileges for easier operations. You can then control user access by adding or removing a user from the appropriate group.

Logging Infrastructure

Capturing logs at all layers of the infrastructure is very important. If there is a security incident, logs can be critical for forensics. An example of a robust log collector is Splunk, but there are other options.

The following list details the Nutanix best practices and requirements for logging infrastructure in edge sites:

- Deploy a robust logging platform that meets your security requirements.
- Forward all infrastructure logs to the centralized log repository.
- Store the logs in a different cluster, or location, from where you collect them. This measure protects the logs in case of a catastrophic cluster failure, ensuring they can later be used for forensics.
- Ensure that AD sites and services are set up to define a replication and authentication topology if connectivity to the datacenter is lost.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3142

Security Layer Design

You can build private or multitenant solutions on the Nutanix Cloud Platform, so the security responsibilities vary based on the use case. The security approach includes multiple components:

- Physical
- Virtual infrastructure
- Threat vectors
- Workloads

We designed Nutanix infrastructure to deliver a high level of security with less effort. Nutanix publishes custom security baseline documents for compliance, based on United States Department of Defense (DoD) RHEL 7 Security Technical Implementation Guides (STIGs) that cover the entire infrastructure stack and prescribe steps to secure deployments in the field. The STIGs use machine-readable code to automate compliance against rigorous common standards.

Nutanix provides SCMA by default. SCMA checks multiple security entities for both Nutanix storage and AHV, and Nutanix automatically reports inconsistencies and reverts them to the baseline. With SCMA, you can schedule the STIG to run hourly, daily, weekly, or monthly. The STIG has the lowest system priority in the virtual storage controller, ensuring that security checks don't interfere with platform performance.

In addition, Nutanix releases Security Advisories that describe potential security threats and their associated risks plus any identified mitigations or patches. For more detailed information on Nutanix security and compliance features, see the following documents, separated by category:

- Networking: Flow Network Security tech note
- Information: Information Security tech note
- Cloud: Nutanix DRaaS Security tech note
- Database: Nutanix Era Security tech note

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3143

Authentication Best Practices

- Maintain as few user and group management systems as possible. A centrally managed authentication point is preferred to many separately managed systems.
- You should at least take advantage of the external LDAP support provided by Nutanix components.
- Use AD authentication for user and server accounts to ensure that user activity logged for auditing purposes and account security is configured and maintained from a single centralized solution.
  - › You must have a highly available AD infrastructure and network connection to the datacenter.
- Use an SSL or TLS connection to AD to eliminate cleartext exchanges on the network.

Certificate Best Practices

- Protect all consumer-facing components with certificates signed by a trusted certificate authority to provide an extra layer of security and prevent meddler-in-the-middle (MITM) attacks.
  - › You can use internally or externally signed certificates based on your consumer classification and the service the specific component provides.

Cluster Lockdown Best Practices

Don't use Nutanix or vSphere cluster lockdown (feature that lets you enforce SSH access to CVMs and host using key pairs instead of passwords) unless you require passwordless communication. This decision helps restrict direct access to the CVM and hypervisor to as few entities as possible.

Hardening Best Practices

- Enable Advanced Intrusion Detection Environment (AIDE) for the CVM and AHV. AIDE performs checksum verification for all statis binaries and libraries for improved security.
- Enable stack traces for cluster issues for AHV or ESXi and the CVM.
- Enforce a complex password policy (at least 15 characters long with at least 8 different characters) for the hypervisor and CVM.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3144

- Enable a banner for AHV or ESXi and the CVM that retrieves a specific sign-in message via SSH.
- Enforce only SNMPv3 on the CVM.
- Configure SCMA to run hourly to capture unacceptable configuration drift.
- ESXi only: Stop unused services and close unused firewall ports to limit the attack surface.

  Note: Ensure that you don't stop a service or close a firewall port that's required by Nutanix, such as SSH and NFS.

- Generally, we recommend following the Hardening Controller VM section of the AOS Security Guide. If you're using AHV, follow the Hardening AHV section of the AOS Security Guide.

Internet-Facing Services Best Practices

We recommend using multiple internet connections (active-backup) and ISP-provided denial-of-service (DoS) and distributed-denial-of-service (DDoS) filtering to help mitigate the potential effects of a DoS or DDoS attack.

Logging Best Practices

- Configure and maintain a single centralized logging solution for auditing purposes and account security.
- Send log files to a highly available syslog infrastructure.
- At least one of the individual targets of the highly available logging infrastructure should run outside the virtual infrastructure itself so that if the virtual infrastructure is compromised, forensic investigations can access logs that might not be available on the cluster itself.
- Include data from all Nutanix modules and components in logging using the error-log level and ensure that they're searchable. See the Configuring the Remote Syslog Server Settings section of the Acropolis Advanced Administration Guide for more information.
- Use default ESXi logging levels, log rotation, and log file sizes.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3145

- If you have additional security and reliability requirements, use TCP for log transport. Otherwise, use the default syslog protocol, UDP.
- Use port 514 (defined port in syslog RFC) for logging.

Network Segmentation Best Practices

- To protect Nutanix CVM and hypervisor traffic, place them together in their own dedicated VLAN, separate from other VM traffic. This configuration applies to all hosts in a cluster or single node.
- Place out-of-band management on a separate VLAN or physical network to provide additional security.
- We recommend configuring the CVM and hypervisor host VLAN as a native, or untagged, VLAN on the connected switch ports to allow easy node addition and cluster expansion.
- Don't segment Nutanix storage and replication traffic, or iSCSI Volumes traffic, on separate interfaces (VLAN or physical) unless additional segmentation is required by mandatory security policy or the use of separate physical networks.

Role-Based Access Control (RBAC) Best Practices

- Use a least-privilege and separation-of-duties approach when assigning RBAC permissions to ensure that each group or individual user has just enough permissions to perform their duties. Use predefined roles or create new roles as needed.
- Configure RBAC at the Prism Central level because it provides the overlying management construct. This configuration ensures that your least-privilege configuration stays in place and avoids common mistakes that occur when RBAC is configured at multiple different levels.
- Align RBAC structure and default plus custom roles with your company requirements.

Data-at-Rest Encryption Best Practices

> **Note:** AHV encrypts the entire Nutanix cluster, while ESXi gives you the option to define encryption on a per-Nutanix-container basis if required.

- Keep management traffic, including storage traffic, on a separate network.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3146

- Don't use storage encryption.
- Don't use a key management server (KMS).

> **Note:** All methods of DaRE are FIPS 140-2 compliant. However, if you require levels 2, 3, or 4, you also need a hardware component.

Microsegmentation and Firewall Best Practices

- Use Flow Network Security (previously Flow Microsegmentation) to comply with regulatory and business-specific compliance policies such as PCI-DSS, HIPAA, and NIST.
- Use a Palo Alto Networks VM-Series firewall with Flow Network Security to provide advanced threat and vulnerability detection for layers 4–7.

For more information on Flow Network Security, see the Flow Network Security software documentation and the Flow Network Security tech note. For additional information on deploying the Palo Alto VM-Series on AHV, see the Palo Alto Networks VM-Series Firewalls on Xi tech note and the Nutanix and Palo Alto Networks Service Chain Integration Guide.

Automation Layer Design

Nutanix supports intelligent IT operations and advanced automation that enable you to streamline operations, enable IT as a service, and support the needs of developers and business teams. This section covers virtual infrastructure automation and orchestration, focusing on provisioning and maintenance.

Life Cycle Manager (LCM)

Nutanix LCM determines any software and firmware dependencies, intelligently prioritizes updates, and automates the entire upgrade process across all clustered hosts, without any impact to applications or data availability. It supports one-click upgrades across multiple qualified hardware manufacturers and configurations, so IT teams have the flexibility to deploy the best hardware for each use case and still benefit from centralized upgrade capabilities.

LCM offers the best software and firmware upgrade experience for clusters with three or more nodes. In this design, the nodes can locally coordinate data synchronization,

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3147

VM evacuation and migration, and node recovery and availability during the upgrade process for the firmware and software on the individual nodes. The individual nodes might restart multiple times, and that entire process is automated through LCM without affecting applications and data.

Certain LCM features aren't supported when your cluster contains one or two nodes:

- In a one-node scenario, the LCM software and firmware upgrades aren't supported because there's no hardware redundancy. In this design, the user must plan their downtime and trigger the software upgrade manually via Prism or use the respective hardware manufacturer's management tools.
- In a two-node scenario, LCM software and firmware is supported, but during the upgrade process, data synchronization across nodes takes more time because there's only one other node in the cluster to absorb the changes. You must complete witness upgrades separately from data-carrying node upgrades. For this reason, we recommend a larger maintenance window for two-node clusters.

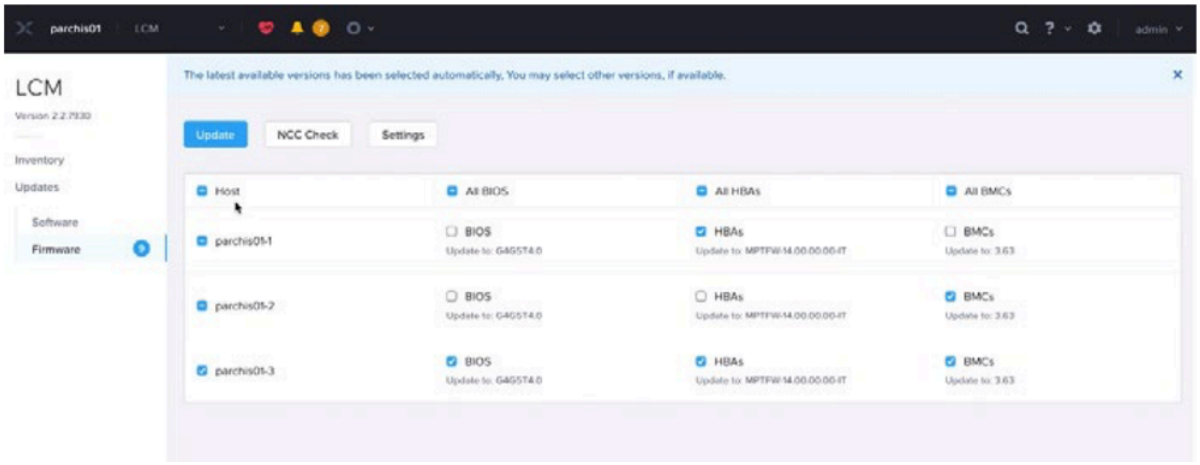


Figure 15: Life Cycle Manager

Foundation

Foundation manages the initial setup and configuration of a cluster. Nutanix nodes can come with AHV and the CVM preinstalled, and with Foundation you can:

- Add the nodes to an existing Nutanix cluster.
- Create a new Nutanix cluster.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3148

- Reimage the nodes with different a AHV and or AOS version or different hypervisor and create a Nutanix cluster.

  Note: The Foundation process may vary for different hardware vendors.

  Nutanix provides a Foundation preconfiguration service that you can install from nutanix.com. With the service, you can define and download the Nutanix cluster configuration to be used during the Foundation process. The downloaded file contains all configuration required to perform the Foundation operation and comes in json format, which makes it easy to keep track of configurations, document them, and share with your peers.

  See the Field Installation Guide for the functions available for the different Foundation software options.

Foundation Central

Foundation Central enables you to create clusters from factory-imaged nodes and reimage existing nodes that are already registered with Foundation Central remotely from Prism Central. This feature enables you to create clusters on remote sites without having to arrange a personnel visit.

Foundation Central has the following limitations:

- Foundation Central supports creation of a one-node cluster without imaging on factory-shipped nodes with AOS and any hypervisor installed.
- Foundation Central supports creation of a one-node cluster with imaging only on nodes that are shipped with DiscoveryOS installed.
- Imaging logs for the remote nodes aren't available on Prism Central. You can only access these logs in the nodes.
- Foundation Central doesn't support updating the CVM memory and hostname for one-node cluster creation without imaging.

Nutanix Calm

Calm provides infrastructure and application automation and life cycle management for the Nutanix enterprise cloud and public clouds. It provisions, scales, and manages infrastructure and applications across multiple environments to make the entire IT infrastructure more agile and application-centric. Building an enterprise or service

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3149

provider cloud solution with Nutanix Calm helps organizations with delivery and ongoing management of infrastructure, applications, and custom services, leading to lower opex.

We recommend reviewing the Nutanix Calm Reference Architecture guide for further information on implementing Nutanix Calm

Operations Design

Note: We recommend purchasing the Nutanix Cloud Manager (NCM) Starter license, which gives you access to analytics, capacity planning, custom dashboards, and playbooks for Prism Central.

Native runway calculations built into Prism Central automatically calculate the remaining capacity of the system as soon as the Prism Element instance is brought under Prism Central management. Configure these runway calculations to run as part of periodic reports and review them on a regular basis (at least monthly) to ensure that sufficient capacity exists. This configuration is especially important for organizations that have a significant lag between when they commit to purchase additional gear and when the gear is online and available to use.

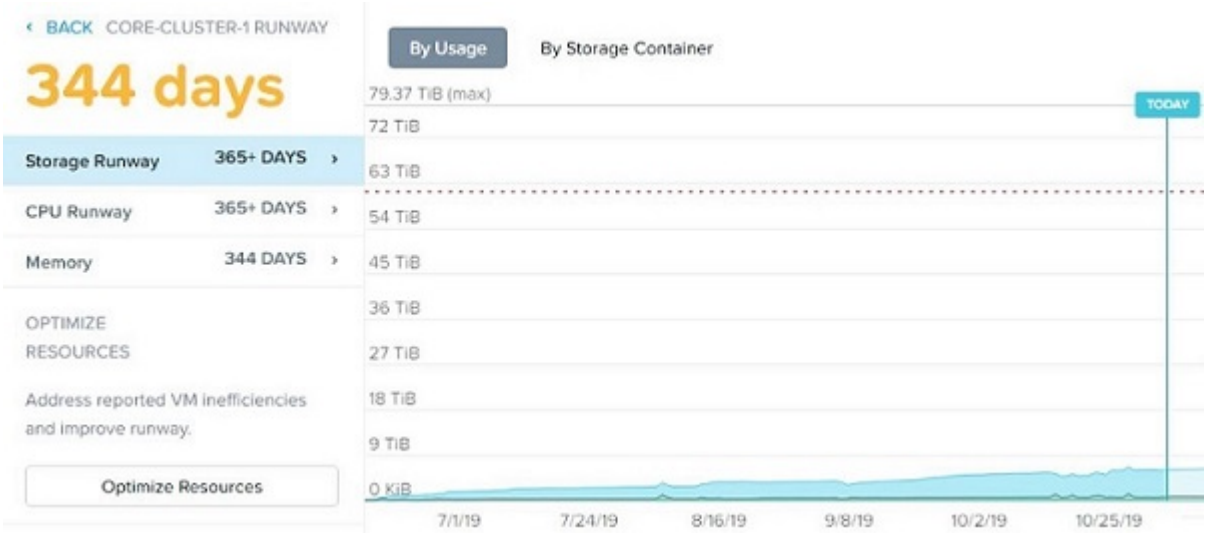


Figure 16: Capacity Runway

Accurate and efficient system-level planning requires accurate sizing for individual workloads. Machine learning in Prism Central provides anomaly detection for VMs when the workload crosses learned thresholds. The system also categorizes VMs based on their behavior, and you can create custom alert policies that match VMs by conditions.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3150

Operations Best Practices and Requirements

- Review capacity planning monthly.
- Perform updates after hours for performance- or migration-sensitive applications to reduce the load on the system.
- Use the latest supported release.
- Update to the next maintenance version four weeks after release and to the current patch version two weeks after release to keep updates relatively small.
- Maintain a preproduction environment to test any necessary changes to firmware, software, or hardware before implementing the change in production. Preproduction environments can help you avoid the cost of outages.
- Configure alerts and alert policies in Prism Central, not Prism Element, to create consistency across multiple clusters and reduce the effort involved in making multiple changes. Prism Central–based alert policies also allow you to detect anomalies.
- Use SMTP for alert transmission to create consistency across multiple clusters, reduce the effort involved in making multiple changes, enable anomaly detection, and offer more options for delivery.

BCDR Design

Nutanix provides a range of data protection features. Our general recommendation for BCDR design is: If an application has native data protection mechanisms (Exchange database availability groups (DAG), SQL Server Always On, Oracle RAC), use those to provide application BCDR. If an application doesn't provide a data protection mechanism, use the built-in Nutanix protection mechanisms.

Consult the Multi-Datacenter Design for Nutanix Core and BC/DR section of the Nutanix Hybrid Cloud Reference Architecture for considerations and strategies for multi-datacenter designs.

BCDR Logical Implementations for Edge Sites

Disaster recovery patterns for edge sites vary from organization to organization, but one-to-one and many-to-one implementations are the most common.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3151

One-to-One

For smaller environments with only a pair of locations, protect applications between two availability zones in the same region or across regions. You can protect the same workload or application with different RPO thresholds. The availability zone location you choose (same region or across regions) defines the RPO value for the protected application or workload: If an application or workload requires RPO 0, choose availability zones in the same region (latency requirement for RPO 0 is 5 ms RTT or less).

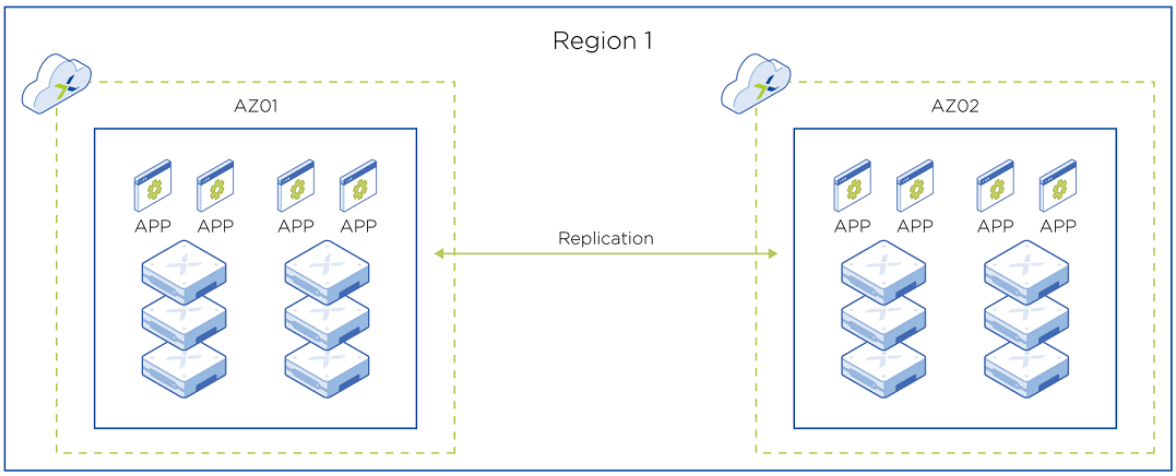


Figure 17: Two Availability Zones in the Same Region

Many-to-One

The many-to-one pattern maps multiple source edge clusters to single disaster recovery target Nutanix cluster or core datacenter. In the most common configuration, each edge location is a separate availability zone that replicates data to the disaster recovery hub, which is located in a separate availability zone in the same region.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3152

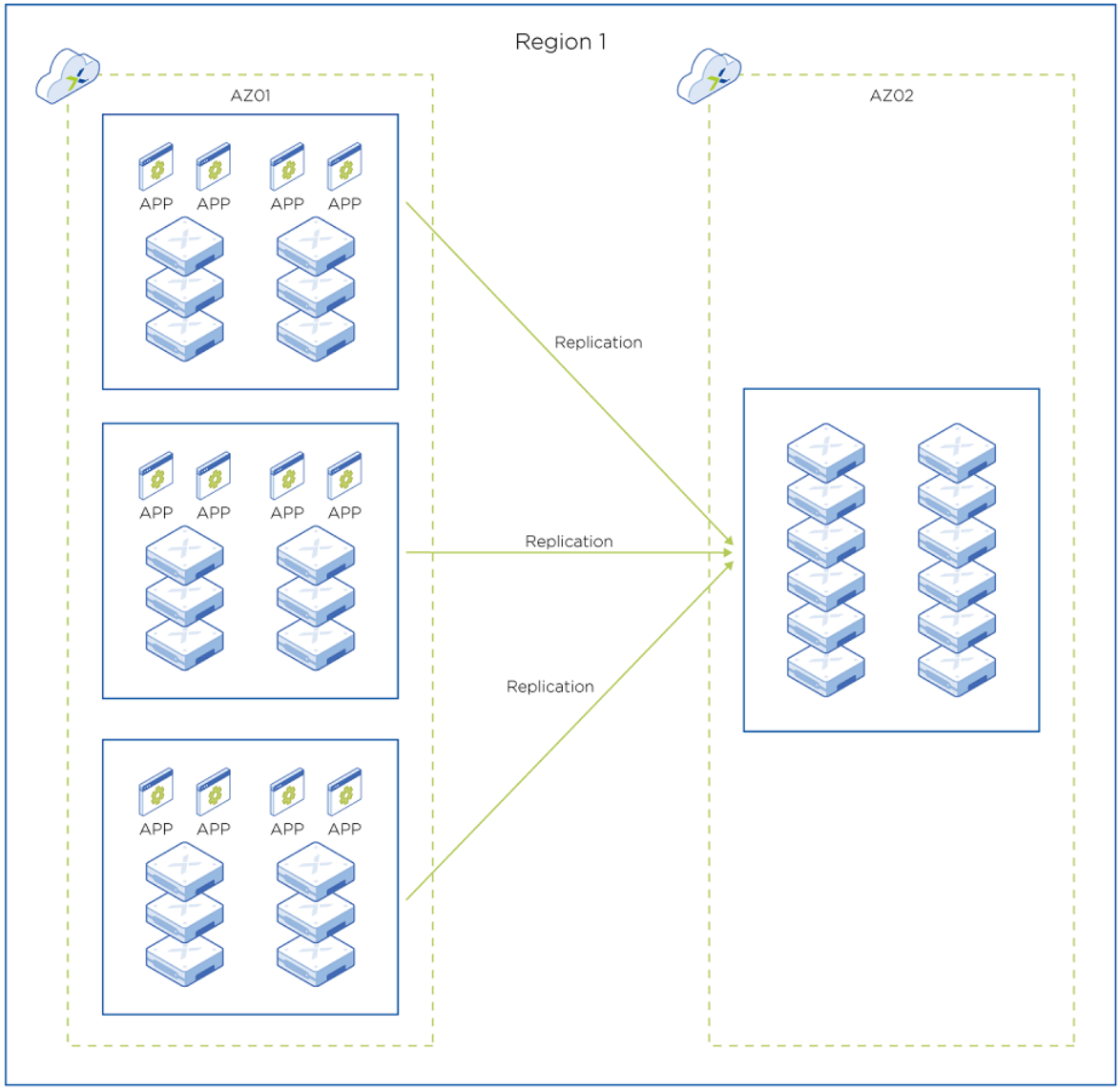


Figure 18: Multiple Availability Zones in a Single Region

You can also have multiple availability zones across multiple regions.

© 2024 Nutanix, Inc. All rights reserved

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3153

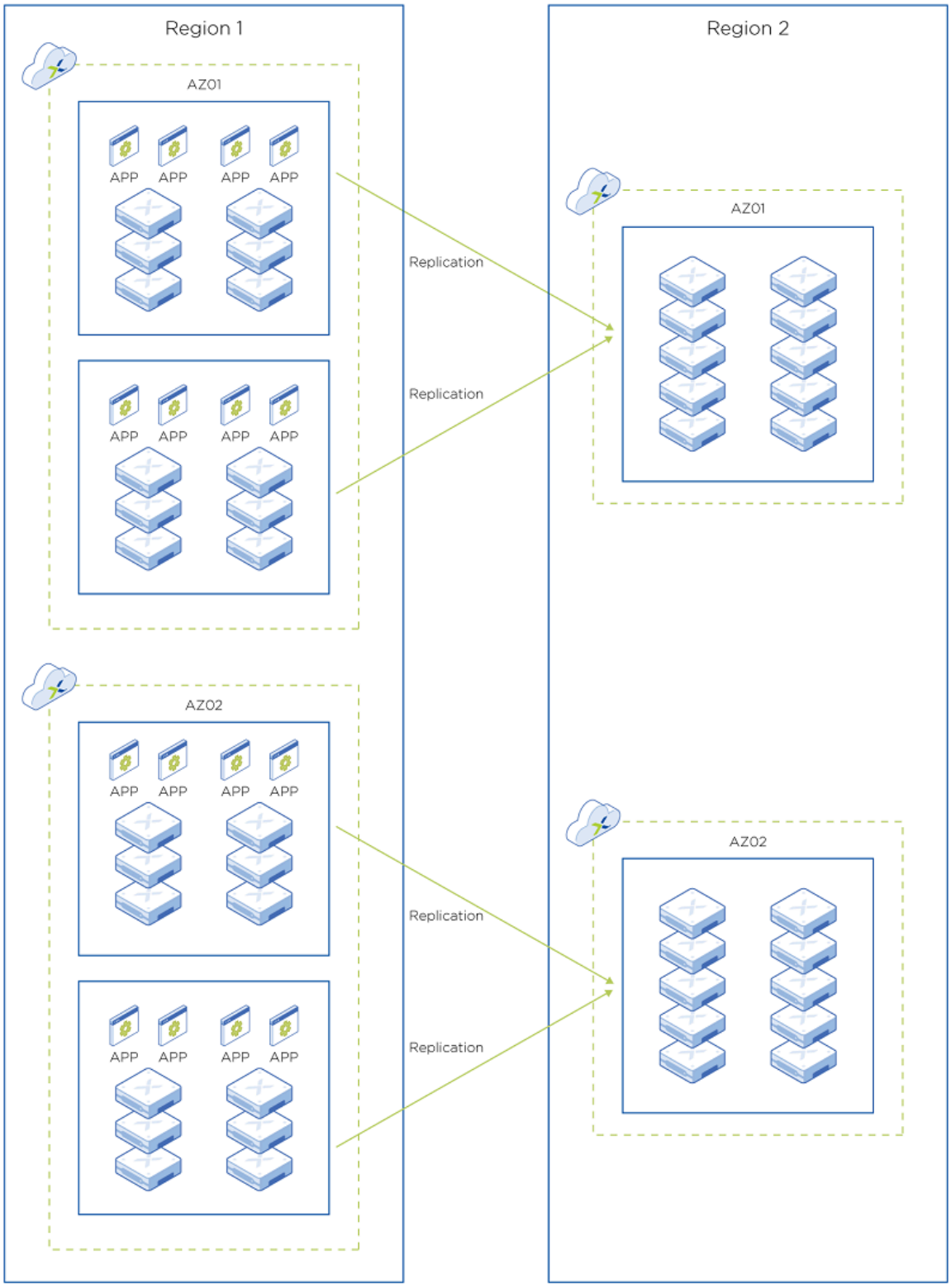


Figure 19: Multiple Availability Zones across Multiple Regions

© 2024 Nutanix, Inc. All rights reserved |

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3154

Note: Consult the Nutanix Hybrid Cloud Reference Architecture to evaluate other implementations.

Nutanix BCDR Solutions

A good disaster recovery solution involves different levels of service because applications have different levels of criticality to the business and therefore different disaster recovery requirements. For this reason, this document includes multiple architectures for a variety of scenarios. The following flow chart walks through the decision tree for choosing the best Nutanix disaster recovery solution for your requirements.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3155

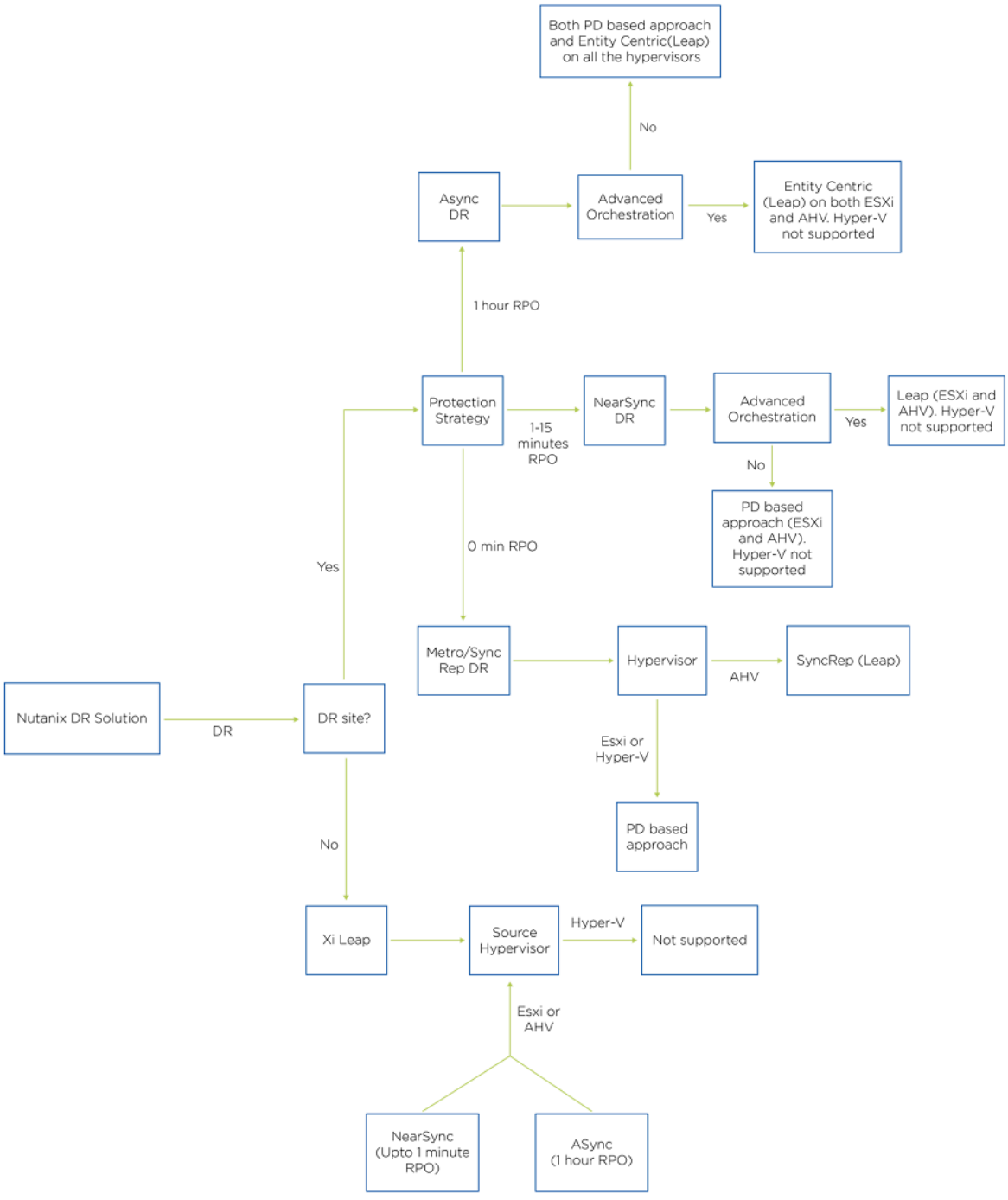


Figure 20: Disaster Recovery Decision Flowchart

© 2024 Nutanix, Inc. All rights reserved

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3156

1. Nutanix Metro Availability
   a. Pros: Can provide zero data loss (RPO 0), minimal to zero recovery time (RTO 0), and RTO 0 during a disaster recovery avoidance event.
   b. Cons: Requires stretched layer 2 networking of some form between edge sites or within the Edge site, requires a Nutanix Cloud Infrastructure Ultimate license, is only supported with ESXi, and is highly dependent on the network connectivity being resilient and providing a high enough throughput to accommodate application change rates.
   c. See the Metro Availability best practice guide on the Nutanix Support Portal for more information.
2. Synchronous replication
   a. Pros: Available with Nutanix AHV or VMware vSphere. Protects workloads with RPO 0. Used when you can't provide spanned L2 across datacenters but still need to provide RPO 0 to applications.
   b. Cons: Requires high bandwidth and low latency, requires a Nutanix Cloud Infrastructure Ultimate license or an advanced replication add-on license, only supported with Nutanix Disaster Recovery (previously Leap), and requires that the source cluster have more than three nodes.
3. NearSync replication
   a. Pros: Provides an RPO between 1 and 15 minutes to storage-intensive workloads over limited connectivity.
   b. Cons: Capacity of each SSD in the cluster must be at least 1.2 TB, only supported with Nutanix Disaster Recovery, requires a Nutanix AOS Enterprise license or a Leap Advanced Add-On license, and requires that the source cluster have more than three nodes.
4. Asynchronous replication
   a. Pros: Provides an RPO of one hour or more to applications using low-bandwidth, high-latency datacenter links.
   b. Cons: Requires a Nutanix AOS Enterprise license or Leap Advanced Add-On License and requires that the source cluster have more than three nodes.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3157

General BCDR Best Practices and Requirements

- Keep as few VMs per protection domain as possible in your design.
  - › If you're using asynchronous replication, configure at most 200 VMs per protection domain.
  - › If you're using NearSync replication, configure at most 10 VMs per protection domain.
- Group VMs with similar RPO requirements in the same protection domain.
  - › Node size and capacity can limit the possible RPO for the VMs running on it. See the Resource Requirements Supporting Snapshot Frequency (Asynchronous, NearSync and Metro) section of the Data Protection and Recovery with Prism Element guide for details.
- Put NearSync VMs in their own protection domains (NearSync can only have one schedule).
- Limit consistency groups to fewer than 10 VMs.
- Only use consistency groups for applications with a shared state, such as database replicas.
- Only add one VM to any consistency group that uses application-consistent snapshots.
- Configure snapshot intervals to be shorter than your desired RPO to allow for failure and recovery without manual intervention. The interval should be half your desired RPO including data transmission timing.
- Configure snapshot schedules to retain the minimum number of snapshots needed to meet your retention policy.
- If you're using synchronous replication, create one container on the source and one on the destination with the same name.
- If you're using synchronous replication, ensure that the two participating clusters are within 5 ms round trip time (RTT) of each other.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3158

- Use Metro Availability for business-critical applications that require zero data loss (RPO 0), minimal to zero recovery time (RTO 0), or RTO 0 during a disaster recovery avoidance event.
  - › Metro Availability is only supported with ESXi.

For additional details, see the Data Protection and Recovery with Prism Element guide on the Nutanix Support Portal.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3159

6. Optional Nutanix Products and Services

Nutanix offers optional products and services that you can choose to incorporate when implementing enterprise edge solutions on the Nutanix platform. These options can help you quickly satisfy unique organizational requirements.

- Nutanix Cloud Manager: NCM Starter and Pro licenses add to the base capabilities of Nutanix Prism to provide monitoring, analytics, and automation capabilities from a single management interface.
- Nutanix Cloud Clusters (NC2): NC2 extends the Nutanix stack to the public cloud, creating a single management domain that spans private and public clouds and removes the friction from multicloud operations. For more information, see the Nutanix Cloud Clusters on AWS tech note and the Disaster Recovery with Nutanix Cloud Clusters (NC2) on AWS tech note.
- Flow Network Security: Microsegmentation and other capabilities offered by Flow Network Security further enhance the security of your Nutanix operations.
- Nutanix Files: Files enables Nutanix clusters with full-featured file services capabilities, eliminating the need for standalone NAS appliances or file servers.
- Nutanix Objects: Objects enables a Nutanix cluster to provide S3-compatible, software-defined, scale-out object stores for a variety of use cases, eliminating the need for standalone object storage while supporting applications that rely on object stores with an on-premises alternative.
- Nutanix Mine: Mine is an integrated backup solution that combines the benefits of the Nutanix architecture with the capabilities of proven backup vendors.
- NCM Self-Service: NCM Self-Service (previously Calm) provides application-level orchestration and lifecycle management, simplifying application management and enabling self-service.
- Karbon: Karbon integrates certified Kubernetes with the Nutanix operating environment, enabling Nutanix clusters to support both VM- and container-based applications while simplifying Kubernetes deployment and management.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3160

7. Conclusion

The Nutanix Cloud Platform remains a common platform for both traditional datacenters and enterprise edge sites. This document is intended to demonstrate valuable methods and practices that organizations, both large and small, can use to implement Nutanix solutions to solve their IT and business problems. There is no one-size-fits-all solution for enterprise edge deployments; this document is only intended to provide customers with suggested best practices they can use to design and evolve their private, hybrid, and multicloud solutions.

For more information on any details of this document, please visit our website at www.nutanix.com or reach out to our sales team. You can also contact one of the many global support phone numbers listed on our website. For feedback or questions, please contact us using the Nutanix NEXT Community forums.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3161

8. Appendix

Best Practices for Enterprise Edge Sites

High-Level Design Best Practices

- Logically group the manageability, replication, and BCDR components of your edge sites in a single region or availability zone.
- Use Prism Central as the primary control plane.
  - › If you use ESXi, you also need VMware vCenter.
- Use the simplified block-and-pod architecture detailed in the Block and Pod Architecture section of the Nutanix Hybrid Cloud Reference Architecture.
  - › Large-scale sites (more than four blocks with the expectation of additional blocks in the future) with the characteristics of a datacenter should reference the Nutanix Hybrid Cloud Reference Architecture.
- Build clusters with one or three nodes.
  - › If you need to be able to scale your edge solution beyond two nodes or add storage-only nodes to the cluster, you should implement a three-node cluster.
- If you use them, deploy storage-only nodes in pairs.
  - › You can only use storage-only nodes in clusters with three or more nodes.
- Define an SOP that stipulates how to scale one- or two-node clusters in your design, as this step isn't a function of the core AOS and doesn't have a workflow.

Software Best Practices

Use the following software versions:

- Prism Central: pc.2020.7
- Nutanix AOS 5.20

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3162

- Nutanix AHV 5.15
- VMware vSphere 6.7 or 7.0
- VMware vCenter 6.7 or 7.0

Failure Domain Best Practices

- Design and deploy the management plane to be highly available.
- At a minimum, design to meet the availability requirements of the managed workload or service with the highest uptime requirement.
- Confine workload domain to a single edge site.
- Confine workloads domain to a defined security zone.
- Ensure that the API gateway is always available because other third-party integrations (such as the backup vendor integration) may rely on it.
- Configure built-in RBAC to restrict access to management platform resources.
- Design your management plane to reside in the region or location where your edge clusters reside.
- Use redundant power from two different power supplies.
- Use redundant top-of-rack switches.
- Ensure redundant upstream connectivity to top-of-rack switches from each Nutanix node.
- Ensure redundant connectivity from edge to central datacenter.
- Use Nutanix scale-out architecture and data protection capabilities to replicate data to a second Nutanix cluster if one cluster fails.
- Deploy the application across multiple clusters.
- Use an independent and redundant cooling system for each datacenter room.
- Ensure redundant networking connectivity from different providers between datacenter buildings.
- Ensure redundant internet connectivity from different providers.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3163

- Where possible, use multiple buildings and server rooms in separate buildings or campuses so that the failure of a single server room doesn't affect production. Distribute multicomponent services equally across datacenter server rooms.
- Ensure strict SLA compliance and keep well-documented resources and processes to help keep MTTR short.

General Networking Best Practices

- Configure IPMI, iLO, or iDRAC server-facing ports in the management network as access ports and don't use VLAN trunking for these ports. Restrict access to this critical management network.
- Never use these switches for Nutanix deployments:
  - Cisco Nexus 2000 (Fabric Extender)
  - 10 Gbps expansion cards in a 1 Gbps access switch
- In small edge sites running a handful of VMs, use a simple network topology consisting of a pair of top-of-rack switches interconnected to a firewall and router.
- In medium and larger deployments with multiple racks, use a leaf-spine topology because it's easy to scale, achieves high performance with low latency, and provides resilience.
- Ensure that every Nutanix node in a cluster is in the same layer 2 broadcast domain and shares the same IP subnet.
- You can populate nodes designed exclusively for edge or ROBO with 1 Gbps networking for one- and two-node clusters with latency spikes of approximately 6–8 ms.
  - Limit your cluster size to at most eight nodes if you plan on using 1 Gbps networking.
- Ensure that when there are two or more nodes in a cluster, each layer of the network topology is highly available and tolerates individual device failures.
  - Avoid configurations or technologies that don't maintain system availability during single-device outages or upgrades, such as stacked switches.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3164

- Ensure that there are no more than three switches between any two Nutanix nodes in the same cluster.
- Don't use WAN or remote links between Nutanix nodes in the same Nutanix cluster.
- Separate Nutanix CVM and hypervisor hosts in a dedicated VLAN that doesn't include any VM traffic.
- Don't place Nutanix nodes in the same Nutanix cluster if the stretched layer 2 network spans multiple edge sites, buildings, datacenters, or availability zones or if there's a remote link between the two locations.
  - › Using a stretched layer 2 network over a layer 3 network is only acceptable when the Nutanix cluster is in the same switch fabric or aggregation layer, such as when a layer 2 network stretches between two racks in the same datacenter.
- Don't use features like block or rack awareness to stretch a Nutanix cluster between different physical sites.
- Configure adequate uplinks between switches or interswitch links for east-west storage traffic to minimize port-to-port oversubscription. For example, use multiple 40 Gbps uplinks (or interswitch links).
- Connect hosts using redundant links.
- Configure switch ports facing Nutanix servers as spanning tree portfast or edge to skip the listening and learning phases and prevent cluster outages caused by changes to spanning tree topology.
- Configure the CVM and hypervisor VLAN as native, or untagged, on server-facing switch ports. Newly added nodes use untagged traffic for discovery and work out of the box, reducing manual server configuration.
- Use tagged VLANs on the switch ports for all guest workloads to keep the workloads separate from each other and from the CVM and hypervisor network.
- Reduce network oversubscription to ensure as close to a one-to-one ratio as possible. Dropped network packets or a congested network immediately affect storage performance.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3165

AHV Networking Best Practices

- Use only the default bridge, br0, with at least two of the fastest network uplink adapters of the same speed to simplify the design.
  - › Converge the management, storage, and workload traffic on this single pair of uplink adapters.
- Only add additional brN bridges when you need a connection to a separate physical network. For example, if the top-of-rack switch has two pairs of switches—one pair for storage and management and another pair for workload traffic—it makes sense to create another bridge, br1, and place the workloads on this bridge.
- Don't modify the configuration of any bridges inside the AHV host unless following an official Nutanix guide.
- To keep network configuration simple and reduce risk, use the standard 1,500-byte MTU in the hosts, CVMs, and workload VMs. Nutanix doesn't recommend jumbo frames unless specifically required by high-performance Nutanix Volumes iSCSI workloads or specific workload requirements.
  - › When switching from 1,500-byte frames to 9,000-byte frames, performance improvements are generally not significant unless the workload uses the maximum network bandwidth for read traffic. For more information on when to use jumbo frames, see the Nutanix Volumes best practice guide and AHV Networking best practice guide.
- Connect at least one 10 Gbps or faster NIC to each tor switch to maintain high availability if one switch is lost.
- Use NICs from the same vendor within a bond to ensure compatibility and prevent undesired failover behavior.
- Use VLANs to separate logical networks. Physical hosts have a limited number of network ports and each port adds complexity. You can separate traffic logically without numerous physical ports.
- To simplify the design, use active-backup uplink load balancing.

vSphere Networking Best Practices

- Don't modify vSwitchNutanix.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3166

- Convert vSwitch0 to the virtual distributed switch (VDS) following the instructions in Migrate from a Standard Switch to a Distributed Switch. Converting to the VDS allows you to centrally manage networking for all hosts, instead of configuring each host network individually. The VDS also enables advanced networking functions such as load-based teaming, LACP, and traffic shaping.
- To simplify the design, connect at least two of the fastest adapters of the same speed to vSwitch0 and use the **Route Based on Physical NIC Load** load balancing method to ensure that traffic is balanced between uplink adapters.
  - › Connect these adapters to two separate top-of-rack switches to ensure redundancy.
- Connect at least one 10 Gbps or faster NIC to each top-of-rack switch to maintain high availability if one switch is lost.
- Don't add more vSwitches unless you need to connect to another physical network to meet security or workload requirements.
- All CVM storage, hypervisor host, and workload traffic should flow through vSwitch0, using VLANs to separate the workload traffic and all other traffic.
- Use the default 1,500-byte frame size on all uplinks unless there is a specific performance or application requirement that justifies 9,000-byte jumbo frames.

Virtualization Best Practices

- If you're using the disaster recovery runbook automation feature, you need to deploy separate vCenter and Prism Central instances in each region or availability zone.
- Enable HA to automatically restart VMs in case of node failure.
- Enable DRS with the default automation level so that it can move VMs as needed to ensure optimal performance.

  Note: Moving VMs may temporarily affect Nutanix data locality.
- Configure **DAS.IGNOREINSUFFICIENTHBDATASTORE** if one Nutanix container is presented to the ESXi hosts to eliminate false positives when a cluster uses a single datastore.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3167

- Disable automation level, HA, and DRS for all CVMs. HA doesn't need to reserve resources for CVMs because they're bound to a single node and can't be restarted elsewhere in the cluster.
- Set Host failures cluster tolerates to **1** for replication factor 2 and **2** for replication factor 3. These settings ensure that the proper amount of resources are automatically reserved for the cluster.
- Set the host isolation response to **Power off and restart VMs** to ensure that VMs are moved to a healthy host and continue to function.
- Set the host isolation response to **Leave powered on** for CVMs. You don't want CVMs to be turned off if there's a transient network disruption.
- Disable Storage I/O Control. If Storage I/O Control is enabled, it can cause storage unavailability, unnecessary lock files, and complications with Metro Availability.

Management Best Practices

- Deploy a scaled-out Prism Central instance for edge sites to simplify capacity planning, platform lifecycle management, and virtual networking management, and to reduce management overhead.
- Deploy one instance of vCenter HA for all workloads and configure it with Platform Services Controller embedded.
- Configure at least three NTP servers (NTP standard recommendation is five to detect rogue time sources) and ensure that they're accessible at all solution layers, including AOS, AHV, and Prism Central, plus vCenter and ESXi if you're using vSphere.
- Use the same NTP servers for all infrastructure components.
- Don't use an AD domain controller as an NTP source.
- If you're in a dark site with no internet connectivity, use a switch or GPS time source.
- Configure NTP sources specific to the region where the edge clusters reside.
- Configuring at least two DNS servers and make them accessible at all layers (AOS, Prism Central, ESXi, vCenter, and network switches) to ensure that components can reliably resolve addresses at all times.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3168

- Configure DNS sources specific to the region where the edge clusters reside.
- Use RBAC for all the consoles and element managers and use AD as the directory service for user and group accounts.
- Where possible, use AD groups to assign privileges for easier operations.
- Deploy a robust logging platform that meets your security requirements.
- Forward all infrastructure logs to the centralized log repository.
- Store the logs in a different cluster, or location, from where you collect them. This measure protects the logs in case of a catastrophic cluster failure, ensuring they can later be used for forensics.
- Ensure that AD sites and services are set up to define a replication and authentication topology in the event that connectivity to the datacenter is lost.

Security Best Practices

Authentication

- Maintain as few user and group management systems as possible. A centrally managed authentication point is preferred to many separately managed systems.
- You should at least take advantage of the external LDAP support provided by Nutanix components.
- Use AD authentication for user and server accounts to ensure that user activity logged for auditing purposes and account security is configured and maintained from a single centralized solution.
  - › You must have a highly available AD infrastructure and network connection to the datacenter.
- Use an SSL or TLS connection to AD to eliminate cleartext exchanges on the network.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3169

Certificates

- Protect all consumer-facing components with certificates signed by a trusted certificate authority to provide an extra layer of security and prevent meddler-in-the-middle (MITM) attacks.
  - › You can use internally or externally signed certificates based on your consumer classification and the service the specific component provides.

Cluster Lockdown

- Don't use Nutanix or vSphere cluster lockdown (feature that lets you enforce SSH access to CVMs and host using key pairs instead of passwords) unless you require passwordless communication.

Hardening

- Enable Advanced Intrusion Detection Environment (AIDE) for the CVM and AHV. AIDE performs checksum verification for all statis binaries and libraries for improved security.
- Enable stack traces for cluster issues for AHV or ESXi and CVM.
- Enforce a complex password policy (at least 15 characters long with at least 8 different characters) for the hypervisor and CVM.
- Enable a banner for AHV or ESXi and the CVM that retrieves a specific sign-in message via SSH.
- Enforce only SNMPv3 on the CVM.
- Configure SCMA to run hourly to capture unacceptable configuration drift.
- ESXi only: Stop unused services and close unused firewall ports to limit the attack surface.

  Note: Ensure that you don't stop a service or close a firewall port that's required by Nutanix, such as SSH and NFS.

- Generally, we recommend following the Hardening Controller VM section of the AOS Security Guide. If you're using AHV, follow the Hardening AHV section of the AOS Security Guide.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3170

Internet-Facing Services

- Use multiple internet connections (active-backup) and ISP-provided denial-of-service (DoS) and distributed-denial-of-service (DDoS) filtering to help mitigate the potential effects of a DoS or DDoS attack.

Logging

- Configure and maintain a single centralized logging solution for auditing purposes and account security.
- Send log files to a highly available syslog infrastructure.
- At least one of the individual targets of the highly available logging infrastructure should run outside the virtual infrastructure itself so that if the virtual infrastructure is compromised, forensic investigations can access logs that might not be available on the cluster itself.
- Include data from all Nutanix modules and components in logging using the error-log level and ensure that they're searchable. See the Configuring the Remote Syslog Server Settings section of the Acropolis Advanced Administration Guide for more information.
- Use default ESXi logging levels, log rotation, and log file sizes.
- If you have additional security and reliability requirements, use TCP for log transport. Otherwise, use the default syslog protocol, UDP.
- Use port 514 (defined port in syslog RFC) for logging.

Network Segmentation

- To protect Nutanix CVM and hypervisor traffic, place them together in their own dedicated VLAN, separate from other VM traffic. This configuration applies to all hosts in a cluster or single node.
- Place out-of-band management on a separate VLAN or physical network to provide additional security.
- We recommend configuring the CVM and hypervisor host VLAN as a native, or untagged, VLAN on the connected switch ports to allow easy node addition and cluster expansion.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3171

- Don't segment Nutanix storage and replication traffic, or iSCSI Volumes traffic, on separate interfaces (VLAN or physical) unless additional segmentation is required by mandatory security policy or the use of separate physical networks.

Role-Based Access Control (RBAC)

- Use a least-privilege and separation-of-duties approach when assigning RBAC permissions to ensure that each group or individual user has just enough permissions to perform their duties. Use predefined roles or create new roles as needed.
- Configure RBAC at the Prism Central level because it provides the overlying management construct. This configuration ensures that your least-privilege configuration stays in place and avoids common mistakes that occur when RBAC is configured at multiple different levels.
- Align RBAC structure and default plus custom roles with your company requirements.

Data-at-Rest Encryption

- Keep management traffic, including storage traffic, on a separate network.
- Don't use storage encryption.
- Don't use a key management server (KMS).

Microsegmentation and Firewall

- Use Flow Network Security (previously Flow Microsegmentation) to comply with regulatory and business-specific compliance policies such as PCI-DSS, HIPAA, and NIST.
- Use a Palo Alto Networks VM-Series firewall with Flow Network Security to provide advanced threat and vulnerability detection for layers 4–7.

Operations Best Practices

- Purchase the Nutanix Cloud Manager (NCM) Starter license, which gives you access to analytics, capacity planning, custom dashboards, and playbooks for Prism Central.
- Review capacity planning monthly.
- Perform updates after hours for performance- or migration-sensitive applications to reduce the load on the system.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3172

- Use the latest supported release.
- Update to the next maintenance version four weeks after release and to the current patch version two weeks after release to keep updates relatively small.
- Maintain a preproduction environment to test any necessary changes to firmware, software, or hardware before implementing the change in production. Preproduction environments can help you avoid the cost of outages.
- Configure alerts and alert policies in Prism Central, not Prism Element, to create consistency across multiple clusters and reduce the effort involved in making multiple changes. Prism Central–based alert policies also allow you to detect anomalies.
- Use SMTP for alert transmission to create consistency across multiple clusters, reduce the effort involved in making multiple changes, enable anomaly detection, and offer more options for delivery.

BCDR Best Practices

- Keep as few VMs per protection domain as possible in your design.
  - › If you're using asynchronous replication, configure at most 200 VMs per protection domain.
  - › If you're using NearSync replication, configure at most 10 VMs per protection domain.
- Group VMs with similar RPO requirements in the same protection domain.
  - › Node size and capacity can limit the possible RPO for the VMs running on it. See the Resource Requirements Supporting Snapshot Frequency (Asynchronous, NearSync and Metro) section of the Data Protection and Recovery with Prism Element guide for details.
- Put NearSync VMs in their own protection domains (NearSync can only have one schedule).
- Limit consistency groups to fewer than 10 VMs.
- Only use consistency groups for applications with a shared state, such as database replicas.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3173

- Only add one VM to any consistency group that uses application-consistent snapshots.
- Configure snapshot intervals to be shorter than your desired RPO to allow for failure and recovery without manual intervention. The interval should be half your desired RPO including data transmission timing.
- Configure snapshot schedules to retain the minimum number of snapshots needed to meet your retention policy.
- If you're using synchronous replication, create one container on the source and one on the destination with the same name.
- If you're using synchronous replication, ensure that the two participating clusters are within 5 ms round trip time (RTT) of each other.
- Use Metro Availability for business-critical applications that require zero data loss (RPO 0), minimal to zero recovery time (RTO 0), or RTO 0 during a disaster recovery avoidance event.
  - › Metro Availability is only supported with ESXi.

References

1. AHV best practice guide
2. AHV Networking best practice guide
3. Data Efficiency tech note
4. Data Protection and Disaster Recovery best practices guide
5. Disaster Recovery with Nutanix Cloud Clusters (NC2) on AWS tech note
6. Flow Network Security tech note
7. Hybrid Cloud Reference Architecture
8. Information Security tech note
9. Nutanix AHV Virtualization tech note
10. Nutanix DRaaS Security tech note
11. Nutanix Era Security tech note
12. Nutanix Hardware Compatibility Lists
13. Nutanix Volumes best practice guide

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3174

14. Palo Alto Networks VM-Series Firewalls on Xi tech note
15. Physical Networking best practice guide
16. Prism tech note
17. ROBO Deployment and Operations
18. Security Advisories
19. Virtual Machine High Availability tech note
20. VMware vSphere best practice guide
21. VMware vSphere Documentation

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3175

About Nutanix

Nutanix offers a single platform to run all your apps and data across multiple clouds while simplifying operations and reducing complexity. Trusted by companies worldwide, Nutanix powers hybrid multicloud environments efficiently and cost effectively. This enables companies to focus on successful business outcomes and new innovations. Learn more at Nutanix.com.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3176

List of Figures

Figure 1: Availability Zones in a Region..... 12
Figure 2: Edge Sites in an Availability Zone..... 13
Figure 3: Single Site, Multiple Availability Domains, Active-Active..... 15
Figure 4: Single Site, Multiple Availability Domains, Active-Passive..... 16
Figure 5: Multiple Sites, Fan-In or Central Datacenter..... 17
Figure 6: Multiple Sites, Chain Structure..... 19
Figure 7: Overview of Nutanix Recoverability Options..... 23
Figure 8: Overview of the Technical Design..... 32
Figure 9: Management Plane Failure Domains..... 38
Figure 10: Nutanix Cluster Failure Domains..... 39
Figure 11: Server Room Failure Domains..... 40
Figure 12: Small Edge Site Network Topology..... 43
Figure 13: Leaf-Spine Topology for Medium and Larger Edge Sites..... 43
Figure 14: AHV Networking..... 47
Figure 15: Life Cycle Manager..... 59
Figure 16: Capacity Runway..... 61
Figure 17: Two Availability Zones in the Same Region..... 63
Figure 18: Multiple Availability Zones in a Single Region..... 64
Figure 19: Multiple Availability Zones across Multiple Regions..... 65
Figure 20: Disaster Recovery Decision Flowchart..... 67

v1.1 | November 2024 | RA-2147

REFERENCE ARCHITECTURE

Nutanix for Enterprise Edge Computing

NUTANIX

Legal

© 2024 Nutanix, Inc. All rights reserved. Nutanix, the Enterprise Cloud Platform, the Nutanix logo and the other Nutanix products, features, and/or programs mentioned herein are registered trademarks or trademarks of Nutanix, Inc. in the United States and other countries. All other brand and product names mentioned herein are for identification purposes only and are the property of their respective holder(s), and Nutanix may not be associated with, or sponsored or endorsed by such holder(s). This document is provided for informational purposes only and is presented "as is" with no warranties of any kind, whether implied, statutory or otherwise.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

Contents

1. Executive Summary..... 5

2. Introduction.....6
Purpose..... 6
Audience.....6

3. Nutanix Cloud Platform Overview.....7
Physical Layer.....7
Hypervisors.....9
Management.....9
Business Continuity and Disaster Recovery.....9
Automation.....11
Security and Compliance..... 11

4. High-Level Design Considerations..... 12
Choosing an Enterprise Edge Architecture..... 12
Choosing a Hypervisor.....20
System Availability..... 20
System Recoverability.....22
Performance and Scalability..... 25
Manageability.....26
Choosing a Control Plane.....27
Choosing the Right Licensing and Support.....27
Choosing Hardware.....29
High-Level Design Recommendations.....30

5. Detailed Technical Design.....32
Required Software Versions..... 32
Physical Layer Design..... 33
Virtualization Layer Design..... 49
Management Layer Design.....51
Security Layer Design.....54
Automation Layer Design.....58
Operations Design.....61
BCDR Design.....62

6. Optional Nutanix Products and Services..... 71

7. Conclusion..... 72

8. Appendix..... 73
Best Practices for Enterprise Edge Sites..... 73
References..... 85

About Nutanix..... 87

List of Figures..... 88

1. Executive Summary

Each organization defines edge computing differently; we define edge computing as workloads (applications and services) hosted and contained outside the core enterprise datacenter. These workloads fall into three categories:

1. Internet of Things (IoT) edge
   a. End users: developers, data scientists
   b. Roles: data acquisition, inferencing, modeling
   c. Typical use cases: manufacturing, transportation, robotics
2. Enterprise edge
   a. End user: enterprise IT
   b. Roles: localized applications, service hosting, remote office
   c. Typical use cases: file server, remote desktops, latency sensitive applications, business continuity planning (BCP)
3. Telco edge
   a. End user: the enterprise (operated and managed by the service provider)
   b. Typical use cases: multi-access edge computing, carrier-grade network function virtualization (NFV) services

This reference architecture focuses on the Nutanix Cloud Platform as a solution for enterprise edge workloads.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3182

2. Introduction

Purpose

We created this reference architecture to assist architects through the design process of implementing enterprise edge sites. After reading this document, architects should understand Nutanix best practices for enterprise edge sites and the implications and justifications of the design choices they make.

Audience

This reference architecture is part of the Nutanix Solutions Library. We wrote it for IT decision makers and architects responsible for deploying enterprise edge applications and services. Readers of this document should already be familiar with Nutanix.

This document often refers readers to the Nutanix Hybrid Cloud Reference Architecture.

Unless otherwise stated, the solution described in this document is valid on AOS versions 5.20 and later.

Document Version History

Version Number	Published	Notes
1.0	July 2022	Original publication.
1.1	November 2024	Updated AOS release cycle descriptions.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3183

3. Nutanix Cloud Platform Overview

Physical Layer

Nutanix converges compute, storage, storage networking, and virtualization, reducing complexity and replacing the separate servers, storage systems, and storage area networks (SANs) found in conventional datacenter architectures. Each node in a Nutanix cluster includes compute, memory, and storage, and nodes are grouped into clusters. AOS software running on each node pools storage across nodes and distributes operating functions across all nodes in the cluster for performance, scalability, and resilience.

Hardware

The Nutanix Cloud Platform provides significant flexibility when it comes to hardware platform selection. Available options include:

- Nutanix NX appliances
- Original equipment manufacturer (OEM) appliances from leading vendors such as Dell, Lenovo, HPE, and Fujitsu
- Other third-party servers from a wide range of vendors

The Nutanix Hardware Compatibility Lists contain the most up-to-date information on supported systems.

Compute

The process for sizing systems to meet compute needs in a Nutanix environment is similar to that of other architectures. However, you must ensure that your design provides enough compute (CPU and RAM) to support the CVM.

Storage

Nutanix nodes offer a range of storage configurations:

- Hybrid nodes combine flash SSDs for performance and HDDs for capacity.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3184

- All-flash nodes use traditional flash SSDs.
- NVMe nodes use NVMe SSDs.

You can mix different node types in the same cluster.

Nutanix AOS storage exhibits data avoidance and efficiency using techniques such as thin provisioning, intelligent cloning, compression, deduplication, and erasure coding. These techniques accelerate application performance and optimize storage capacity. They are intelligent and adaptive, requiring little or no fine-tuning in most cases, which reduces operating expenses and frees your IT staff to focus on growth and innovation. Unlike traditional storage architectures, the Nutanix web-scale design ensures that data efficiency techniques scale as the cluster grows.

For more information, see the Data Efficiency tech note.

Networking

The distributed storage architecture relies on the performance and resilience of the physical network. A good design provides high performance while maintaining simplicity. For more details on networking, see the Physical Networking best practice guide and the AHV Networking best practice guide.

Cluster Design

A Nutanix cluster is the management boundary of the storage provided to a group of workloads. A Nutanix deployment can have either single clusters with mixed workloads or dedicated clusters for each workload type in a block-and-pod design. Designs with dedicated clusters can include the following cluster types:

Management clusters

Designed to run VMs that support datacenter management services, such as Nutanix Prism Central, VMware vCenter, and Active Directory (AD) domain controllers, and other management workloads, such as DNS, DHCP, NTP, and syslog.

Edge clusters

Reside at an edge or remote and branch office (ROBO) deployment to run VMs or ROBO workloads. These clusters are typically distinguished from normal workload

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3185

clusters by their small size and limited external bandwidth and can contain a variety of node types and sizes.

Hypervisors

This solution covers two enterprise-grade hypervisors: Nutanix AHV and VMware ESXi (vSphere). Both fulfill a similar set of requirements and use cases. Nutanix AHV is included at no additional cost with every Nutanix node. For more information on AHV, see the Nutanix AHV Virtualization tech note and the AHV best practice guide. For information on VMware vSphere on Nutanix, see the VMware vSphere best practice guide.

Note: Nutanix also supports Microsoft Hyper-V; however, this document only covers AHV and ESXi.

Management

Nutanix Prism is the centralized management solution for Nutanix environments. Prism combines multiple aspects of datacenter management into a single consumer-grade design that provides complete infrastructure and virtualization management, operational insights, and troubleshooting.

For more detailed information about Prism, see the Prism software documentation and the Prism tech note.

Business Continuity and Disaster Recovery

We built Nutanix with resilience in mind, so the platform includes redundancy for power and other hardware components and enables you to protect entire datacenters. Nutanix provides native business continuity, including backup and restore and disaster recovery, at the hardware, node, data, VM, and datacenter or site levels.

For more detailed information about Nutanix business continuity and disaster recovery (BCDR), read the Data Protection and Disaster Recovery best practices guide, the Disaster Recovery with Nutanix Cloud Clusters (NC2) on AWS tech note, the Nutanix Disaster Recovery (previously Leap) software documentation, and the Nutanix Mine software documentation.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3186

Snapshots and Clones

An individual cluster can create a snapshot of a vDisk or an entire VM. Nutanix snapshots are redirect-on-write, where the pointers that indicate which physical disk extent maps to a virtual disk are updated only as data changes.

Snapshots can be application-consistent or crash-consistent. AOS can trigger an application-consistent snapshot in Nutanix Guest Tools or VMware tools, depending on which hypervisor you use.

For ESXi-triggered clones, AOS supports offloading the clone using vStorage API for Array Integration (VAAI). The VM must be turned off and the clone must reside on the same datastore as the primary VM in order to trigger offloading.

> **Note:** Nutanix snapshots are a vital element of a data protection strategy; however, they aren't a substitute for a full backup methodology.

Replication Options

You can also replicate Nutanix snapshots to multiple destination clusters to provide multiple redundant copies if needed. Configure these arrangements as part of the snapshot schedule by specifying each remote site that should receive a copy and how many copies it should retain.

> **Note:** One-to-many relationships are allowed (Site A to Site B, Site A to Site C, Site A to Site N), but cascading relationships (Site A to Site B to Site N) aren't supported.

Protection Domains

With Prism Element, you can group VMs into protection domains. During a failover event, all the entities in the protection domain are activated at the remote site as a group. The RPO you choose for these entities determines whether the system uses traditional asynchronous snapshots or lightweight snapshots for this process.

You can also create a consistency group for all VMs and volume groups in a protection domain. Consistency groups enable you to snapshot all members of the group in a crash-consistent manner.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3187

Automation

Automation and orchestration are critical to IT success. By simplifying infrastructure management across the entire lifecycle, automating operations, and enabling self-service, Nutanix helps you deploy datacenter infrastructure that delivers a high degree of scalability, availability, and flexibility with Prism (centralized automation management), Nutanix Cloud Manager (NCM) Self-Service (previously Calm; application orchestration), and simplified test and development automation.

Security and Compliance

Nutanix takes a security-first approach that includes a secure platform, extensive automation, and a robust partner ecosystem. Security Configuration Management Automation (SCMA) monitors the health of storage and VMs, automatically healing any deviations from the baseline, and data-at-rest encryption (DaRE) features add to our robust security capabilities. We also provide additional configuration options if you need to add an extra layer of security to fulfill business or technical requirements.

For more detailed information on Nutanix security and compliance features, see the following documents, separated by category:

- Networking: Flow Network Security tech note
- Information: Information Security tech note
- Cloud: Nutanix DRaaS Security tech note
- Database: Nutanix Era Security tech note

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3188

4. High-Level Design Considerations

There are several high-level design decisions you must make before proceeding to the detailed technical design.

Choosing an Enterprise Edge Architecture

First, you need to know what availability you need and what failures the design must protect against. These are key input requirements.

You also need to be familiar with the regions and availability zones as defined in the High-Level Design Considerations section of the Nutanix Hybrid Cloud Reference Architecture. Briefly, a region holds one or more availability zones. Each availability zone contains one or more datacenters or edge locations.

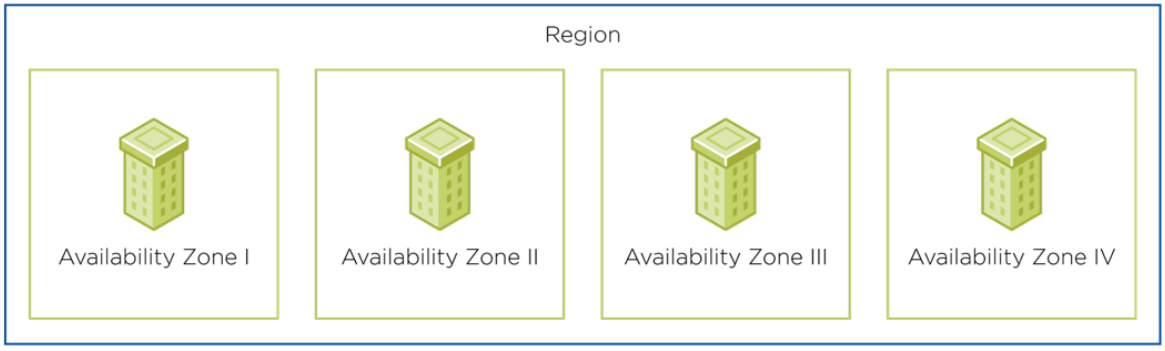


Figure 1: Availability Zones in a Region

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3189

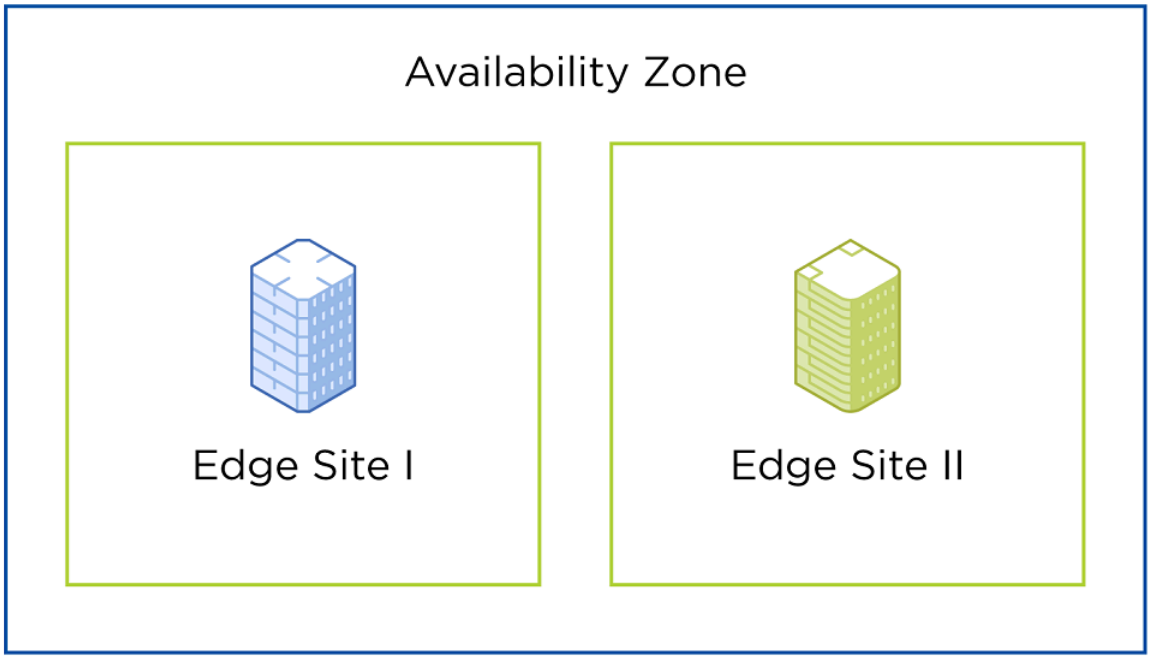


Figure 2: Edge Sites in an Availability Zone

Because an enterprise edge deployment can cover many locations often distributed across multiple geographies, we suggest that you logically group the manageability, replication, and BCDR components of your edge sites into a single region with multiple availability zones. This logical grouping provides design advantages for the control plane, scalability and performance, and BCDR.

> **Note:** If your enterprise edge deployment has a small number of sites and single locations, you may not need this grouping.

When choosing an enterprise edge architecture, keep the following things in mind:

- Latency requirements can vary depending on the deployment and the resources being consumed. For example, witness VMs hosted in the cloud can tolerate up to 500 ms of latency per 100 instances, while Prism Central can only tolerate 150 ms of latency per Prism Element instance that it manages.
- Bandwidth requirements vary based on desired recovery point objectives (RPOs), replication mediums, and the resources being consumed.
- A scaled-out Prism Central instance can manage 400 clusters and up to 2,000 nodes.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3190

- You need accurate NTP access.
- You must consider whether you want a WAN-restricted topology or open internet access.
- You need to review your BCDR requirements, planned versus unplanned downtime, and environmental risk.
- You can replicate data to more than one location using different replication types if needed. For example, you might use NearSync replication between sites located in the same availability zone and asynchronous replication to a datacenter in another region.

Edge Operating Models

Nutanix supports the following enterprise edge operating models, independent of the operating model of the core datacenter:

- Single site, active
  - › Applications are active in the edge site.
  - › Backups are stored in the same edge site that the applications run in.
  - › Long-time archiving is stored offsite.
  - › This model provides limited protection against datacenter failure.
- Single site, multiple failure domains, active-active
  - › Applications are active in one or more failure domains during normal production.
  - › Failure domains can be in different locations in the site (for example, opposite ends of a campus).
  - › Failure domains can provide disaster avoidance and disaster recovery for each other.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3191

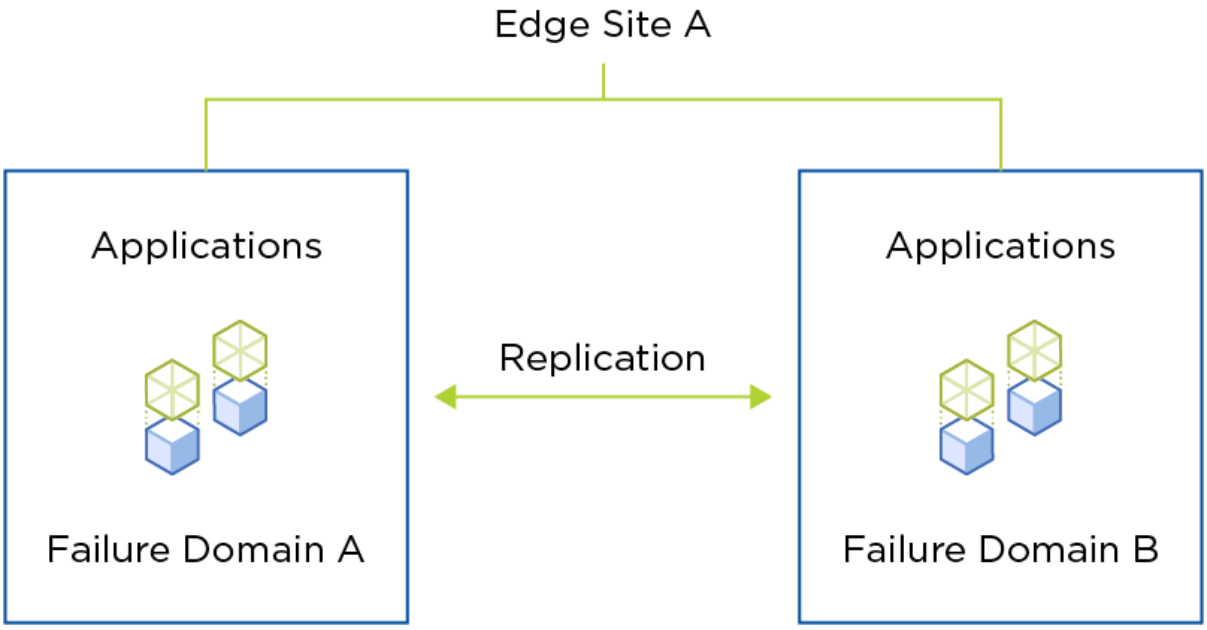


Figure 3: Single Site, Multiple Availability Domains, Active-Active

- Multiple sites, active-passive
  - › Edge-based applications typically run at the edge site during normal production.
  - › Usually the central datacenter (passive site) provides disaster avoidance and disaster recovery for the active enterprise edge site.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3192

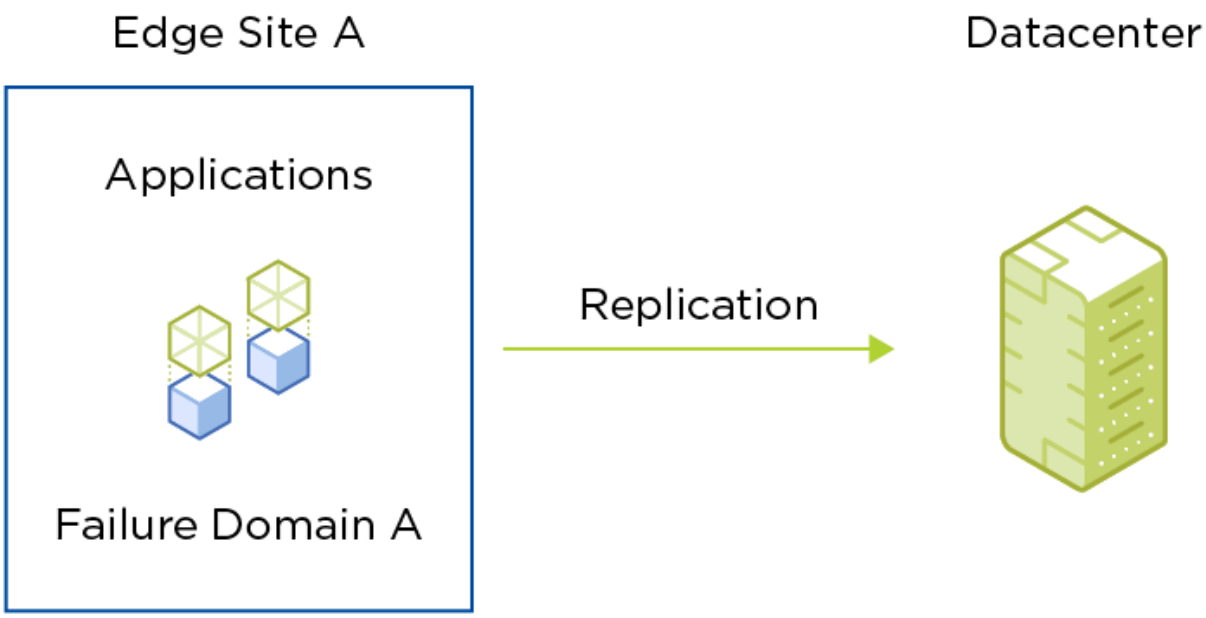


Figure 4: Single Site, Multiple Availability Domains, Active-Passive

- Multiple sites, fan-in or central datacenter
  - › Multiple enterprise edge sites replicate data to the datacenter.
  - › The datacenter acts as disaster recovery for the edge sites.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3193

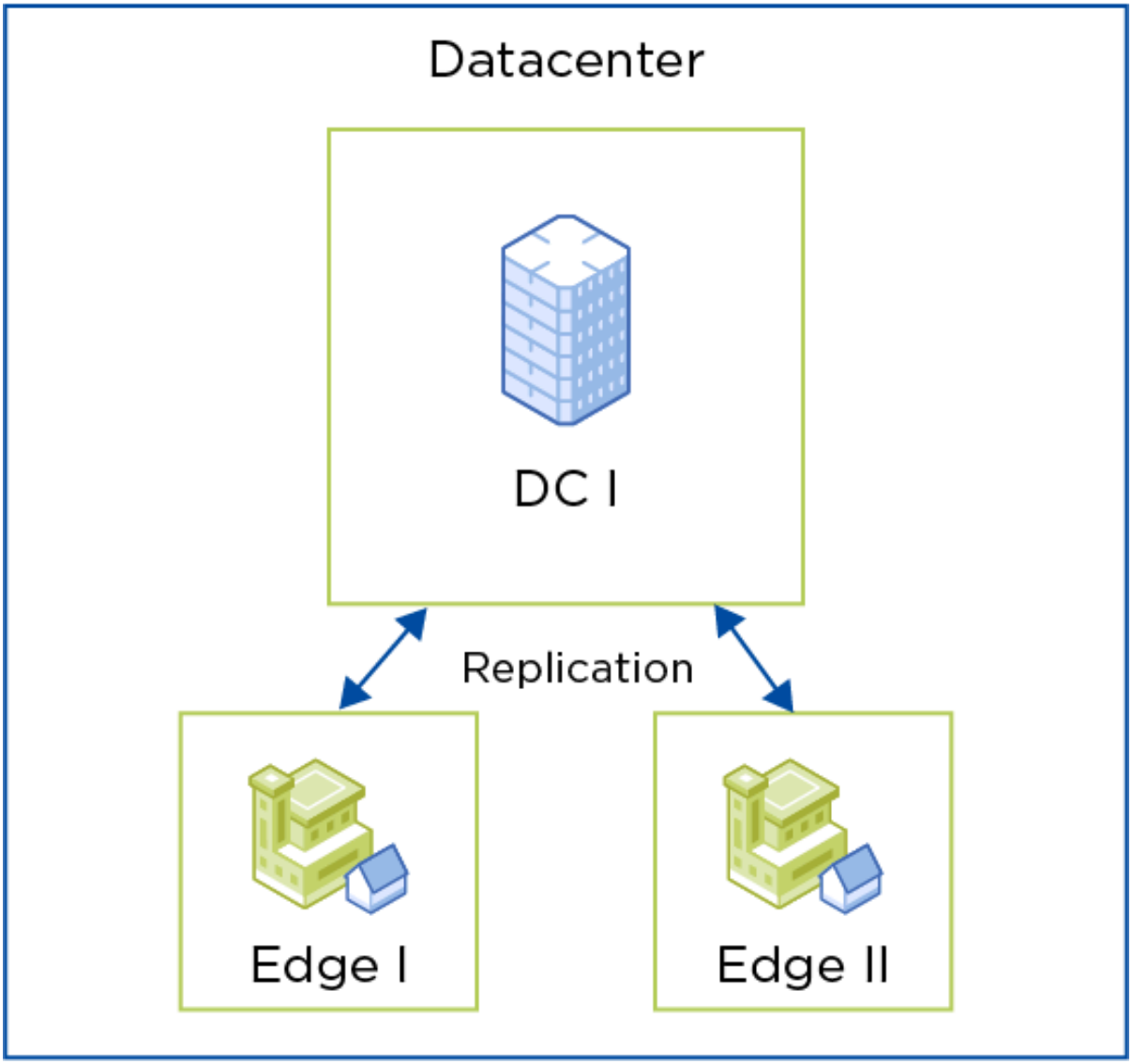


Figure 5: Multiple Sites, Fan-In or Central Datacenter

© 2024 Nutanix, Inc. All rights reserved

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3194

- Multiple sites, chain structure
  - › The datacenter provides disaster recovery for the closest edge site or sites.
  - › This model is often used by organizations with multiple datacenters or regions.
  - › The first-tier edge sites connected to the datacenter acts as disaster recovery sites for the next tier of edge sites. Some organizations call these locations regional datacenters.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3195

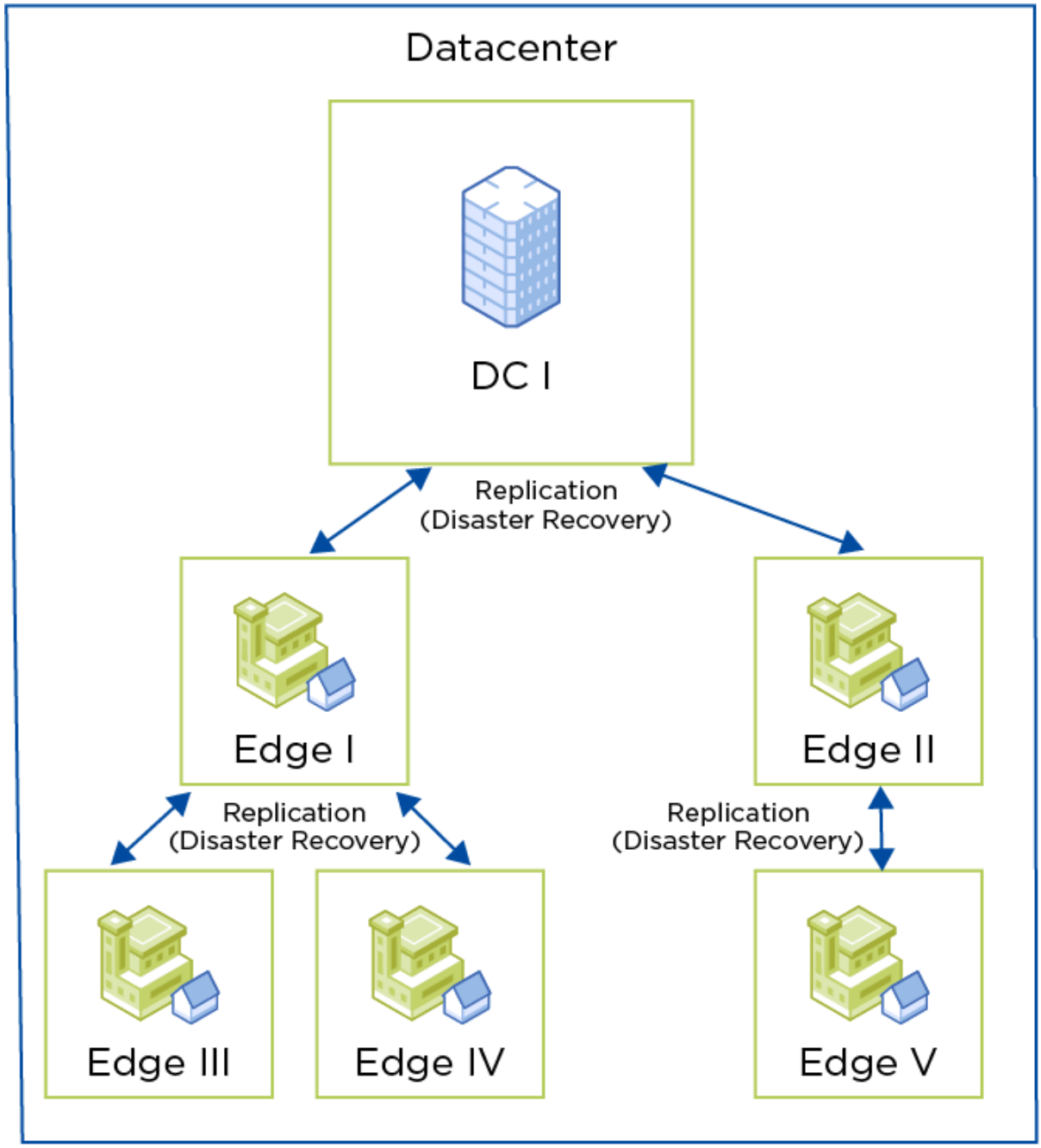


Figure 6: Multiple Sites, Chain Structure

© 2024 Nutanix, Inc. All rights reserved |

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3196

Choosing a Hypervisor

Nutanix supports multiple hypervisors: Nutanix AHV, VMware vSphere, and Microsoft Hyper-V. This design covers the deployment of either Nutanix AHV or VMware vSphere.

Nutanix AHV is included with AOS and delivers high performance, flexible migrations, integrated networking, security hardening, automated data protection and disaster recovery, and rich analytics. AHV is a lean virtualization solution with robust, integrated management features. VMware vSphere is a proven virtualization platform used by many organizations. It has a robust ecosystem but is a complex platform with many design choices and settings to tune that often requires the purchase of additional licenses.

System Availability

When evaluating availability requirements, start by building a dependency map of the applications and services hosted at the enterprise edge coupled with the service-level agreement (SLA; measured in 9s of availability) that the Nutanix system needs to support. Next, categorize availability events as planned or unplanned to enable you to plan for unforeseen events.

Single-Node Clusters

Let's say, for example, that an edge site has a single node in the Nutanix cluster (ROBO1) that hosts compute and storage. During write operations, the cluster mirrors data across the internal drives. In the event of a drive loss, the cluster enters a read-only state until the drive failure has been addressed, meaning that any hardware failure renders the system, application, and service offline.

You could address the availability constraints of the single-node cluster in the following ways:

Replicate data to a neighboring node: Deploy and maintain two separate single-node clusters that each serve as a replication partner to the other and independent failure domains.

Replicate data to the central datacenter or cloud.

The advantages of the single-node cluster are:

- It's an operationally well-understood and simplified model.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3197

- It has lower capex.
- It offers 1 GbE support.

The disadvantages of the single-node cluster are:

- It can support fewer VMs.
- You can't easily expand the cluster; it requires additional planning.
- It doesn't support storage optimization features.
- Without standard operating procedures (SOPs), RPOs and RTOs can be negatively affected.
- Planned outages such as patches and updates can require downtime.

Two-Node Clusters

A two-node cluster (ROBO2) improves system availability. In this design, two Nutanix nodes replicate data synchronously (RPO 0) while supporting VM high availability and migration features like automatic restart and migration, dramatically decreasing the RTO.

Two-node clusters offer reliability for smaller sites that must be cost effective and run with tight margins. These clusters only use a witness in failure scenarios to coordinate rebuilding data and automatic upgrades. You can deploy the witness offsite up to 500 ms away for asynchronous replication and 200 ms away for Metro Availability. Multiple clusters can use the same witness for two-node and metro clusters.

The advantages of the two-node cluster are:

- It aggregates system resources (compute and storage).
- It reduces the RPO and RTO.
- It automatically recovers resources.
- There's minimal impact from planned outages such as patches and updates.
- It supports asynchronous replication with lower RPOs to a neighboring cluster.

The disadvantages of the two-node cluster are:

- You can't easily expand the cluster; it requires additional planning.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3198

- It relies heavily on the availability of a witness VM.
- Staff needs familiarity with SOPs for node patching and upgrading.
- It doesn't support storage optimization features.

Three-Node or Greater Clusters

Clusters with three or more nodes (ROBO3) follow the traditional datacenter deployment strategy and have the same levels of availability and platform-specific features to optimize compute and storage resources. Clusters with three or more nodes address availability concerns by providing advanced clustering and data distribution, which result in lower RTOs for planned versus unplanned system outages.

The advantages of clusters with three or more nodes are:

- They support all Nutanix features and functionalities.
- Their clustering and data distribution yield a lower RTO.
- They have zero down time for patches, upgrades, and cluster expansion operations.

The disadvantages of clusters with three or more nodes are:

- They have a higher capex due to the additional nodes.
- For optimum performance, they require a 10 GbE network connection for all nodes. However, 1 GbE is sufficient for clusters with up to eight members.
- They use additional compute resources.
- They have increased power and cooling requirements.

System Recoverability

System recoverability defines how you recover the service or application hosted at the edge when the primary copy has been compromised or lost.

Nutanix has several recoverability options for customers who want to protect and back up their data against defined SLAs. The following figure and table illustrate four common recoverability strategies that you can use regardless of the edge strategy you deployed.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3199

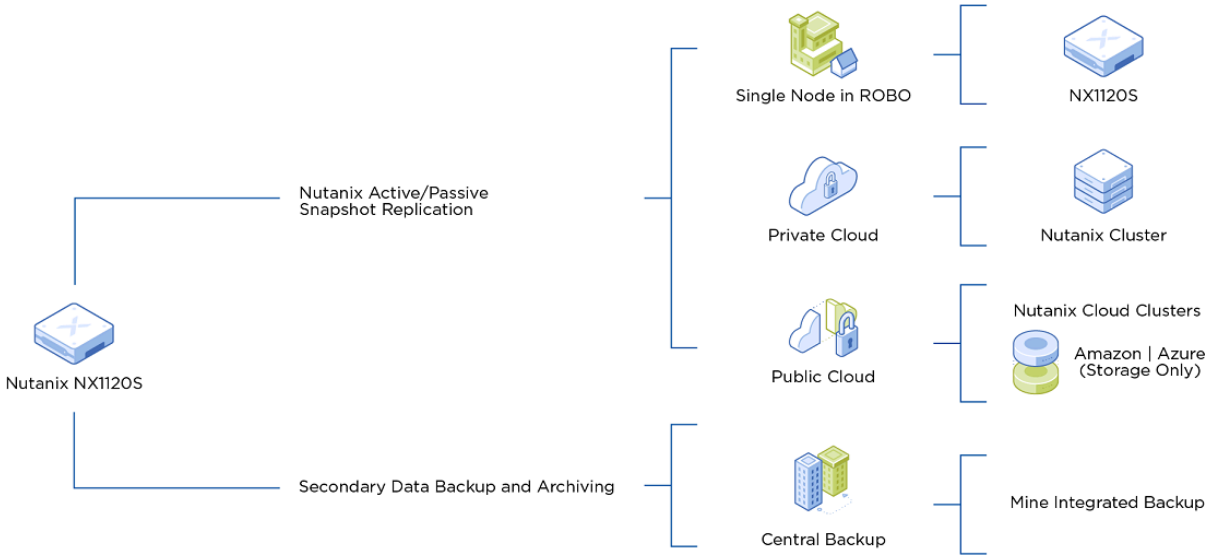


Figure 7: Overview of Nutanix Recoverability Options

Table: Replication Options with Nutanix

Destination	Strategy	Description	RPO	Recovery Method
Single-node ROBO	Asynchronous replication	Used when the source and the destination are single-node clusters.	6 hours	VM
Private cloud	Near-synchronous (NearSync) replication	Used when there are at least three nodes in a cluster on both the primary and the remote site.	1–15 minutes	VM
Private cloud	Asynchronous replication	Used when replicating to a cluster of at least three nodes in the primary datacenter.	60 minutes	VM

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3200

Destination	Strategy	Description	RPO	Recovery Method
Public cloud	Nutanix Cloud Clusters (NC2; asynchronous)	Used when customers need to host Nutanix on AWS, GCP, or the Nutanix public cloud; allows customers to use the same replication strategies as the private cloud.	60 minutes	VM
Public cloud	Amazon S3 / EBS, Azure Blob	Uses the Cloud Connect feature to replicate VMs to AWS S3 (EBS for metadata) or Azure Blob Storage. With this option, customers can't turn on VMs because they're just using a storage target or service in the public cloud.	60 minutes	VM
Central backup	Nutanix Mine (secondary data backup and archiving)	Used when customers need a dedicated, turnkey solution that supports backup and archiving using integrated solutions from Veeam and HYCU.	60 minutes	VM- or file-level backup

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3201

For more information on NearSync requirements and limitations, see Requirements of Data Protection with NearSync Replication. For more information on single-node clusters, consult Single-node Clusters. To understand more about the Cloud Connect feature and protection domains, see Asynchronous Replication Using Cloud Connect (On-Prem to Cloud).

Performance and Scalability

When you build an enterprise edge solution, you need to carefully define your performance and scalability requirements because node deployment strategy can adversely affect the scalability of the solution. For example, with ROBO1, you're limited to a single node and can't expand your deployment by adding additional nodes or take advantage of data distribution across multiple compute nodes. ROBO2 has similar constraints.

> **Note:** If you need to be able to scale your edge solution beyond two nodes or add storage-only nodes to the cluster, you should implement a three-node cluster.

Regardless of whether your sites are classified as small (fewer than 10 VMs) or large (more than 50 VMs), you need to standardize the resources the edge sites provide and consume from the core datacenter. To accomplish this standardization, consider the four key elements of edge sites:

1. Devices and applications
   a. Create a dependency map of physical devices and applications that your infrastructure interfaces with or provides services for.
   b. Understand whether you plan to scale your devices and applications linearly over time.
   c. Establish whether the device or application should have a dedicated cluster or share a mixed cluster with other applications and services.
2. Clusters
   a. Define the maximum size of the clusters in your edge sites and the maximum number of edge sites in your organization.
   b. Reference the configuration maximums of Nutanix components and third-party components used in your design.
   c. Define the services that edge sites should provide (file sharing, NFV).

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3202

3. Network
   a. Choose the optimal network layout, considering how sites receive and send public versus private traffic and connect to the core datacenter.
   b. Use minimal bandwidth and a latency standardized for connectivity to the core datacenter.
4. Cloud
   a. Determine your cloud deployment model (hybrid, private, public).
   b. Determine which additional cloud resources you need, such as additional storage to cover replication from additional edge sites.
   c. Determine how much additional bandwidth you need in order to add additional edge sites to the cloud.

Manageability

The deployment model you use for the enterprise edge solution influences overall manageability.

Dedicated or Mixed Clusters

Typically, in enterprise edge sites organizations deploy between 5 and 10 VMs. In this instance, a mixed workload cluster makes the most sense. However, with larger deployments (for example, large distribution centers) that serve many mission-critical applications and have many regulatory compliance requirements, the complexity of sizing and operating the mixed environment increases dramatically.

When you operate edge sites at a large scale, your architecture, design choices, and requirements start to look more like those of a traditional datacenter. For these cases, we encourage you to review the Will You Deploy Dedicated or Mixed Clusters? section of the Nutanix Hybrid Cloud Reference Architecture.

Storage-Only Nodes in Clusters

Storage-only nodes add storage capacity and I/O performance to a cluster. Storage-only nodes can be any node type, but they're typically configured with just enough CPU and memory resources to run the CVM because no application VMs run on them. These nodes are members of the AOS cluster but aren't visible to the hypervisor cluster for nonstorage functions, so the hypervisor can't schedule other VMs to run on them.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3203

Note: You can only add storage-only nodes to clusters with three or more nodes.

Note: We recommend deploying storage-only nodes in pairs.

Choosing a Control Plane

When working with larger edge deployments geographically dispersed across multiple regions, we expect the organization to face control plane proliferation, so you must give additional thought to the operational administration of the clusters. In this design:

- The primary control plane is Prism Central.
- If you use ESXi, you also need VMware vCenter.

Each of these control planes has a maximum size that dictates the number of VMs, nodes, and clusters a single instance can manage. For AOS 5.20 (the minimum version required for these solutions), Prism Central (scaled-out configuration) can manage a maximum of:

- 25,000 VMs
- 400 clusters
- 2,000 nodes

These limits are quickly realized when you work with multiple sites and auxiliary solutions, especially when sharing a Prism Central instance with the core datacenter infrastructure. At very large scale (multiple sites, geographically dispersed), it makes sense to deploy an additional Prism Central instance in the management cluster in your core datacenter to manage the edge sites or to deploy a Prism Central instance specific to the region it manages.

Choosing the Right Licensing and Support

When evaluating the different Nutanix platform options available, there are two key decision points:

- Your software and support licensing types
- Your platform vendor

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3204

Software and Support Licensing

Nutanix nodes are primarily available in two different purchasing or licensing options: appliances or software-only.

Appliances:

- Available directly from Nutanix or through our OEM relationships.
- Appliance-based licensing is referred to as life-of-device licensing, meaning it's only applicable to the appliance it was purchased with.
- The manufacturer of the appliance takes all support calls for software and hardware issues. For example, if you choose a Dell appliance, Dell takes all support calls and escalates to Nutanix for software support as needed. With a Nutanix NX appliance, all support calls go directly to Nutanix.

Software-only:

- Decouples software and support licensing from the underlying hardware, which enables:
  - License portability. You can use the same license even when the underlying hardware changes, as with a hardware vendor change or a node refresh.

    Note: Licenses are portable for like-for-like hardware replacements. If the hardware specification of the nodes changes, you might need to purchase additional licenses.

  - Deployment on additional supported hardware platforms, based on our qualified list of platforms, which you can find on the Hardware Compatibility Lists page.
  - Direct software support from Nutanix while the server vendor provides hardware support.
- Another type of software-only licensing is the core licensing option, which is best for customers who prefer the benefits of the software-only model but want hardware from a specific OEM server vendor. Core licensing enables customers to purchase software-only licenses and buy hardware from any of the appliance vendors. For example, XC-Core uses Dell XC OEM appliances but decouples software and hardware support.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3205

Vendor Considerations

When it comes to selecting a hardware vendor, there are many factors to evaluate:

- Brand loyalty
- Support quality
- Hardware quality
- Operational experience
- Configuration options
- Physical form factor

Choosing Hardware

Most edge workloads can successfully run on any of the Nutanix and OEM models available, but some models and configurations may be a better fit than others. Once you know the requirements of your workloads, you can use Sizer (a Nutanix product that calculates node and cluster configuration based on inputs) to determine the best configuration for your clusters.

The following sections provide considerations for hardware model selection and performance.

Model Types

The various Nutanix and OEM appliance models and servers give you the flexibility to identify and use the right solution to meet financial, space, and performance requirements for different projects.

Servers for this solution fall under the edge category, which are similar to the servers used for general workloads and EUC but may offer fewer options for CPU and storage because they're optimized for edge-specific use cases.

Performance Considerations

Nutanix and AOS meet the performance demands of different workloads without continuous performance tuning. However, different cluster design and configuration options still yield performance benefits. Selecting the appropriate node model and

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3206

configuration to meet application and solutions requirements is an important design decision. The primary design considerations for performance are:

- Number of drives: The number of HDDs or SSDs in a node can dramatically affect its performance characteristics.
  - › Write-heavy workloads benefit from additional storage devices to provide performance and consistency.
  - › Workloads like VDI typically have minimal capacity requirements but higher IOPS demands. It's common to use nodes with partially populated storage bays and as few as two flash devices per node, providing the right amount of storage capacity while still exceeding performance demands.
- All flash: All-flash clusters only use SSDs and provide higher IOPS and a more consistent I/O profile than HDDs.
- NVMe: New flash technology allows NVMe devices to deliver higher levels of I/O than SSDs with lower latencies.
  - › To realize the full benefits of NVMe, nodes are typically configured with remote direct memory access (RDMA). RDMA allows one node to write directly to the memory of another node by allowing a VM running in the user space to directly access a NIC, which avoids TCP and kernel overhead resulting in CPU savings and performance gains.
- Size of flash tier: In hybrid configurations containing SSD and HDD devices, the bulk of the performance comes from the flash tier. The flash tier in hybrid clusters should be sized to meet or exceed the size of the working set for all applications running on the cluster. There's no penalty for having too much flash in a cluster but not having enough can result in inconsistent performance.

High-Level Design Recommendations

To summarize, for edge computing on Nutanix solutions, we recommend the following:

- Logically group the manageability, replication, and BCDR components of your edge sites in a single region or availability zone.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3207

- Use Prism Central as the primary control plane.
  - › If you use ESXi, you also need VMware vCenter.
- Use the simplified block-and-pod architecture detailed in the Block and Pod Architecture section of the Nutanix Hybrid Cloud Reference Architecture.
  - › If you're building a large-scale site (more than four blocks with the expectation of additional blocks in the future) with the characteristics of a datacenter, see the Nutanix Hybrid Cloud Reference Architecture.
- Build clusters with one or three nodes.
  - › If you need to be able to scale your edge solution beyond two nodes or add storage-only nodes to the cluster, you should implement a three-node cluster.
- If you use them, deploy storage-only nodes in pairs.
  - › You can only use storage-only nodes in clusters with three or more nodes.
- Define an SOP that stipulates how to scale one- or two-node clusters in your design, as this step isn't a function of the core AOS and doesn't have a workflow.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3208

5. Detailed Technical Design

This section provides technical guidelines for each layer of the design stack.

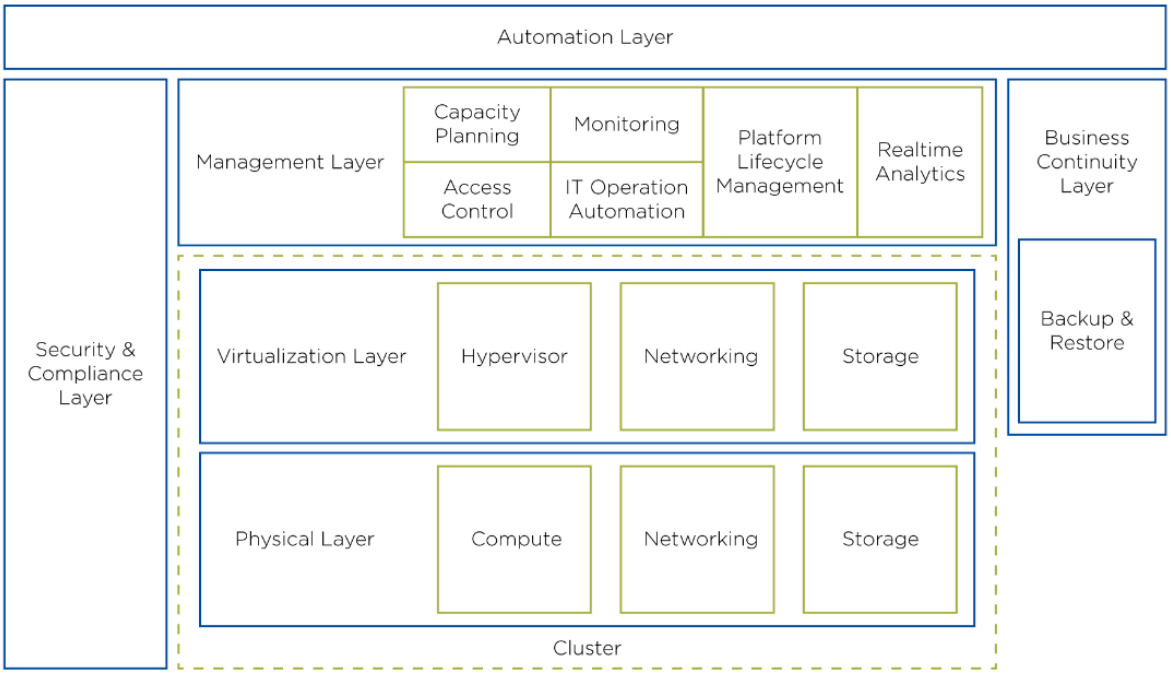


Figure 8: Overview of the Technical Design

Required Software Versions

We used the versions in the following table for this design.

Table: Software Versions

Name	Version	Reasoning
Prism Central	pc.2020.7	Use the latest version available.
Nutanix AOS	5.20	Use the latest version available.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3209

Name	Version	Reasoning
Nutanix AHV	5.15	Use the latest version available.
VMware vSphere	6.7 or 7.0	Use either major release.
VMware vCenter	6.7 or 7.0	Recommended for vSphere deployments.

Physical Layer Design

This section guides you through the process of designing all physical aspects of your Nutanix edge deployment.

Choosing the Cluster Size

When designing a Nutanix cluster, it's important to consider hardware vendor recommendations, security, and operational requirements that may dictate the optimal cluster size. The following table provides a comprehensive list of the design considerations that pertain to cluster size.

Table: Cluster Size Design Considerations

Area	Limiting Factor	Considerations
Operations and manageability	Maintenance window	Define and validate your maintenance window and make sure the cluster upgrade process fits in the window. Example: If you have a maintenance window of 12 hours and a full single node upgrade takes at least 45 minutes, your maximum cluster size is 12–15 nodes.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3210

Area	Limiting Factor	Considerations
Security and compliance	Security zones in an organization or business unit	Collect all relevant security and compliance requirements. Example: You have multiple security zones: internet perimeter, prod, test and dev, and inner perimeter. Every security zone has different cluster sizes: internet-facing perimeter clusters usually have fewer nodes and workloads to minimize impact of a security breach or DDoS attack. Less-critical test and dev clusters may also have more relaxed change management policies and can therefore have many hosts.
Vendor recommendations and limitations	Hypervisor limitations, management plane limitations, and vendor recommendations	Each product has limitations and vendor recommendations. Don't cross boundaries set by the vendor. Check the vendor's limitations and recommendations table.
Business continuity	RPO, RTO, and backup window	Collect BCDR requirements, RPO, RTO, backup and restore time window, and backup system performance statistics. Example: RPO: 24 hours, RTO: 48 hours. Ensure you can recover and restore from backup and restart workloads within 48 hours. A cluster where total storage capacity exceeds the technical capabilities of the backup system could fail to meet desired RTO.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3211

Area	Limiting Factor	Considerations
Workload considerations	Application architecture, application licensing, and application criticality	Verify application architecture with the application team or vendor, including HA, disaster recovery, scale-in vs. scale-out, and performance requirements. For example: Application has its own HA or disaster recovery. If the application can provide native HA or disaster recovery, the RPO and RTO considerations described in the Business continuity row of this table may not apply. Consider the licensing model for each application and its implications. For example: Oracle or MS SQL licensing models are based on physical core count. Design clusters for database performance and capacity requirements to avoid cluster oversizing and minimize license costs.
Networking	Total available network switch ports and available network switch ports per rack	You need to know the available physical ports per rack and rack row when choosing cluster size and number of clusters. For example: A configuration with 96 × 10 Gbps ports available per rack, 48 × 1 Gbps ports available per rack, 2 × 10 Gbps uplinks per Nutanix host, and 1 × 1 Gbps uplink for out-of-band management can have at most 48 nodes per rack (total capacity of the top-of-rack switches).

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3212

Area	Limiting Factor	Considerations
Datacenter facility	Available server rooms, total power and cooling, power and cooling per rack, total available rack units, available rack units per rack, and floor weight capacity	Power and cooling are two of the most important factors limiting Nutanix cluster size and node density. Don't exceed any hard limits when designing your cluster layout. When calculating power consumption and thermal dissipation, use the maximum values provided by vendor. A typical datacenter rack is 42RU. Some datacenters have racks up to 58RU.
One- and two-node clusters	Planned vs. unplanned downtime and scalability	You need to know how to handle planned vs. unplanned events, and you need a plan for scaling beyond one node.

AHV deployments have the following limits:

- A scaled-out implementation of Prism Central on AHV can manage up to 400 clusters, 2,000 nodes, or 25,000 VMs (whichever limit is hit first).

  Note: One- and two-node AHV clusters are only available for ROBO deployments.

VMware vSphere deployments have the following limits:

- A scaled-out implementation of Prism Central on ESXi can manage up to 400 clusters, 2,000 nodes, or 25,000 VMs (whichever limit is hit first).
- VMware vCenter can support 2,000 hosts and 25,000 VMs (turned on).
- A single VMware ESXi cluster can support a minimum of 2 nodes and a maximum of 48.

  › The maximum number of nodes in a Nutanix cluster with ESXi is limited by the hypervisor version. For more details, refer to official VMware vSphere Documentation.

  Note: Two-node ESXi clusters are only available for ROBO deployments.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3213

Failure Domain Considerations

Failure domains are the physical or logical parts of a computing environment or location that are adversely affected when a device or service experiences an issue or outage. The device or services affected greatly influence the size of the failure domain and its potential impact. For example, a router generally has a bigger failure domain than a wireless access point because more endpoints rely on a single router than a single access point. Identifying possible failure domains and keeping them small where possible reduces the chance of widespread disruption.

Building redundancy within and across failure domains helps mitigate the risks of failure. Nutanix clusters are resilient to a drive, node, block, and rack failures because they use redundancy factor 2 by default, allowing Nutanix clusters to self-heal.

Management Plane–Level Failure Domain

One of the most important failure domains is the management plane. The more workload domains a single management plane manages, the bigger the impact of a failure. When deploying the management plane, consider the following risk mitigations to reduce the impact of a failure:

- At a minimum, design to meet the availability requirements of the managed workload or service with the highest uptime requirement.
- Confine workload domain to a single edge site and defined security zone.
- Ensure that the API gateway is always available because other third-party integrations (such as the backup vendor integration) may rely on it.
- Configure built-in RBAC to restrict access to management platform resources.
- Design your management plane to reside in the region or location where your edge clusters reside.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3214

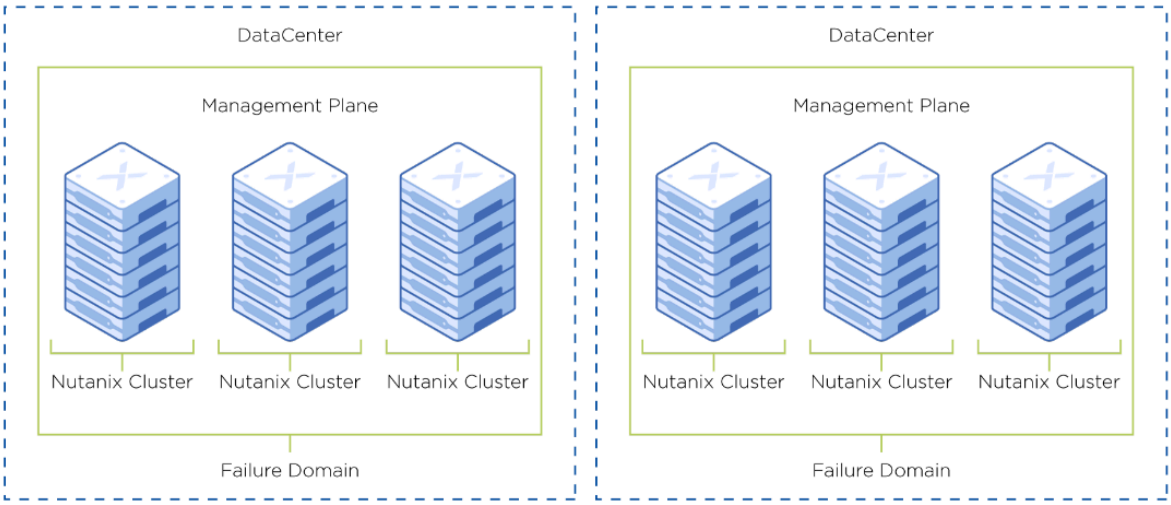


Figure 9: Management Plane Failure Domains

Cluster-Level Failure Domain

Nutanix clusters are another important failure domain. Large clusters result in larger failure domains and potentially higher business impacts, since they typically host considerably more workloads. To mitigate the risk of data unavailability or service disruption, design for redundancy at the cluster level to protect data and services and apply the following mitigations:

- Use redundant power.
- Use redundant top-of-rack switches.
- Ensure redundant upstream connectivity to top-of-rack switches from each Nutanix node.
- Ensure redundant connectivity from edge to central datacenter.
- Use Nutanix scale-out architecture and data protection capabilities to replicate data to a second Nutanix cluster if one cluster fails.
- Deploy the application across multiple clusters.
- For smaller edge sites (fewer than five VMs) with cost constraints, consider implementing two single-node clusters because they operate as independent failure domains without the complexities of managing two-node clusters.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3215

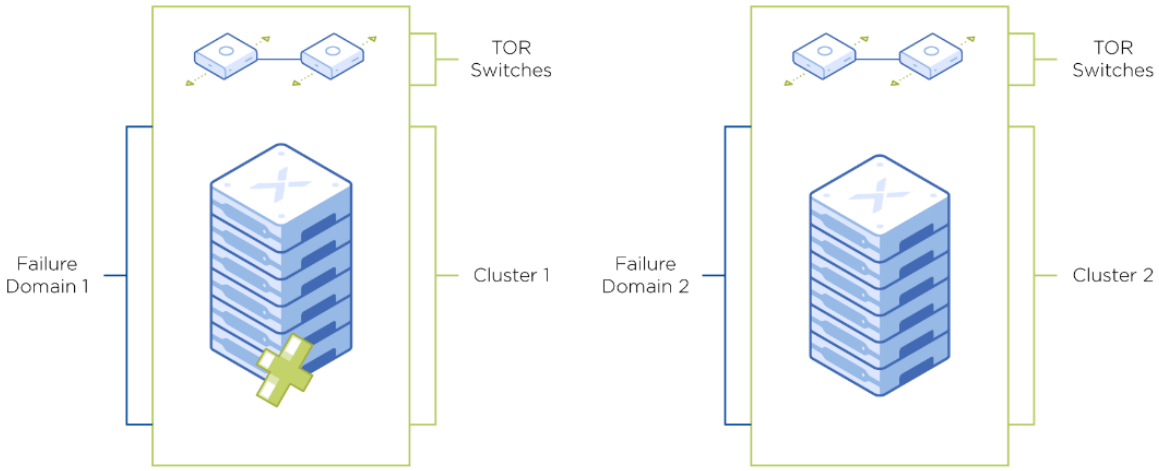


Figure 10: Nutanix Cluster Failure Domains

Rack and Server Room Failure Domains

Edge deployments can have a dedicated server room or a single wiring closet, but both represent a failure domain. Configure your deployment with the following mitigations:

- Use redundant power.
- Use independent cooling.
- Provide a redundant server room in a separate fire zone.
- Place the applications in multiple server rooms. For example, have AD domain controllers in separate server rooms.

If your edge site runs mission-critical workloads, consider mitigating risk by:

- Deploying stretched clusters across two server rooms in the edge site, representing a single failure domain with member nodes distributed across both rooms.
- Deploying two independent clusters across two server rooms in the edge site, representing two independent failure domains

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3216

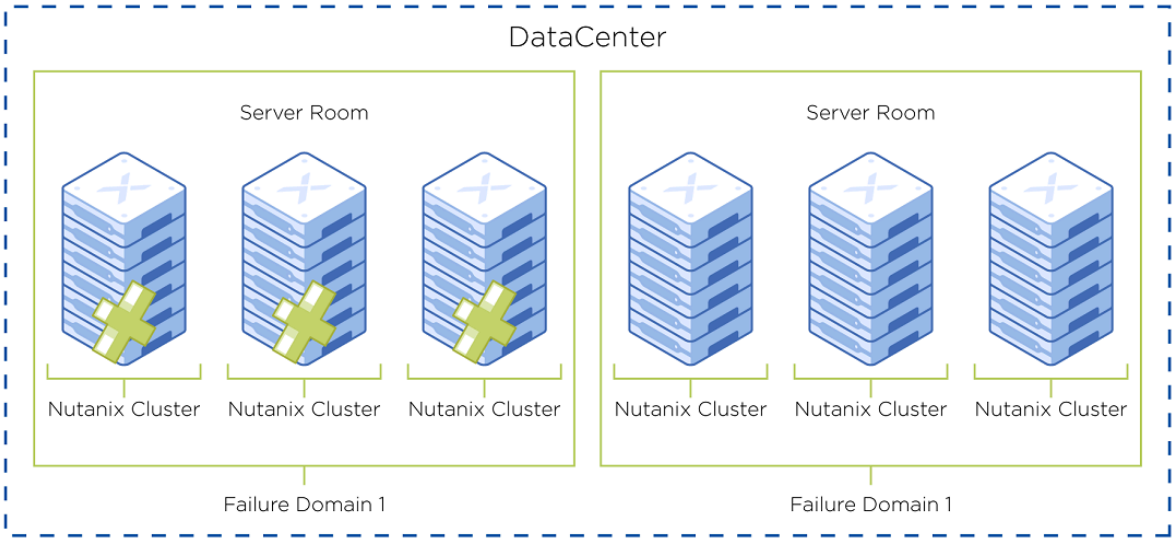


Figure 11: Server Room Failure Domains

Datacenter Failure Domains

Edge sites can lack the IT personnel necessary to assist during a failure scenario and keep the mean time to repair (MTTR) short. You should design your system with the following mitigations:

- Use redundant power.
- Use an independent and redundant cooling system for each datacenter room.
- Ensure redundant networking connectivity from different providers between datacenter buildings.
- Ensure redundant internet connectivity from different providers.
- Where possible, use multiple buildings and server rooms in separate buildings or campuses so that the failure of a single server room doesn't affect production. Distribute multicomponent services equally across datacenter server rooms.
- Ensure strict SLA compliance and keep well-documented resources and processes to help keep MTTR short.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3217

Designing Workload Domains

This design uses a single workload domain at each edge site. Each workload domain consists of a set of Nutanix nodes managed by the same management instance (Prism Central or VMware vCenter) and connected to the same network domain.

A single workload domain can include different hardware and software combinations and have all ESXi or AHV nodes or mix ESXi (running VMs) and AHV (not running VMs) nodes in a single cluster. Single workload domains at edge sites provide the following advantages:

- Efficient space usage
- Default redundancy level
- Simple consumption
- Decreased capex and opex

Note: Using a single workload domain increases the negative effect of a domain failure.

Note: If your edge site runs multiple workloads with different requirements or constraints, consider using multiple workload domains. Refer to the Designing Workload Domains section in the Nutanix Hybrid Cloud Reference Architecture.

Networking for Edge Sites

A Nutanix cluster can tolerate multiple simultaneous failures and protect the cluster's read and write storage capabilities. However, this level of resilience requires a highly available, redundant network connecting a cluster's nodes. Even with intelligent data placement, if network connectivity between more than the allowed number of nodes breaks down, VMs on the cluster could experience write failures and enter read-only mode.

Consult the Physical Networking best practice guide to learn more about general networking guidelines and design requirements and recommendations.

Physical Switches

Edge sites operating as datacenters require datacenter switches with large buffers (10 Gbps or faster), which are critical in a large AOS cluster that sustains critical growth or hosts storage-intensive applications. In this case, see the Physical Switches section of the Nutanix Hybrid Cloud Reference Architecture.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3218

In smaller edge clusters or ROBO deployments that have fewer than eight nodes or don't host write-intensive applications, the switch may not experience buffer contention, and you can relax these switch restrictions. The following switches don't meet high-performance datacenter switch requirements but are acceptable for these smaller edge clusters:

- Arista 7050
- Arista 7150S
- Cisco Catalyst 9000
- Cisco Catalyst 3000
- HPE FM2072

There are some switch types you should never use for any Nutanix deployment:

- Cisco Nexus 2000 (Fabric Extender)
- 10 Gbps expansion cards in a 1 Gbps access switch

Although Nutanix recommends an out-of-band management switch network separate from the primary network in traditional datacenter deployments, for enterprise edge sites these recommendations can be relaxed since the nodes typically have between one and three nodes. Configure IPMI, iLO, or iDRAC server-facing ports in the management network as access ports and don't use VLAN trunking for these ports. Restrict access to this critical management network.

Network Topology

In small edge sites running a handful of VMs, a simple network topology consisting of a pair of top-of-rack switches interconnected to a firewall and router is the simplest option. This simplified setup can address the requirements of a deployment with between one and three nodes.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3219

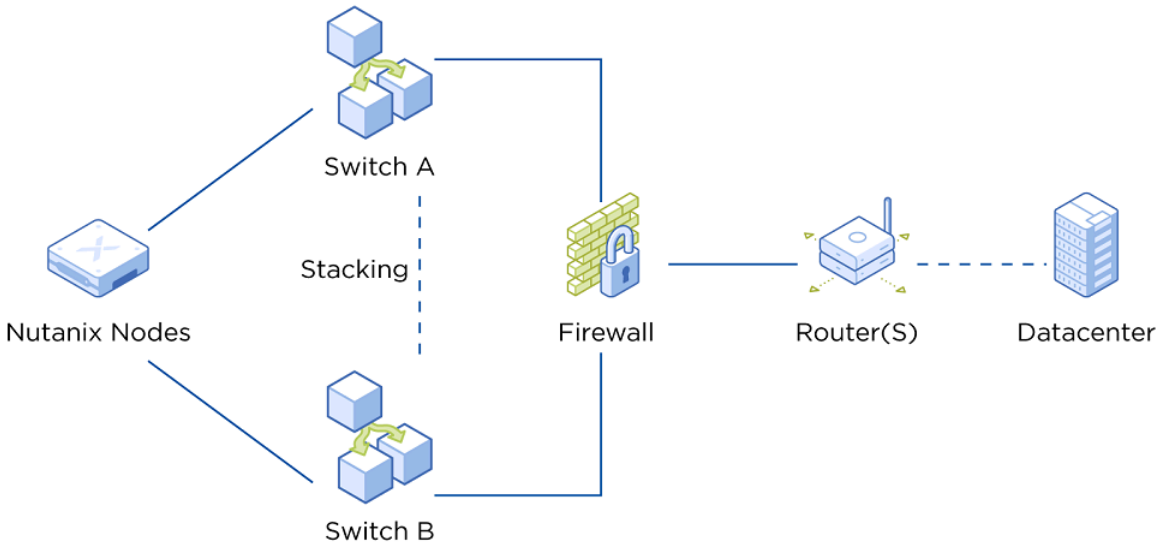


Figure 12: Small Edge Site Network Topology

For medium and larger deployments with multiple racks, Nutanix recommends using a leaf-spine topology because it's easy to scale, achieves high performance with low latency, and provides resilience. A leaf-spine topology requires at least two spine switches and two leaf switches. Every leaf connects to every spine using uplink ports.

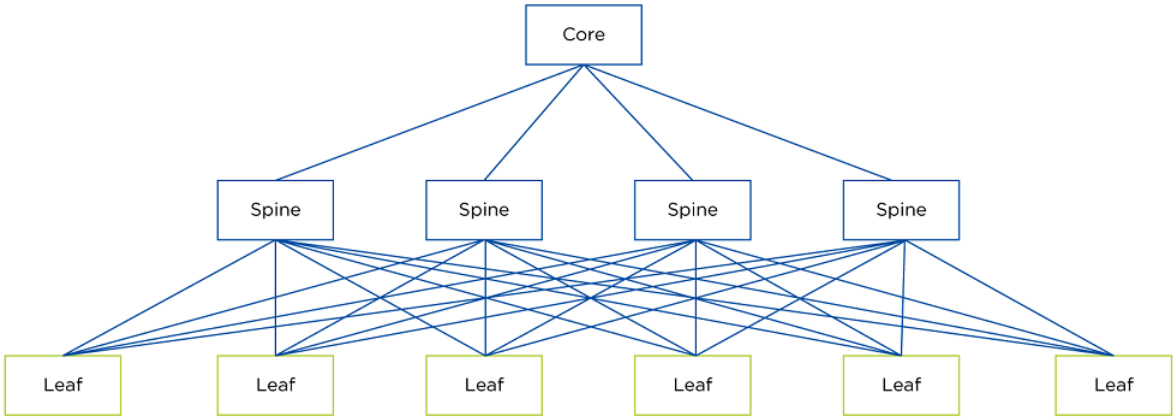


Figure 13: Leaf-Spine Topology for Medium and Larger Edge Sites

Note: If you're considering implementing a leaf-spine network topology, review the Network Topology section in the Nutanix Hybrid Cloud Reference Architecture for specific guidelines and recommendations.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3220

The following list details Nutanix best practices and requirements for edge site network topology:

- Ensure that every Nutanix node in a cluster is in the same layer 2 broadcast domain and shares the same IP subnet.
- You can populate nodes designed exclusively for edge or ROBO with 1 Gbps networking for one- and two-node clusters with latency spikes of approximately 6 to 8 ms.
  - › Limit your cluster size to at most eight nodes if you plan on using 1 Gbps.
- Ensure that when there are two or more nodes in a cluster, each layer of the network topology is highly available and tolerates individual device failures.
  - › Avoid configurations or technologies that don't maintain system availability during single-device outages or upgrades, such as stacked switches.
- Ensure that there are no more than three switches between any two Nutanix nodes in the same cluster.
- Don't use WAN or remote links between Nutanix nodes in the same Nutanix cluster.
- Separate Nutanix CVM and hypervisor hosts in a dedicated VLAN that doesn't include any VM traffic.
- Don't place Nutanix nodes in the same Nutanix cluster if the stretched layer 2 network spans multiple edge sites, buildings, datacenters, or availability zones or if there's a remote link between the two locations.
  - › Using a stretched layer 2 network over a layer 3 network is only acceptable when the Nutanix cluster is in the same switch fabric or aggregation layer, such as when a layer 2 network stretches between two racks in the same datacenter.
- Don't use features like block or rack awareness to stretch a Nutanix cluster between different physical sites.
- Configure adequate uplinks between switches or interswitch links for east-west storage traffic to minimize port-to-port oversubscription. For example, use multiple 40 Gbps uplinks (or interswitch links).
- Connect hosts using redundant links.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3221

- Configure switch ports facing Nutanix servers as spanning tree portfast or edge to skip the listening and learning phases and prevent cluster outages caused by changes to spanning tree topology.
- Configure the CVM and hypervisor VLAN as native, or untagged, on server-facing switch ports. Newly added nodes use untagged traffic for discovery and work out of the box, reducing manual server configuration.
- Use tagged VLANs on the switch ports for all guest workloads to keep the workloads separate from each other and from the CVM and hypervisor network.
- Reduce network oversubscription to ensure as close to a one-to-one ratio as possible. Dropped network packets or a congested network immediately affect storage performance.

Broadcast Domains

Nutanix recommends a traditional layer 2 network design to ensure that CVMs and hosts can communicate in the same broadcast domain even if they're in separate racks. The CVM and host must be in the same broadcast domain and IP subnet.

> **Note:** If you choose a layer 3 network design, refer to the Broadcast Domains section of the Nutanix Hybrid Cloud Reference Architecture.

Network Scalability

Because edge sites are typically small, they contain a simplified core, aggregation, and access layer switch design. In this scenario, to scale, you simply add additional access layer switches, taking into consideration the oversubscription ratios in the design.

If you used a leaf-spine network topology, see the Scaling the Network section of the Nutanix Hybrid Cloud Reference Architecture.

Connectivity to the Core Datacenter

There are multiple ways to establish connectivity from the edge to the core datacenter, including traditional VPNs and direct connect methods. Evaluating the various advantages and disadvantages of each method is beyond the scope of this document; however, keep in mind the latency and bandwidth requirements for edge sites:

- Witness VMs hosted in the cloud can sustain up to 500 ms of latency per 100 instances they manage.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3222

- Prism Central requires at least1.5 Mbps and a maximum latency of 150 ms to run CRUD operations, collect statistics, and perform updates.
- Scheduled replications have no set bandwidth requirements.

AHV Networking

AHV uses Open vSwitch (OVS) for all VM networking. The virtual switch is referred to as a bridge and uses a br prefix in the name. AHV also includes a Linux bridge called virbr0. The virbr0 Linux bridge carries management traffic between the CVM and AHV host. All other storage, host, and workload network traffic flows through the br0 OVS bridge or additional brN bridges if configured.

Read the AHV Networking best practice guide for in-depth guidance on any settings not covered here.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3223

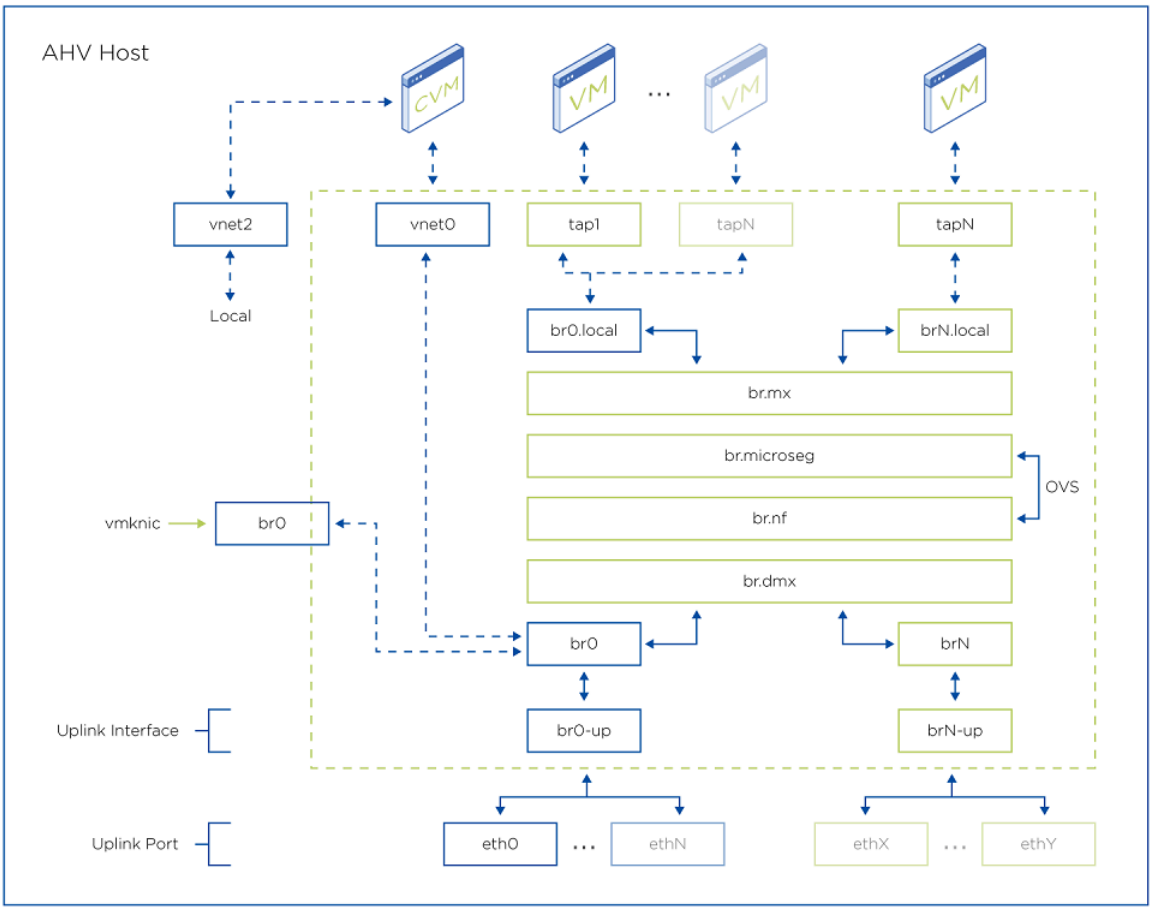


Figure 14: AHV Networking

The following list details the Nutanix best practices and requirements for edge site AHV networking:

- Use only the default bridge, br0, with at least two of the fastest network uplink adapters of the same speed to simplify the design.
  - › Converge the management, storage, and workload traffic on this single pair of uplink adapters.
- Only add additional brN bridges when you need a connection to a separate physical network. For example, if the top-of-rack switch has two pairs of switches—one pair for storage and management and another pair for workload traffic—it makes sense to create another bridge, br1, and place the workloads on this bridge.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3224

- Don't modify the configuration of any bridges inside the AHV host unless following an official Nutanix guide.
- To keep network configuration simple and reduce risk, use the standard 1,500-byte MTU in the hosts, CVMs, and workload VMs. Nutanix doesn't recommend jumbo frames unless specifically required by high-performance Nutanix Volumes iSCSI workloads or specific workload requirements.
  - When switching from 1,500-byte frames to 9,000-byte frames, performance improvements are generally not significant unless the workload uses the maximum network bandwidth for read traffic. For more information on when to use jumbo frames, see the Nutanix Volumes best practice guide and AHV Networking best practice guide.
- Connect at least one 10 Gbps or faster NIC to each tor switch to maintain high availability if one switch is lost.
- Use NICs from the same vendor within a bond to ensure compatibility and prevent undesired failover behavior.
- Use VLANs to separate logical networks. Physical hosts have a limited number of network ports and each port adds complexity. You can separate traffic logically without numerous physical ports.
- To simplify the design, use active-backup uplink load balancing.

vSphere Networking

VMware vSphere networking follows many of the same design decisions as AHV networking. Nutanix hosts with vSphere ESXi use two virtual switches (vSwitches), named vSwitchNutanix and vSwitch0. vSwitchNutanix is the internal, standard vSwitch used for management and storage traffic between the CVM and the hypervisor. vSwitch0 is also a standard vSwitch by default, used for communication between CVMs and workload traffic.

The critical design choices for vSphere networking are covered here, and you can refer to the VMware vSphere Networking best practice guide for more details.

The following list details the Nutanix best practices and requirements for edge site vSphere networking:

- Don't modify vSwitchNutanix.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3225

- Convert vSwitch0 to the virtual distributed switch (VDS) following the instructions in Migrate from a Standard Switch to a Distributed Switch. Converting to the VDS allows you to centrally manage networking for all hosts, instead of configuring each host network individually. The VDS also enables advanced networking functions such as load-based teaming, LACP, and traffic shaping.
- To simplify the design, connect at least two of the fastest adapters of the same speed to vSwitch0 and use the **Route Based on Physical NIC Load** load balancing method to ensure that traffic is balanced between uplink adapters.
  - › Connect these adapters to two separate top-of-rack switches to ensure redundancy.
- Connect at least one 10 Gbps or faster NIC to each top-of-rack switch to maintain high availability if one switch is lost.
- Don't add more vSwitches unless you need to connect to another physical network to meet security or workload requirements.
- All CVM storage, hypervisor host, and workload traffic should flow through vSwitch0, using VLANs to separate the workload traffic and all other traffic.
- Use the default 1,500-byte frame size on all uplinks unless there is a specific performance or application requirement that justifies 9,000-byte jumbo frames.

Virtualization Layer Design

This section describes technical design considerations for Nutanix AHV and VMware ESXi.

Nutanix AHV

AHV delivers virtualization capabilities for the most demanding workloads, and provides an open platform for server virtualization, network virtualization, security, and application mobility. When combined with comprehensive operational insights and virtualization management from Prism and Prism Central, AHV provides a complete datacenter solution.

Nutanix AHV has built-in VM high availability (VMHA) and a resource contention avoidance engine called Acropolis Dynamic Scheduling (ADS). ADS is always on and doesn't require any manual tuning. There are two main levels of VMHA for AHV: best

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3226

effort (no node or memory reservations required) and guarantee (some memory reserved on each node to enable failover). Use the guarantee level for VMHA in production environments and best effort in test and development environments. For additional information, see the Virtual Machine High Availability tech note.

Like VMware's Enhanced vMotion Capability (EVC), which allows VMs to move between different processor generations, AHV determines the lowest processor generation in the cluster and constrains all QEMU domains to that level. This feature enables you to mix processor generations in an AHV cluster and to live-migrate between hosts.

VMware vSphere

If you use vSphere in your enterprise edge deployment, deploy a highly available vCenter instance with an embedded Platform Services Controller to manage the ESXi-based Nutanix clusters. Nutanix upgrade automation features, such as one-click upgrades and LCM, require the advanced control features that vCenter provides. You also need vCenter Server to create and manage the VMware vSphere cluster responsible for the Distributed Resource Scheduler (DRS) and HA, and Prism Central to manage the Nutanix components.

> **Note:** If you're using the disaster recovery runbook automation feature, you need to deploy separate vCenter and Prism Central instances in each region or availability zone.

EVC allows VMs to move between different processor generations in a cluster. EVC mode is a manually configured option, unlike the corresponding feature in AHV. Enable EVC at cluster installation to help ensure that future node additions are seamless. Set EVC mode to the highest compatibility level the cluster processors support.

VMware HA and DRS are core features you should use in your edge site design. Nutanix best practices specify a few HA and DRS configuration changes from the default:

- Enable HA to automatically restart VMs in case of node failure.
- Enable DRS with the default automation level so that it can move VMs as needed to ensure optimal performance.

  > **Note:** Moving VMs may temporarily affect Nutanix data locality.

- Configure **DAS.IGNOREINSUFFICIENTHBDATASTORE** if one Nutanix container is presented to the ESXi hosts to eliminate false positives when a cluster uses a single datastore.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3227

- Disable automation level, HA, and DRS for all CVMs. HA doesn't need to reserve resources for CVMs because they're bound to a single node and can't be restarted elsewhere in the cluster.
- Set Host failures cluster tolerates to **1** for replication factor 2 and **2** for replication factor 3. These settings ensure that the proper resources are automatically reserved for the cluster.
- Set the host isolation response to **Power off and restart VMs** to ensure that VMs are moved to a healthy host and continue to function.
- Set the host isolation response to **Leave powered on** for CVMs. You don't want CVMs to be turned off if there's a transient network disruption.
- Disable Storage I/O Control. If Storage I/O Control is enabled, it can cause storage unavailability, unnecessary lock files, and complications with Metro Availability.

Management Layer Design

Prism Central

There are two deployment architectures for Prism Central that you can use and scale depending on the size and goals of the design:

1. Single-VM Prism Central: One instance in each region or availability. Required if you use the disaster recovery runbook automation feature, which requires that the source and target sites have separate Prism Central instances controlling them. Requires additional cluster resources to run the required VMs.
2. Scaled-out Prism Central cluster: Three-VM cluster. Increases management plane availability and the total number of objects you can manage. Requires additional cluster resources to run the required VMs.

We recommend deploying the scaled-out Prism Central instance for edge sites to simplify capacity planning, platform lifecycle management, and virtual networking management, and to reduce management overhead.

VMware vCenter Server

You can deploy vCenter in many different sizes, and the size ultimately determines how large an environment you can support in terms of VMs, hosts, and clusters. Refer to the

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3228

official VMware documentation for the version you're deploying to determine the proper size for your design.

You can deploy vCenter as a single VM or as a vCenter High Availability (vCenter HA) instance. vCenter HA doesn't increase the size of the environment it can manage because a single virtual appliance is active at any time. The size of the environment that can be managed is based on the size of the VMs deployed.

We recommend deploying one instance of vCenter HA for all workloads and configuring it with Platform Services Controller embedded.

Dependent Infrastructure

There are a variety of other infrastructure services that are necessary for a successful Nutanix deployment, such as NTP, DNS, and AD. You may already have these infrastructure services deployed and available for use when you deploy your Nutanix environment, but if you don't, you need to deploy them as part of the new environment.

NTP

If clock times drift too far apart, some products may have trouble communicating across layers of the solution. Network Time Protocol (NTP) synchronizes computer clock times including network, storage, compute, and software.

The following list details the Nutanix best practices and requirements for NTP for edge sites:

- Configure at least three NTP servers (NTP standard recommendation is five to detect rogue time sources) and ensure that they're accessible at all solution layers, including AOS, AHV, and Prism Central, plus vCenter and ESXi if you're using vSphere.
- Use the same NTP servers for all infrastructure components.
- Don't use an AD domain controller as an NTP source.
- If you're in a dark site with no internet connectivity, use a switch or GPS time source.
- Configure NTP sources specific to the region where the edge clusters reside.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3229

DNS

Domain Name System (DNS) is a directory service that translates domain names of the form domainname.ext to IP addresses. DNS ensures that all layers can resolve names and communicate.

We recommend configuring at least two DNS servers and making them accessible at all layers (AOS, Prism Central, ESXi, vCenter, and network switches) to ensure that components can reliably resolve addresses at all times. We also recommend configuring DNS sources specific to the region where the edge clusters reside.

Active Directory

Active Directory (AD) often serves as the authoritative directory for all applications and infrastructure in an organization. For this design, all the consoles and element managers use RBAC and use AD as the directory service for user and group accounts. Where possible, use AD groups to assign privileges for easier operations. You can then control user access by adding or removing a user from the appropriate group.

Logging Infrastructure

Capturing logs at all layers of the infrastructure is very important. If there is a security incident, logs can be critical for forensics. An example of a robust log collector is Splunk, but there are other options.

The following list details the Nutanix best practices and requirements for logging infrastructure in edge sites:

- Deploy a robust logging platform that meets your security requirements.
- Forward all infrastructure logs to the centralized log repository.
- Store the logs in a different cluster, or location, from where you collect them. This measure protects the logs in case of a catastrophic cluster failure, ensuring they can later be used for forensics.
- Ensure that AD sites and services are set up to define a replication and authentication topology if connectivity to the datacenter is lost.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3230

Security Layer Design

You can build private or multitenant solutions on the Nutanix Cloud Platform, so the security responsibilities vary based on the use case. The security approach includes multiple components:

- Physical
- Virtual infrastructure
- Threat vectors
- Workloads

We designed Nutanix infrastructure to deliver a high level of security with less effort. Nutanix publishes custom security baseline documents for compliance, based on United States Department of Defense (DoD) RHEL 7 Security Technical Implementation Guides (STIGs) that cover the entire infrastructure stack and prescribe steps to secure deployments in the field. The STIGs use machine-readable code to automate compliance against rigorous common standards.

Nutanix provides SCMA by default. SCMA checks multiple security entities for both Nutanix storage and AHV, and Nutanix automatically reports inconsistencies and reverts them to the baseline. With SCMA, you can schedule the STIG to run hourly, daily, weekly, or monthly. The STIG has the lowest system priority in the virtual storage controller, ensuring that security checks don't interfere with platform performance.

In addition, Nutanix releases Security Advisories that describe potential security threats and their associated risks plus any identified mitigations or patches. For more detailed information on Nutanix security and compliance features, see the following documents, separated by category:

- Networking: Flow Network Security tech note
- Information: Information Security tech note
- Cloud: Nutanix DRaaS Security tech note
- Database: Nutanix Era Security tech note

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3231

Authentication Best Practices

- Maintain as few user and group management systems as possible. A centrally managed authentication point is preferred to many separately managed systems.
- You should at least take advantage of the external LDAP support provided by Nutanix components.
- Use AD authentication for user and server accounts to ensure that user activity logged for auditing purposes and account security is configured and maintained from a single centralized solution.
  - › You must have a highly available AD infrastructure and network connection to the datacenter.
- Use an SSL or TLS connection to AD to eliminate cleartext exchanges on the network.

Certificate Best Practices

- Protect all consumer-facing components with certificates signed by a trusted certificate authority to provide an extra layer of security and prevent meddler-in-the-middle (MITM) attacks.
  - › You can use internally or externally signed certificates based on your consumer classification and the service the specific component provides.

Cluster Lockdown Best Practices

Don't use Nutanix or vSphere cluster lockdown (feature that lets you enforce SSH access to CVMs and host using key pairs instead of passwords) unless you require passwordless communication. This decision helps restrict direct access to the CVM and hypervisor to as few entities as possible.

Hardening Best Practices

- Enable Advanced Intrusion Detection Environment (AIDE) for the CVM and AHV. AIDE performs checksum verification for all statis binaries and libraries for improved security.
- Enable stack traces for cluster issues for AHV or ESXi and the CVM.
- Enforce a complex password policy (at least 15 characters long with at least 8 different characters) for the hypervisor and CVM.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3232

- Enable a banner for AHV or ESXi and the CVM that retrieves a specific sign-in message via SSH.
- Enforce only SNMPv3 on the CVM.
- Configure SCMA to run hourly to capture unacceptable configuration drift.
- ESXi only: Stop unused services and close unused firewall ports to limit the attack surface.

  Note: Ensure that you don't stop a service or close a firewall port that's required by Nutanix, such as SSH and NFS.

- Generally, we recommend following the Hardening Controller VM section of the AOS Security Guide. If you're using AHV, follow the Hardening AHV section of the AOS Security Guide.

Internet-Facing Services Best Practices

We recommend using multiple internet connections (active-backup) and ISP-provided denial-of-service (DoS) and distributed-denial-of-service (DDoS) filtering to help mitigate the potential effects of a DoS or DDoS attack.

Logging Best Practices

- Configure and maintain a single centralized logging solution for auditing purposes and account security.
- Send log files to a highly available syslog infrastructure.
- At least one of the individual targets of the highly available logging infrastructure should run outside the virtual infrastructure itself so that if the virtual infrastructure is compromised, forensic investigations can access logs that might not be available on the cluster itself.
- Include data from all Nutanix modules and components in logging using the error-log level and ensure that they're searchable. See the Configuring the Remote Syslog Server Settings section of the Acropolis Advanced Administration Guide for more information.
- Use default ESXi logging levels, log rotation, and log file sizes.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3233

- If you have additional security and reliability requirements, use TCP for log transport. Otherwise, use the default syslog protocol, UDP.
- Use port 514 (defined port in syslog RFC) for logging.

Network Segmentation Best Practices

- To protect Nutanix CVM and hypervisor traffic, place them together in their own dedicated VLAN, separate from other VM traffic. This configuration applies to all hosts in a cluster or single node.
- Place out-of-band management on a separate VLAN or physical network to provide additional security.
- We recommend configuring the CVM and hypervisor host VLAN as a native, or untagged, VLAN on the connected switch ports to allow easy node addition and cluster expansion.
- Don't segment Nutanix storage and replication traffic, or iSCSI Volumes traffic, on separate interfaces (VLAN or physical) unless additional segmentation is required by mandatory security policy or the use of separate physical networks.

Role-Based Access Control (RBAC) Best Practices

- Use a least-privilege and separation-of-duties approach when assigning RBAC permissions to ensure that each group or individual user has just enough permissions to perform their duties. Use predefined roles or create new roles as needed.
- Configure RBAC at the Prism Central level because it provides the overlying management construct. This configuration ensures that your least-privilege configuration stays in place and avoids common mistakes that occur when RBAC is configured at multiple different levels.
- Align RBAC structure and default plus custom roles with your company requirements.

Data-at-Rest Encryption Best Practices

> **Note:** AHV encrypts the entire Nutanix cluster, while ESXi gives you the option to define encryption on a per-Nutanix-container basis if required.

- Keep management traffic, including storage traffic, on a separate network.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3234

- Don't use storage encryption.
- Don't use a key management server (KMS).

> **Note:** All methods of DaRE are FIPS 140-2 compliant. However, if you require levels 2, 3, or 4, you also need a hardware component.

Microsegmentation and Firewall Best Practices

- Use Flow Network Security (previously Flow Microsegmentation) to comply with regulatory and business-specific compliance policies such as PCI-DSS, HIPAA, and NIST.
- Use a Palo Alto Networks VM-Series firewall with Flow Network Security to provide advanced threat and vulnerability detection for layers 4–7.

For more information on Flow Network Security, see the Flow Network Security software documentation and the Flow Network Security tech note. For additional information on deploying the Palo Alto VM-Series on AHV, see the Palo Alto Networks VM-Series Firewalls on Xi tech note and the Nutanix and Palo Alto Networks Service Chain Integration Guide.

Automation Layer Design

Nutanix supports intelligent IT operations and advanced automation that enable you to streamline operations, enable IT as a service, and support the needs of developers and business teams. This section covers virtual infrastructure automation and orchestration, focusing on provisioning and maintenance.

Life Cycle Manager (LCM)

Nutanix LCM determines any software and firmware dependencies, intelligently prioritizes updates, and automates the entire upgrade process across all clustered hosts, without any impact to applications or data availability. It supports one-click upgrades across multiple qualified hardware manufacturers and configurations, so IT teams have the flexibility to deploy the best hardware for each use case and still benefit from centralized upgrade capabilities.

LCM offers the best software and firmware upgrade experience for clusters with three or more nodes. In this design, the nodes can locally coordinate data synchronization,

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3235

VM evacuation and migration, and node recovery and availability during the upgrade process for the firmware and software on the individual nodes. The individual nodes might restart multiple times, and that entire process is automated through LCM without affecting applications and data.

Certain LCM features aren't supported when your cluster contains one or two nodes:

- In a one-node scenario, the LCM software and firmware upgrades aren't supported because there's no hardware redundancy. In this design, the user must plan their downtime and trigger the software upgrade manually via Prism or use the respective hardware manufacturer's management tools.
- In a two-node scenario, LCM software and firmware is supported, but during the upgrade process, data synchronization across nodes takes more time because there's only one other node in the cluster to absorb the changes. You must complete witness upgrades separately from data-carrying node upgrades. For this reason, we recommend a larger maintenance window for two-node clusters.

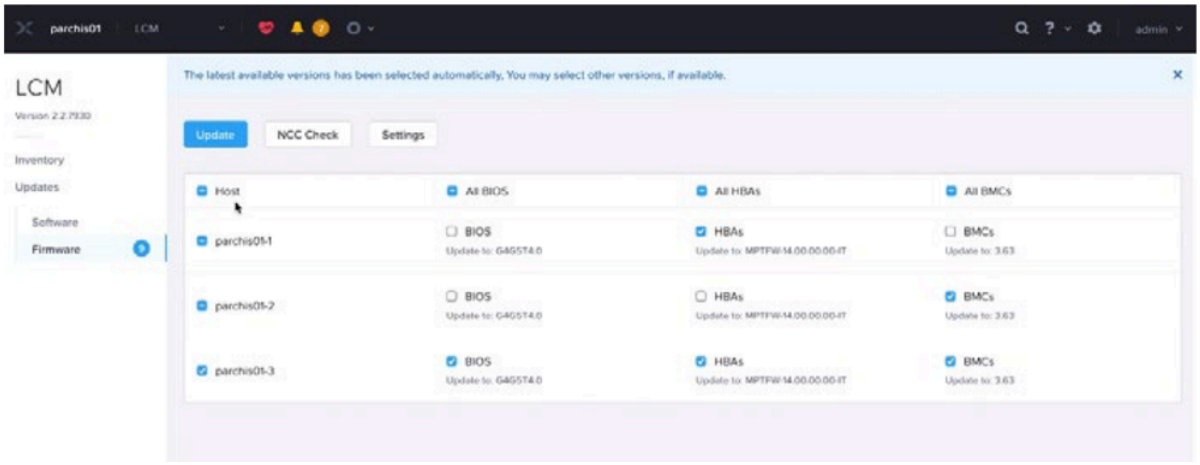


Figure 15: Life Cycle Manager

Foundation

Foundation manages the initial setup and configuration of a cluster. Nutanix nodes can come with AHV and the CVM preinstalled, and with Foundation you can:

- Add the nodes to an existing Nutanix cluster.
- Create a new Nutanix cluster.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3236

- Reimage the nodes with different a AHV and or AOS version or different hypervisor and create a Nutanix cluster.

  Note: The Foundation process may vary for different hardware vendors.

  Nutanix provides a Foundation preconfiguration service that you can install from nutanix.com. With the service, you can define and download the Nutanix cluster configuration to be used during the Foundation process. The downloaded file contains all configuration required to perform the Foundation operation and comes in json format, which makes it easy to keep track of configurations, document them, and share with your peers.

  See the Field Installation Guide for the functions available for the different Foundation software options.

Foundation Central

Foundation Central enables you to create clusters from factory-imaged nodes and reimage existing nodes that are already registered with Foundation Central remotely from Prism Central. This feature enables you to create clusters on remote sites without having to arrange a personnel visit.

Foundation Central has the following limitations:

- Foundation Central supports creation of a one-node cluster without imaging on factory-shipped nodes with AOS and any hypervisor installed.
- Foundation Central supports creation of a one-node cluster with imaging only on nodes that are shipped with DiscoveryOS installed.
- Imaging logs for the remote nodes aren't available on Prism Central. You can only access these logs in the nodes.
- Foundation Central doesn't support updating the CVM memory and hostname for one-node cluster creation without imaging.

Nutanix Calm

Calm provides infrastructure and application automation and life cycle management for the Nutanix enterprise cloud and public clouds. It provisions, scales, and manages infrastructure and applications across multiple environments to make the entire IT infrastructure more agile and application-centric. Building an enterprise or service

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3237

provider cloud solution with Nutanix Calm helps organizations with delivery and ongoing management of infrastructure, applications, and custom services, leading to lower opex.

We recommend reviewing the Nutanix Calm Reference Architecture guide for further information on implementing Nutanix Calm

Operations Design

> **Note:** We recommend purchasing the Nutanix Cloud Manager (NCM) Starter license, which gives you access to analytics, capacity planning, custom dashboards, and playbooks for Prism Central.

Native runway calculations built into Prism Central automatically calculate the remaining capacity of the system as soon as the Prism Element instance is brought under Prism Central management. Configure these runway calculations to run as part of periodic reports and review them on a regular basis (at least monthly) to ensure that sufficient capacity exists. This configuration is especially important for organizations that have a significant lag between when they commit to purchase additional gear and when the gear is online and available to use.

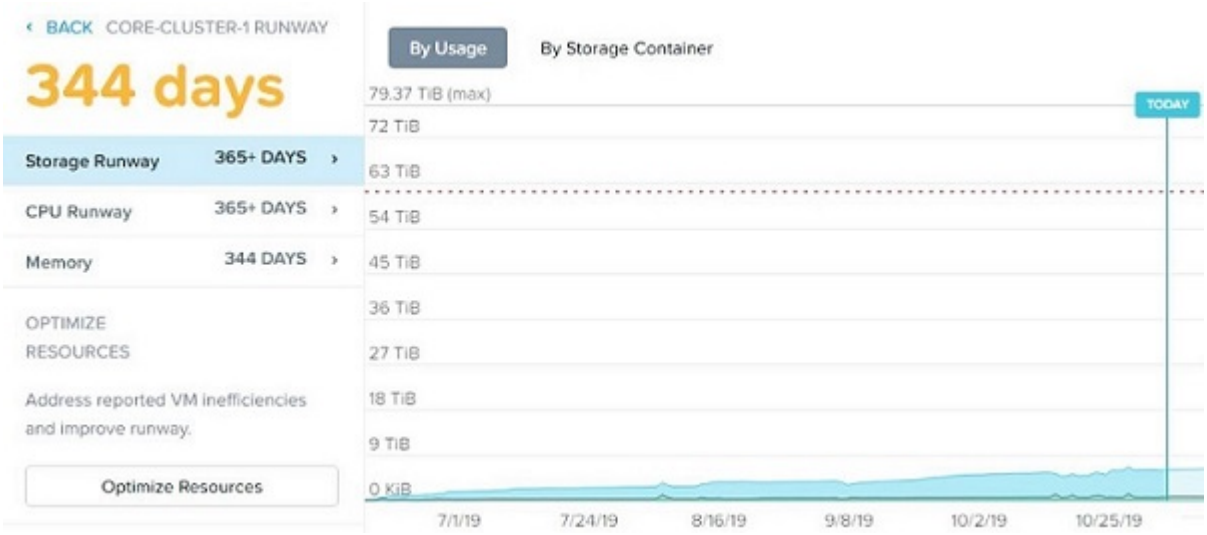


Figure 16: Capacity Runway

Accurate and efficient system-level planning requires accurate sizing for individual workloads. Machine learning in Prism Central provides anomaly detection for VMs when the workload crosses learned thresholds. The system also categorizes VMs based on their behavior, and you can create custom alert policies that match VMs by conditions.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3238

Operations Best Practices and Requirements

- Review capacity planning monthly.
- Perform updates after hours for performance- or migration-sensitive applications to reduce the load on the system.
- Use the latest supported release.
- Update to the next maintenance version four weeks after release and to the current patch version two weeks after release to keep updates relatively small.
- Maintain a preproduction environment to test any necessary changes to firmware, software, or hardware before implementing the change in production. Preproduction environments can help you avoid the cost of outages.
- Configure alerts and alert policies in Prism Central, not Prism Element, to create consistency across multiple clusters and reduce the effort involved in making multiple changes. Prism Central–based alert policies also allow you to detect anomalies.
- Use SMTP for alert transmission to create consistency across multiple clusters, reduce the effort involved in making multiple changes, enable anomaly detection, and offer more options for delivery.

BCDR Design

Nutanix provides a range of data protection features. Our general recommendation for BCDR design is: If an application has native data protection mechanisms (Exchange database availability groups (DAG), SQL Server Always On, Oracle RAC), use those to provide application BCDR. If an application doesn't provide a data protection mechanism, use the built-in Nutanix protection mechanisms.

Consult the Multi-Datacenter Design for Nutanix Core and BC/DR section of the Nutanix Hybrid Cloud Reference Architecture for considerations and strategies for multi-datacenter designs.

BCDR Logical Implementations for Edge Sites

Disaster recovery patterns for edge sites vary from organization to organization, but one-to-one and many-to-one implementations are the most common.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3239

One-to-One

For smaller environments with only a pair of locations, protect applications between two availability zones in the same region or across regions. You can protect the same workload or application with different RPO thresholds. The availability zone location you choose (same region or across regions) defines the RPO value for the protected application or workload: If an application or workload requires RPO 0, choose availability zones in the same region (latency requirement for RPO 0 is 5 ms RTT or less).

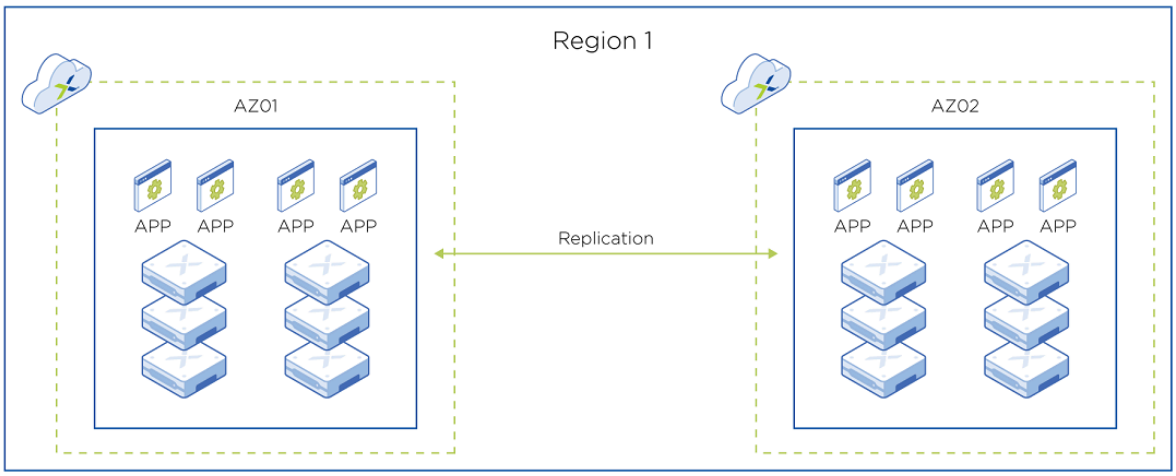


Figure 17: Two Availability Zones in the Same Region

Many-to-One

The many-to-one pattern maps multiple source edge clusters to single disaster recovery target Nutanix cluster or core datacenter. In the most common configuration, each edge location is a separate availability zone that replicates data to the disaster recovery hub, which is located in a separate availability zone in the same region.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3240

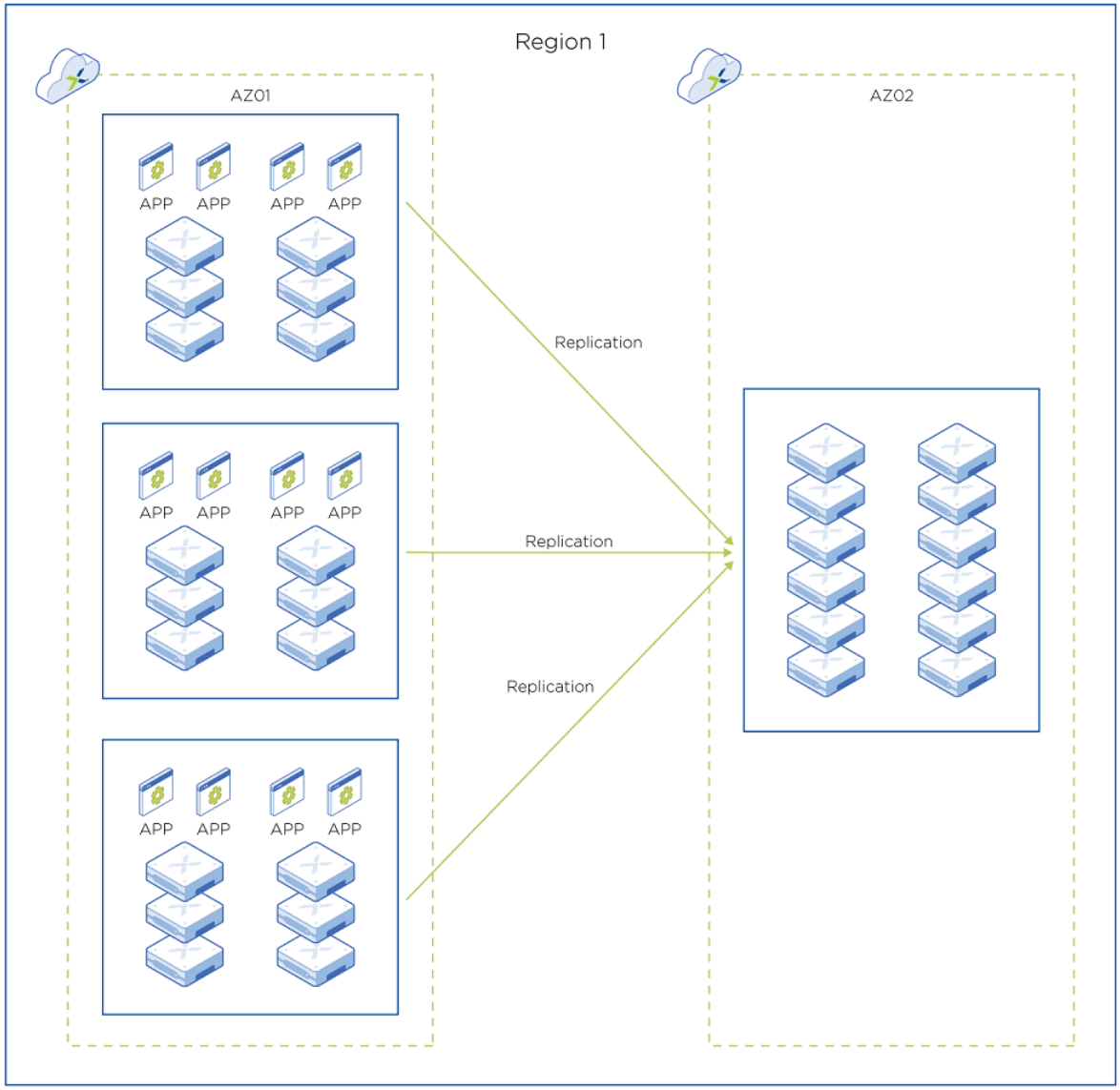


Figure 18: Multiple Availability Zones in a Single Region

You can also have multiple availability zones across multiple regions.

© 2024 Nutanix, Inc. All rights reserved

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3241

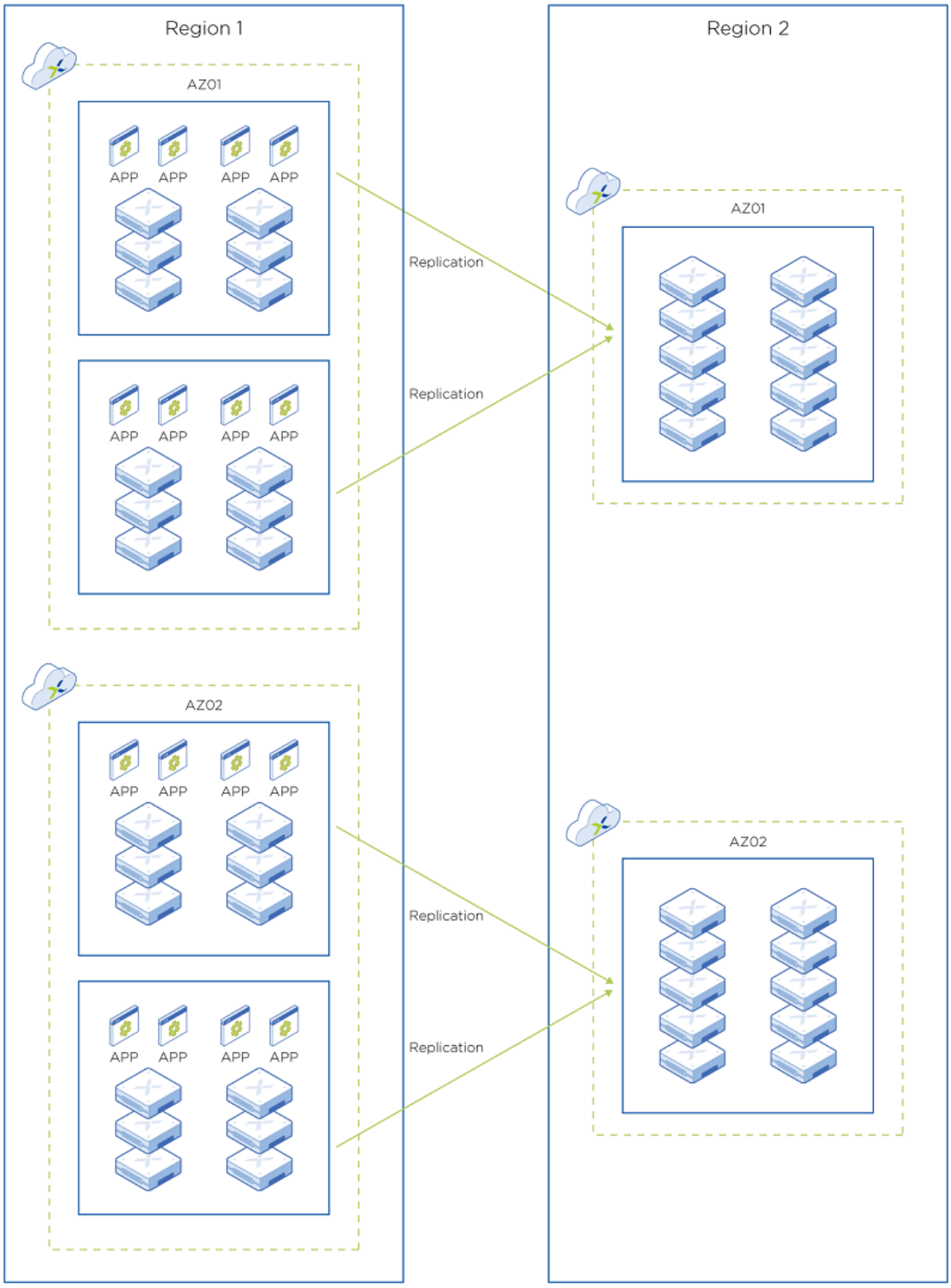


Figure 19: Multiple Availability Zones across Multiple Regions

© 2024 Nutanix, Inc. All rights reserved |

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3242

Note: Consult the Nutanix Hybrid Cloud Reference Architecture to evaluate other implementations.

Nutanix BCDR Solutions

A good disaster recovery solution involves different levels of service because applications have different levels of criticality to the business and therefore different disaster recovery requirements. For this reason, this document includes multiple architectures for a variety of scenarios. The following flow chart walks through the decision tree for choosing the best Nutanix disaster recovery solution for your requirements.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3243

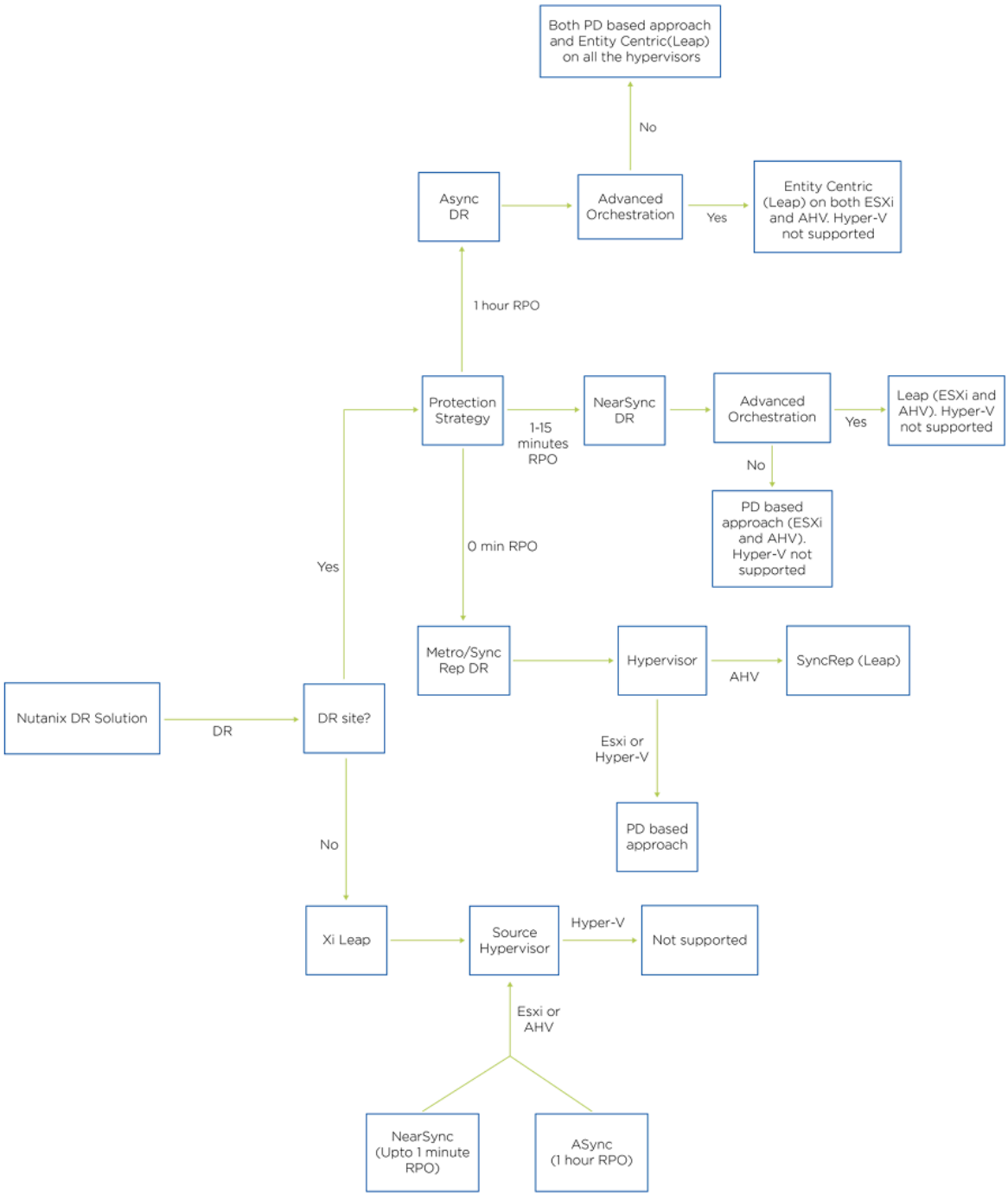


Figure 20: Disaster Recovery Decision Flowchart

© 2024 Nutanix, Inc. All rights reserved

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3244

1. Nutanix Metro Availability
   a. Pros: Can provide zero data loss (RPO 0), minimal to zero recovery time (RTO 0), and RTO 0 during a disaster recovery avoidance event.
   b. Cons: Requires stretched layer 2 networking of some form between edge sites or within the Edge site, requires a Nutanix Cloud Infrastructure Ultimate license, is only supported with ESXi, and is highly dependent on the network connectivity being resilient and providing a high enough throughput to accommodate application change rates.
   c. See the Metro Availability best practice guide on the Nutanix Support Portal for more information.
2. Synchronous replication
   a. Pros: Available with Nutanix AHV or VMware vSphere. Protects workloads with RPO 0. Used when you can't provide spanned L2 across datacenters but still need to provide RPO 0 to applications.
   b. Cons: Requires high bandwidth and low latency, requires a Nutanix Cloud Infrastructure Ultimate license or an advanced replication add-on license, only supported with Nutanix Disaster Recovery (previously Leap), and requires that the source cluster have more than three nodes.
3. NearSync replication
   a. Pros: Provides an RPO between 1 and 15 minutes to storage-intensive workloads over limited connectivity.
   b. Cons: Capacity of each SSD in the cluster must be at least 1.2 TB, only supported with Nutanix Disaster Recovery, requires a Nutanix AOS Enterprise license or a Leap Advanced Add-On license, and requires that the source cluster have more than three nodes.
4. Asynchronous replication
   a. Pros: Provides an RPO of one hour or more to applications using low-bandwidth, high-latency datacenter links.
   b. Cons: Requires a Nutanix AOS Enterprise license or Leap Advanced Add-On License and requires that the source cluster have more than three nodes.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3245

General BCDR Best Practices and Requirements

- Keep as few VMs per protection domain as possible in your design.
  - › If you're using asynchronous replication, configure at most 200 VMs per protection domain.
  - › If you're using NearSync replication, configure at most 10 VMs per protection domain.
- Group VMs with similar RPO requirements in the same protection domain.
  - › Node size and capacity can limit the possible RPO for the VMs running on it. See the Resource Requirements Supporting Snapshot Frequency (Asynchronous, NearSync and Metro) section of the Data Protection and Recovery with Prism Element guide for details.
- Put NearSync VMs in their own protection domains (NearSync can only have one schedule).
- Limit consistency groups to fewer than 10 VMs.
- Only use consistency groups for applications with a shared state, such as database replicas.
- Only add one VM to any consistency group that uses application-consistent snapshots.
- Configure snapshot intervals to be shorter than your desired RPO to allow for failure and recovery without manual intervention. The interval should be half your desired RPO including data transmission timing.
- Configure snapshot schedules to retain the minimum number of snapshots needed to meet your retention policy.
- If you're using synchronous replication, create one container on the source and one on the destination with the same name.
- If you're using synchronous replication, ensure that the two participating clusters are within 5 ms round trip time (RTT) of each other.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3246

- Use Metro Availability for business-critical applications that require zero data loss (RPO 0), minimal to zero recovery time (RTO 0), or RTO 0 during a disaster recovery avoidance event.
  - › Metro Availability is only supported with ESXi.

For additional details, see the Data Protection and Recovery with Prism Element guide on the Nutanix Support Portal.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3247

6. Optional Nutanix Products and Services

Nutanix offers optional products and services that you can choose to incorporate when implementing enterprise edge solutions on the Nutanix platform. These options can help you quickly satisfy unique organizational requirements.

- Nutanix Cloud Manager: NCM Starter and Pro licenses add to the base capabilities of Nutanix Prism to provide monitoring, analytics, and automation capabilities from a single management interface.
- Nutanix Cloud Clusters (NC2): NC2 extends the Nutanix stack to the public cloud, creating a single management domain that spans private and public clouds and removes the friction from multicloud operations. For more information, see the Nutanix Cloud Clusters on AWS tech note and the Disaster Recovery with Nutanix Cloud Clusters (NC2) on AWS tech note.
- Flow Network Security: Microsegmentation and other capabilities offered by Flow Network Security further enhance the security of your Nutanix operations.
- Nutanix Files: Files enables Nutanix clusters with full-featured file services capabilities, eliminating the need for standalone NAS appliances or file servers.
- Nutanix Objects: Objects enables a Nutanix cluster to provide S3-compatible, software-defined, scale-out object stores for a variety of use cases, eliminating the need for standalone object storage while supporting applications that rely on object stores with an on-premises alternative.
- Nutanix Mine: Mine is an integrated backup solution that combines the benefits of the Nutanix architecture with the capabilities of proven backup vendors.
- NCM Self-Service: NCM Self-Service (previously Calm) provides application-level orchestration and lifecycle management, simplifying application management and enabling self-service.
- Karbon: Karbon integrates certified Kubernetes with the Nutanix operating environment, enabling Nutanix clusters to support both VM- and container-based applications while simplifying Kubernetes deployment and management.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3248

7. Conclusion

The Nutanix Cloud Platform remains a common platform for both traditional datacenters and enterprise edge sites. This document is intended to demonstrate valuable methods and practices that organizations, both large and small, can use to implement Nutanix solutions to solve their IT and business problems. There is no one-size-fits-all solution for enterprise edge deployments; this document is only intended to provide customers with suggested best practices they can use to design and evolve their private, hybrid, and multicloud solutions.

For more information on any details of this document, please visit our website at www.nutanix.com or reach out to our sales team. You can also contact one of the many global support phone numbers listed on our website. For feedback or questions, please contact us using the Nutanix NEXT Community forums.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3249

8. Appendix

Best Practices for Enterprise Edge Sites

High-Level Design Best Practices

- Logically group the manageability, replication, and BCDR components of your edge sites in a single region or availability zone.
- Use Prism Central as the primary control plane.
  - › If you use ESXi, you also need VMware vCenter.
- Use the simplified block-and-pod architecture detailed in the Block and Pod Architecture section of the Nutanix Hybrid Cloud Reference Architecture.
  - › Large-scale sites (more than four blocks with the expectation of additional blocks in the future) with the characteristics of a datacenter should reference the Nutanix Hybrid Cloud Reference Architecture.
- Build clusters with one or three nodes.
  - › If you need to be able to scale your edge solution beyond two nodes or add storage-only nodes to the cluster, you should implement a three-node cluster.
- If you use them, deploy storage-only nodes in pairs.
  - › You can only use storage-only nodes in clusters with three or more nodes.
- Define an SOP that stipulates how to scale one- or two-node clusters in your design, as this step isn't a function of the core AOS and doesn't have a workflow.

Software Best Practices

Use the following software versions:

- Prism Central: pc.2020.7
- Nutanix AOS 5.20

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3250

- Nutanix AHV 5.15
- VMware vSphere 6.7 or 7.0
- VMware vCenter 6.7 or 7.0

Failure Domain Best Practices

- Design and deploy the management plane to be highly available.
- At a minimum, design to meet the availability requirements of the managed workload or service with the highest uptime requirement.
- Confine workload domain to a single edge site.
- Confine workloads domain to a defined security zone.
- Ensure that the API gateway is always available because other third-party integrations (such as the backup vendor integration) may rely on it.
- Configure built-in RBAC to restrict access to management platform resources.
- Design your management plane to reside in the region or location where your edge clusters reside.
- Use redundant power from two different power supplies.
- Use redundant top-of-rack switches.
- Ensure redundant upstream connectivity to top-of-rack switches from each Nutanix node.
- Ensure redundant connectivity from edge to central datacenter.
- Use Nutanix scale-out architecture and data protection capabilities to replicate data to a second Nutanix cluster if one cluster fails.
- Deploy the application across multiple clusters.
- Use an independent and redundant cooling system for each datacenter room.
- Ensure redundant networking connectivity from different providers between datacenter buildings.
- Ensure redundant internet connectivity from different providers.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3251

- Where possible, use multiple buildings and server rooms in separate buildings or campuses so that the failure of a single server room doesn't affect production. Distribute multicomponent services equally across datacenter server rooms.
- Ensure strict SLA compliance and keep well-documented resources and processes to help keep MTTR short.

General Networking Best Practices

- Configure IPMI, iLO, or iDRAC server-facing ports in the management network as access ports and don't use VLAN trunking for these ports. Restrict access to this critical management network.
- Never use these switches for Nutanix deployments:
  - Cisco Nexus 2000 (Fabric Extender)
  - 10 Gbps expansion cards in a 1 Gbps access switch
- In small edge sites running a handful of VMs, use a simple network topology consisting of a pair of top-of-rack switches interconnected to a firewall and router.
- In medium and larger deployments with multiple racks, use a leaf-spine topology because it's easy to scale, achieves high performance with low latency, and provides resilience.
- Ensure that every Nutanix node in a cluster is in the same layer 2 broadcast domain and shares the same IP subnet.
- You can populate nodes designed exclusively for edge or ROBO with 1 Gbps networking for one- and two-node clusters with latency spikes of approximately 6–8 ms.
  - Limit your cluster size to at most eight nodes if you plan on using 1 Gbps networking.
- Ensure that when there are two or more nodes in a cluster, each layer of the network topology is highly available and tolerates individual device failures.
  - Avoid configurations or technologies that don't maintain system availability during single-device outages or upgrades, such as stacked switches.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3252

- Ensure that there are no more than three switches between any two Nutanix nodes in the same cluster.
- Don't use WAN or remote links between Nutanix nodes in the same Nutanix cluster.
- Separate Nutanix CVM and hypervisor hosts in a dedicated VLAN that doesn't include any VM traffic.
- Don't place Nutanix nodes in the same Nutanix cluster if the stretched layer 2 network spans multiple edge sites, buildings, datacenters, or availability zones or if there's a remote link between the two locations.
  - › Using a stretched layer 2 network over a layer 3 network is only acceptable when the Nutanix cluster is in the same switch fabric or aggregation layer, such as when a layer 2 network stretches between two racks in the same datacenter.
- Don't use features like block or rack awareness to stretch a Nutanix cluster between different physical sites.
- Configure adequate uplinks between switches or interswitch links for east-west storage traffic to minimize port-to-port oversubscription. For example, use multiple 40 Gbps uplinks (or interswitch links).
- Connect hosts using redundant links.
- Configure switch ports facing Nutanix servers as spanning tree portfast or edge to skip the listening and learning phases and prevent cluster outages caused by changes to spanning tree topology.
- Configure the CVM and hypervisor VLAN as native, or untagged, on server-facing switch ports. Newly added nodes use untagged traffic for discovery and work out of the box, reducing manual server configuration.
- Use tagged VLANs on the switch ports for all guest workloads to keep the workloads separate from each other and from the CVM and hypervisor network.
- Reduce network oversubscription to ensure as close to a one-to-one ratio as possible. Dropped network packets or a congested network immediately affect storage performance.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3253

AHV Networking Best Practices

- Use only the default bridge, br0, with at least two of the fastest network uplink adapters of the same speed to simplify the design.
  - › Converge the management, storage, and workload traffic on this single pair of uplink adapters.
- Only add additional brN bridges when you need a connection to a separate physical network. For example, if the top-of-rack switch has two pairs of switches—one pair for storage and management and another pair for workload traffic—it makes sense to create another bridge, br1, and place the workloads on this bridge.
- Don't modify the configuration of any bridges inside the AHV host unless following an official Nutanix guide.
- To keep network configuration simple and reduce risk, use the standard 1,500-byte MTU in the hosts, CVMs, and workload VMs. Nutanix doesn't recommend jumbo frames unless specifically required by high-performance Nutanix Volumes iSCSI workloads or specific workload requirements.
  - › When switching from 1,500-byte frames to 9,000-byte frames, performance improvements are generally not significant unless the workload uses the maximum network bandwidth for read traffic. For more information on when to use jumbo frames, see the Nutanix Volumes best practice guide and AHV Networking best practice guide.
- Connect at least one 10 Gbps or faster NIC to each tor switch to maintain high availability if one switch is lost.
- Use NICs from the same vendor within a bond to ensure compatibility and prevent undesired failover behavior.
- Use VLANs to separate logical networks. Physical hosts have a limited number of network ports and each port adds complexity. You can separate traffic logically without numerous physical ports.
- To simplify the design, use active-backup uplink load balancing.

vSphere Networking Best Practices

- Don't modify vSwitchNutanix.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3254

- Convert vSwitch0 to the virtual distributed switch (VDS) following the instructions in Migrate from a Standard Switch to a Distributed Switch. Converting to the VDS allows you to centrally manage networking for all hosts, instead of configuring each host network individually. The VDS also enables advanced networking functions such as load-based teaming, LACP, and traffic shaping.
- To simplify the design, connect at least two of the fastest adapters of the same speed to vSwitch0 and use the **Route Based on Physical NIC Load** load balancing method to ensure that traffic is balanced between uplink adapters.
  - › Connect these adapters to two separate top-of-rack switches to ensure redundancy.
- Connect at least one 10 Gbps or faster NIC to each top-of-rack switch to maintain high availability if one switch is lost.
- Don't add more vSwitches unless you need to connect to another physical network to meet security or workload requirements.
- All CVM storage, hypervisor host, and workload traffic should flow through vSwitch0, using VLANs to separate the workload traffic and all other traffic.
- Use the default 1,500-byte frame size on all uplinks unless there is a specific performance or application requirement that justifies 9,000-byte jumbo frames.

Virtualization Best Practices

- If you're using the disaster recovery runbook automation feature, you need to deploy separate vCenter and Prism Central instances in each region or availability zone.
- Enable HA to automatically restart VMs in case of node failure.
- Enable DRS with the default automation level so that it can move VMs as needed to ensure optimal performance.

  Note: Moving VMs may temporarily affect Nutanix data locality.
- Configure **DAS.IGNOREINSUFFICIENTHBDATASTORE** if one Nutanix container is presented to the ESXi hosts to eliminate false positives when a cluster uses a single datastore.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3255

- Disable automation level, HA, and DRS for all CVMs. HA doesn't need to reserve resources for CVMs because they're bound to a single node and can't be restarted elsewhere in the cluster.
- Set Host failures cluster tolerates to **1** for replication factor 2 and **2** for replication factor 3. These settings ensure that the proper amount of resources are automatically reserved for the cluster.
- Set the host isolation response to **Power off and restart VMs** to ensure that VMs are moved to a healthy host and continue to function.
- Set the host isolation response to **Leave powered on** for CVMs. You don't want CVMs to be turned off if there's a transient network disruption.
- Disable Storage I/O Control. If Storage I/O Control is enabled, it can cause storage unavailability, unnecessary lock files, and complications with Metro Availability.

Management Best Practices

- Deploy a scaled-out Prism Central instance for edge sites to simplify capacity planning, platform lifecycle management, and virtual networking management, and to reduce management overhead.
- Deploy one instance of vCenter HA for all workloads and configure it with Platform Services Controller embedded.
- Configure at least three NTP servers (NTP standard recommendation is five to detect rogue time sources) and ensure that they're accessible at all solution layers, including AOS, AHV, and Prism Central, plus vCenter and ESXi if you're using vSphere.
- Use the same NTP servers for all infrastructure components.
- Don't use an AD domain controller as an NTP source.
- If you're in a dark site with no internet connectivity, use a switch or GPS time source.
- Configure NTP sources specific to the region where the edge clusters reside.
- Configuring at least two DNS servers and make them accessible at all layers (AOS, Prism Central, ESXi, vCenter, and network switches) to ensure that components can reliably resolve addresses at all times.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3256

- Configure DNS sources specific to the region where the edge clusters reside.
- Use RBAC for all the consoles and element managers and use AD as the directory service for user and group accounts.
- Where possible, use AD groups to assign privileges for easier operations.
- Deploy a robust logging platform that meets your security requirements.
- Forward all infrastructure logs to the centralized log repository.
- Store the logs in a different cluster, or location, from where you collect them. This measure protects the logs in case of a catastrophic cluster failure, ensuring they can later be used for forensics.
- Ensure that AD sites and services are set up to define a replication and authentication topology in the event that connectivity to the datacenter is lost.

Security Best Practices

Authentication

- Maintain as few user and group management systems as possible. A centrally managed authentication point is preferred to many separately managed systems.
- You should at least take advantage of the external LDAP support provided by Nutanix components.
- Use AD authentication for user and server accounts to ensure that user activity logged for auditing purposes and account security is configured and maintained from a single centralized solution.
  - › You must have a highly available AD infrastructure and network connection to the datacenter.
- Use an SSL or TLS connection to AD to eliminate cleartext exchanges on the network.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3257

Certificates

- Protect all consumer-facing components with certificates signed by a trusted certificate authority to provide an extra layer of security and prevent meddler-in-the-middle (MITM) attacks.
  - › You can use internally or externally signed certificates based on your consumer classification and the service the specific component provides.

Cluster Lockdown

- Don't use Nutanix or vSphere cluster lockdown (feature that lets you enforce SSH access to CVMs and host using key pairs instead of passwords) unless you require passwordless communication.

Hardening

- Enable Advanced Intrusion Detection Environment (AIDE) for the CVM and AHV. AIDE performs checksum verification for all statis binaries and libraries for improved security.
- Enable stack traces for cluster issues for AHV or ESXi and CVM.
- Enforce a complex password policy (at least 15 characters long with at least 8 different characters) for the hypervisor and CVM.
- Enable a banner for AHV or ESXi and the CVM that retrieves a specific sign-in message via SSH.
- Enforce only SNMPv3 on the CVM.
- Configure SCMA to run hourly to capture unacceptable configuration drift.
- ESXi only: Stop unused services and close unused firewall ports to limit the attack surface.

  Note: Ensure that you don't stop a service or close a firewall port that's required by Nutanix, such as SSH and NFS.

- Generally, we recommend following the Hardening Controller VM section of the AOS Security Guide. If you're using AHV, follow the Hardening AHV section of the AOS Security Guide.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3258

Internet-Facing Services

- Use multiple internet connections (active-backup) and ISP-provided denial-of-service (DoS) and distributed-denial-of-service (DDoS) filtering to help mitigate the potential effects of a DoS or DDoS attack.

Logging

- Configure and maintain a single centralized logging solution for auditing purposes and account security.
- Send log files to a highly available syslog infrastructure.
- At least one of the individual targets of the highly available logging infrastructure should run outside the virtual infrastructure itself so that if the virtual infrastructure is compromised, forensic investigations can access logs that might not be available on the cluster itself.
- Include data from all Nutanix modules and components in logging using the error-log level and ensure that they're searchable. See the Configuring the Remote Syslog Server Settings section of the Acropolis Advanced Administration Guide for more information.
- Use default ESXi logging levels, log rotation, and log file sizes.
- If you have additional security and reliability requirements, use TCP for log transport. Otherwise, use the default syslog protocol, UDP.
- Use port 514 (defined port in syslog RFC) for logging.

Network Segmentation

- To protect Nutanix CVM and hypervisor traffic, place them together in their own dedicated VLAN, separate from other VM traffic. This configuration applies to all hosts in a cluster or single node.
- Place out-of-band management on a separate VLAN or physical network to provide additional security.
- We recommend configuring the CVM and hypervisor host VLAN as a native, or untagged, VLAN on the connected switch ports to allow easy node addition and cluster expansion.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3259

- Don't segment Nutanix storage and replication traffic, or iSCSI Volumes traffic, on separate interfaces (VLAN or physical) unless additional segmentation is required by mandatory security policy or the use of separate physical networks.

Role-Based Access Control (RBAC)

- Use a least-privilege and separation-of-duties approach when assigning RBAC permissions to ensure that each group or individual user has just enough permissions to perform their duties. Use predefined roles or create new roles as needed.
- Configure RBAC at the Prism Central level because it provides the overlying management construct. This configuration ensures that your least-privilege configuration stays in place and avoids common mistakes that occur when RBAC is configured at multiple different levels.
- Align RBAC structure and default plus custom roles with your company requirements.

Data-at-Rest Encryption

- Keep management traffic, including storage traffic, on a separate network.
- Don't use storage encryption.
- Don't use a key management server (KMS).

Microsegmentation and Firewall

- Use Flow Network Security (previously Flow Microsegmentation) to comply with regulatory and business-specific compliance policies such as PCI-DSS, HIPAA, and NIST.
- Use a Palo Alto Networks VM-Series firewall with Flow Network Security to provide advanced threat and vulnerability detection for layers 4–7.

Operations Best Practices

- Purchase the Nutanix Cloud Manager (NCM) Starter license, which gives you access to analytics, capacity planning, custom dashboards, and playbooks for Prism Central.
- Review capacity planning monthly.
- Perform updates after hours for performance- or migration-sensitive applications to reduce the load on the system.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3260

- Use the latest supported release.
- Update to the next maintenance version four weeks after release and to the current patch version two weeks after release to keep updates relatively small.
- Maintain a preproduction environment to test any necessary changes to firmware, software, or hardware before implementing the change in production. Preproduction environments can help you avoid the cost of outages.
- Configure alerts and alert policies in Prism Central, not Prism Element, to create consistency across multiple clusters and reduce the effort involved in making multiple changes. Prism Central–based alert policies also allow you to detect anomalies.
- Use SMTP for alert transmission to create consistency across multiple clusters, reduce the effort involved in making multiple changes, enable anomaly detection, and offer more options for delivery.

BCDR Best Practices

- Keep as few VMs per protection domain as possible in your design.
  - › If you're using asynchronous replication, configure at most 200 VMs per protection domain.
  - › If you're using NearSync replication, configure at most 10 VMs per protection domain.
- Group VMs with similar RPO requirements in the same protection domain.
  - › Node size and capacity can limit the possible RPO for the VMs running on it. See the Resource Requirements Supporting Snapshot Frequency (Asynchronous, NearSync and Metro) section of the Data Protection and Recovery with Prism Element guide for details.
- Put NearSync VMs in their own protection domains (NearSync can only have one schedule).
- Limit consistency groups to fewer than 10 VMs.
- Only use consistency groups for applications with a shared state, such as database replicas.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3261

- Only add one VM to any consistency group that uses application-consistent snapshots.
- Configure snapshot intervals to be shorter than your desired RPO to allow for failure and recovery without manual intervention. The interval should be half your desired RPO including data transmission timing.
- Configure snapshot schedules to retain the minimum number of snapshots needed to meet your retention policy.
- If you're using synchronous replication, create one container on the source and one on the destination with the same name.
- If you're using synchronous replication, ensure that the two participating clusters are within 5 ms round trip time (RTT) of each other.
- Use Metro Availability for business-critical applications that require zero data loss (RPO 0), minimal to zero recovery time (RTO 0), or RTO 0 during a disaster recovery avoidance event.
  - › Metro Availability is only supported with ESXi.

References

1. AHV best practice guide
2. AHV Networking best practice guide
3. Data Efficiency tech note
4. Data Protection and Disaster Recovery best practices guide
5. Disaster Recovery with Nutanix Cloud Clusters (NC2) on AWS tech note
6. Flow Network Security tech note
7. Hybrid Cloud Reference Architecture
8. Information Security tech note
9. Nutanix AHV Virtualization tech note
10. Nutanix DRaaS Security tech note
11. Nutanix Era Security tech note
12. Nutanix Hardware Compatibility Lists
13. Nutanix Volumes best practice guide

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3262

14. Palo Alto Networks VM-Series Firewalls on Xi tech note
15. Physical Networking best practice guide
16. Prism tech note
17. ROBO Deployment and Operations
18. Security Advisories
19. Virtual Machine High Availability tech note
20. VMware vSphere best practice guide
21. VMware vSphere Documentation

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3263

About Nutanix

Nutanix offers a single platform to run all your apps and data across multiple clouds while simplifying operations and reducing complexity. Trusted by companies worldwide, Nutanix powers hybrid multicloud environments efficiently and cost effectively. This enables companies to focus on successful business outcomes and new innovations. Learn more at Nutanix.com.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3264

List of Figures

Figure 1: Availability Zones in a Region..... 12
Figure 2: Edge Sites in an Availability Zone..... 13
Figure 3: Single Site, Multiple Availability Domains, Active-Active..... 15
Figure 4: Single Site, Multiple Availability Domains, Active-Passive..... 16
Figure 5: Multiple Sites, Fan-In or Central Datacenter..... 17
Figure 6: Multiple Sites, Chain Structure..... 19
Figure 7: Overview of Nutanix Recoverability Options..... 23
Figure 8: Overview of the Technical Design..... 32
Figure 9: Management Plane Failure Domains..... 38
Figure 10: Nutanix Cluster Failure Domains..... 39
Figure 11: Server Room Failure Domains..... 40
Figure 12: Small Edge Site Network Topology..... 43
Figure 13: Leaf-Spine Topology for Medium and Larger Edge Sites..... 43
Figure 14: AHV Networking..... 47
Figure 15: Life Cycle Manager..... 59
Figure 16: Capacity Runway..... 61
Figure 17: Two Availability Zones in the Same Region..... 63
Figure 18: Multiple Availability Zones in a Single Region..... 64
Figure 19: Multiple Availability Zones across Multiple Regions..... 65
Figure 20: Disaster Recovery Decision Flowchart..... 67

NX-3155-G9 System Specifications

Platform ANY

NX-3155-G9

December 4, 2024

NUTANIX

Contents

1. System Specifications.....3
   Node Naming (NX-3155-G9).....3
      NX-3155-G9 System Specifications.....4
      NX-3155-G9 GPU Specifications.....10

2. Component Specifications.....11
   Controls and LEDs for Single-node Platforms.....11
   Network Card LED Description.....13
   Power Supply Unit Redundancy and Node Configuration.....15

3. Memory Configurations.....16
   Supported Memory Configurations.....16

4. Nutanix Hardware Naming Convention.....19

Copyright.....21
   License.....21
   Conventions.....21
   Default Cluster Credentials.....21
   Version.....22

1

SYSTEM SPECIFICATIONS

Node Naming (NX-3155-G9)

Nutanix assigns a name to each node in a block, which varies by product type.

The NX-3155-G9 block contains a single node named Node A. It supports hard disk drives (HDD) and non-volatile memory express (NVMe) drives.

Only drive slots 4, 5, 7, 8, 10, and 11 can be populated. All other drive slots must remain empty for thermal reasons.

Figure 1: NX-3155-G9 Front Panel

Table 1: Supported Drive Configurations

Hybrid NVMe + HDD	Two NVMe drives in slots 4 and 5; four HDDs in slots 7, 8, 10, and 11; all other drive slots empty
All-NVMe	Two, four, or six NVMe drive in slots 4, 5, 7, 8, 10, and 11; all other drive slots empty

NX-3155-G9 supports partial population of drives for all-NVMe configurations, with a minimum of two drives. When adding drives in the field, populate the drives two by two, from left to right, in the active drive slots. The NX-3155-G9 does not support odd-numbered drive configurations. Hybrid NVMe + HDD configurations do not support partial population of drives.

Hybrid NVMe + HDD configuration is offered only as a factory installation. You cannot convert an all-NVMe node to a hybrid NVMe + HDD node in the field.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3268

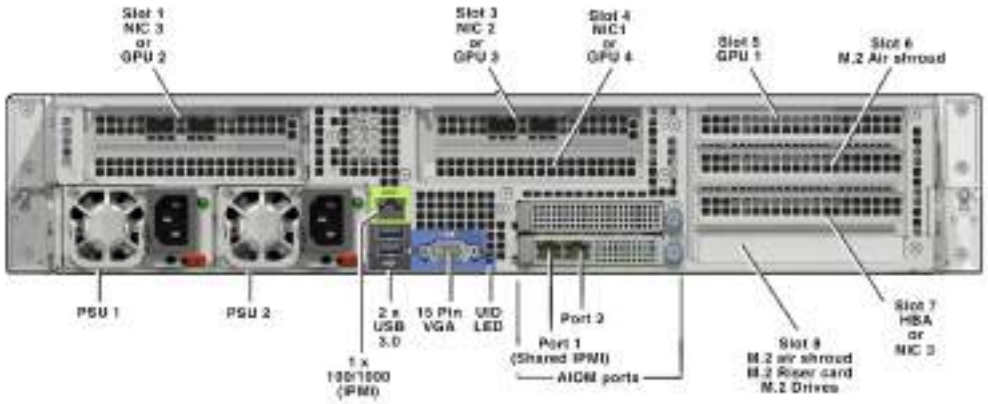


Figure 2: NX-3155-G9 Back Panel

NX-3155-G9 System Specifications

Table 2: System Characteristics

Boot Device	Boot Drive • 2 x 512GB M.2 Boot Device
Chassis	Chassis • 2U1N LFF Chassis

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3269

CPU	Processor Dual Intel Xeon® 5th Gen. (Emerald Rapids) • 2 x Intel Xeon® Silver 4510 [12 cores / 2.40 GHz] • 2 x Intel Xeon® Silver 4514Y [16 cores / 2.00 GHz] • 2 x Intel Xeon® Silver 4516Y+ [24 cores / 2.20 GHz] • 2 x Intel Xeon® Gold 5515+ [8 cores / 3.20 GHz], Excluded from ENERGY STAR certification. • 2 x Intel Xeon® Gold 6526Y [16 cores / 2.80 GHz] • 2 x Intel Xeon® Gold 6542Y [24 cores / 2.90 GHz] • 2 x Intel Xeon® Gold 5520+ [28 cores / 2.20 GHz] • 2 x Intel Xeon® Gold 6548Y+ [32 cores / 2.50 GHz] Dual Intel Xeon® 4th Gen. (Sapphire Rapids) • 2 x Intel Xeon® Silver 4410T [10 cores / 2.70 GHz], Excluded from ENERGY STAR certification. • 2 x Intel Xeon® Silver 4410Y [12 cores / 2.00 GHz] • 2 x Intel Xeon® Silver 4416+ [20 cores / 2.00 GHz] • 2 x Intel Xeon® Gold 5415+ [8 cores / 2.90 GHz], Excluded from ENERGY STAR certification. • 2 x Intel Xeon® Gold 5420+ [28 cores / 2.00 GHz] • 2 x Intel Xeon® Gold 6416H [18 cores / 2.20 GHz] • 2 x Intel Xeon® Gold 6426Y [16 cores / 2.50 GHz] • 2 x Intel Xeon® Gold 6442Y [24 cores / 2.60 GHz] • 2 x Intel Xeon® Gold 6448Y [32 cores / 2.10 GHz]
GPU	Graphics Card • 0, 1 or 2 x NVIDIA A16 64GB • 0, 1 or 2 x NVIDIA A40 48GB • 0, 1 or 2 x NVIDIA H100 80GB (Qualified but not sold by Nutanix) • 0, 1 or 2 x NVIDIA L40 48GB (Qualified but not sold by Nutanix) • 0, 1 or 2 x NVIDIA L40S 48GB • 0, 1, 2, 3 or 4 x NVIDIA A2 16GB (ESXi Only) • 0, 1, 2, 3 or 4 x NVIDIA L4 24GB

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3270

Memory	**Note:** • The 96 GB memory configurations are only available with Emerald Rapids processors. • The minimum memory configuration required for Energy STAR 4.0 certification is 512 GB. If memory is less than 512 GB, the platform is not Energy Star certified, even if the CPU is certified. 32GB DIMM • 4 x 32 GB = 128 GB • 8 x 32 GB = 256 GB • 12 x 32 GB = 384 GB • 16 x 32 GB = 512 GB • 24 x 32 GB = 768 GB • 32 x 32 GB = 1024 GB 64GB DIMM • 4 x 64 GB = 256 GB • 8 x 64 GB = 512 GB • 12 x 64 GB = 768 GB • 16 x 64 GB = 1024 GB • 24 x 64 GB = 1536 GB • 32 x 64 GB = 2048 GB 96GB DIMM • 16 x 96 GB = 1536 GB • 24 x 96 GB = 2304 GB • 32 x 96 GB = 3072 GB 128GB DIMM • 4 x 128 GB = 512 GB • 8 x 128 GB = 1024 GB • 12 x 128 GB = 1536 GB • 16 x 128 GB = 2048 GB • 24 x 128 GB = 3072 GB • 32 x 128 GB = 4096 GB

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3271

Network	Ports on Serverboard • 1x 1GbE Dedicated IPMI AIOM • 1 x 2P 10GBase-T (Port 1 is shared IPMI) • 1 x 2P 10GBase-T + 2P SFP+ (Port 1 is shared IPMI) Add on NICs in PCIe slots • 0, 1, 2 or 3 x 10GbE 4P NIC • 0, 1, 2 or 3 x 10GBaseT 2P NIC • 0, 1, 2 or 3 x 10GBaseT 4P NIC • 0, 1, 2 or 3 x 25GbE 2P NIC
Network Cables	Network Cable • 1M-SFP28 • 3M-SFP28 • 3M-SFP+ • 5M-SFP28 • 5M-SFP+
Power Cable	Power Cable • C13/14 4ft Power Cable
Power Supply	Power Supply • 2 x PWS, 2000W
Server	Server • 1 x NX-3155-G9 Server
Storage	
All NVMe	2, 4 or 6 x NVMe • 1.92TB • 3.84TB • 7.68TB • 15.36TB

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3272

NVMe+HDD	2 x NVMe • 3.84TB • 7.68TB • 15.36TB 4 x HDD • 8TB • 12TB • 18TB
Storage Controller	Storage Controller • 1 x Broadcom 3816 Host Bus Controller (HBA), required for SATA/SAS based drive support
TPM	TPM • 0 or 1 x Unprovisioned Trusted Platform Module
Transceiver	Transceiver • SR SFP+ Transceiver
VGA	1 x VGA connector per node (15-pin female)
Chassis fans	4 x 80 mm heavy-duty fans with PWM fan speed controls.

Table 3: Block, power and electrical

Block	• Height : 88.1 mm • Depth : 799 mm • Width : 445.6 mm Maximum configuration (without rails and accessory kits) • Weight : 25.5 kg
Package	Package maximum weight with rails and accessory kits • Weight : 36.36 kg
Shock	10ms, square wave, one shock on each side • Non-Operating : 20 G 10ms, half-sine, one shock on each side • Operating : 5 G

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3273

Thermal Dissipation	• Typical : 4665 BTU/hr • Maximum : 6663 BTU/hr
Vibration (Random)	5 to 200 Hz., approx. 30 min./axis • Non-Operating : 0.98 Grms 5 to 500 Hz., approx. 15 min./axis • Operating : 0.21 Grms
Vibration (Sinusoidal)	5 to 200 Hz., approx. 15 min./axis • Operating : 0.25 G 5 to 200 Hz., approx. 15 min./axis • Non-Operating : 0.5 G
Power consumption (calculated)	**Note:** • For the power consumption calculations, Max NIC and disk configurations are considered. Max Config • Maximum: 1954 VA • Typical: 1368 VA
Operating environment	Operating temperature : 10-25C Non-Operating temperature : -20-70C Operating relative humidity : 20-85% Non-operating relative humidity : 5-95%

Certifications

- BIS
- BSMI
- CE
- CSA
- CSAus
- EAC
- Energy Star
- FCC
- ICES

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3274

- KCC
- RCM
- Reach
- RoHS
- S-MARK
- SABS
- SII
- UKCA
- UKRSEPRO
- UL
- VCCI-A
- WEEE
- cUL

NX-3155-G9 GPU Specifications

The following table provides minimum firmware and software versions for GPUs supported by NX-3155-G9:

Table 4: Minimum Firmware and Software Versions When Using a GPU Card

Firmware or Software	NVIDIA A2	NVIDIA A16/A40	NVIDIA L40S/L4
BIOS	EH10.201	EH10.201	EH10.201
BMC	01.00.07	01.00.07	01.00.07
Hypervisor	ESXi only	ESXi and AHV	ESXi and AHV
Foundation	5.4.2 with Foundation-platforms-2.13.3	5.4.2 with Foundation-platforms-2.13.3	5.4.2 with Foundation-platforms-2.13.3
AOS	6.5.3.5	6.5.3.5	6.5.3.5
NCC	4.6.5.2	4.6.5.2	4.6.5.2
NVIDIA vGPU driver	GRID 15.2	GRID 15.2	GRID 16.1

2

COMPONENT SPECIFICATIONS

Controls and LEDs for Single-node Platforms

Figure 3: Front Panel Controls and Indicators

Table 5: Front Panel Controls and Indicators

LED or Button	Function
Power button	Power button applies or removes primary power from the power supply to the system (System standby power maintains)
Power LED	Solid green: Indicates power is supplied to the system power supply units. This LED is illuminated when the system is operating normally.
UID/Reset button	Turns information LED *i* On/Off (Single press) Reboots the system (Press and hold for 6s)
Drive LED	Not used
NIC LED (AIOM Port 1)	Indicates network activity on AIOM 10Gbase-T port 1
NIC LED (AIOM Port 2)	Indicates network activity on AIOM 10Gbase-T port 2
Multiple Function *i* LED	Solid blue: UID activated locally Blinking blue: UID activated remotely

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3276

LED or Button	Function
	Solid red: Overheat condition
	Blinking red at 0.25Hz: Power supply failure
	Flashing red at 1Hz: Fan failure

Note: NIC1 and NIC2 LED in the table above are specific to the AIOM only. If it is a dual port AIOM, then NIC1 LED is controlled by one port and NIC2 LED is controlled by the other port.

Table 6: Drive LEDs

Top LED: Activity	Blue or green, blinking = I/O activity, off = idle
Bottom LED: Status	Red solid = failed drive, On five seconds after boot = power on

Back Panel Controls and Indicators

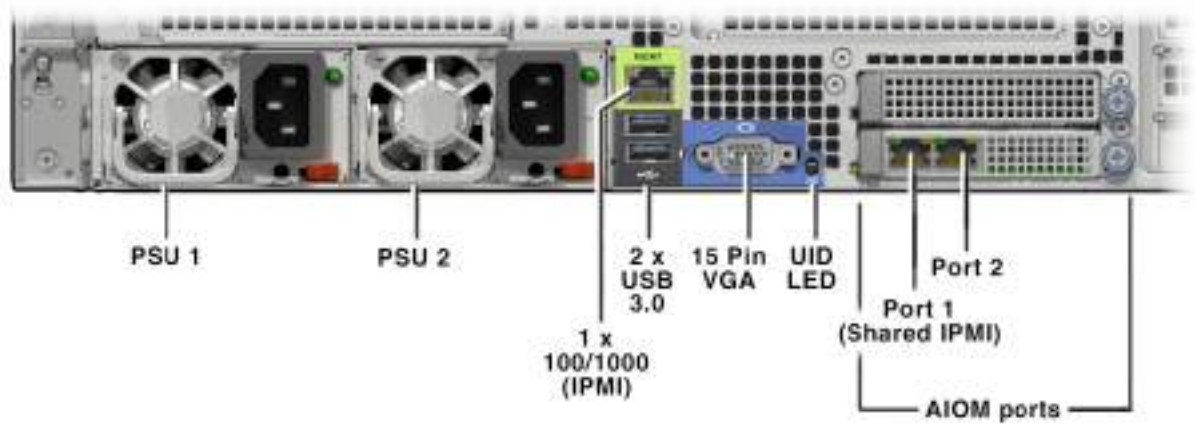


Figure 4: Back Panel Controls and Indicators

Table 7: Back Panel Controls and Indicators

Name	Color	Function
IPMI, Link LED (Left)	Solid Green	100 Mbps
	Solid Amber	1 Gbps
IPMI, Activity LED (Right)	Blinking Amber	Active
AIOM, Link LED (Left)	Off	No link
	Green	Linked at 10 Gb/s
	Amber	Linked at 1 Gb/s
AIOM, Activity LED (Right)	Off	No activity
	Blinking Green	Link up (traffic flowing)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3277

Name	Color	Function
Locator LED (UID)	Blue	Blinking - Node identified

Table 8: Power Supply LED Indicators

Power supply condition	LED status
No AC power to all power supplies	Off
Power supply critical events that cause a shutdown: **Failure**, **Over Current Protection**, **Over Voltage Protection**, **Fan Fail**, **Over Temperature Protection**, **Under Voltage Protection**.	Steady amber
Power supply warning events. Power supply continues to operate. High temperature, over voltage, under voltage and other conditions.	Blinking amber (1 Hz)
When AC is present only: 12VSB on (PS off) or PS in sleep state	Blinking green (1 Hz) minute
Output on and OK	Steady green
AC cord unplugged	Steady amber
Power supply firmware updating mode	Blinking green (2 Hz)

For add-on NIC LED indications, see Network Card LED Description on page 13.

Network Card LED Description

Different NIC manufacturers use different LED colors and blink states. Not all NICs are supported for every Nutanix platform. See the system specifications for your platform to verify which NICs are supported.

Table 9: SuperMicro NICs

NIC	Link (LNK) LED	Activity (ACT) LED
Dual/Quad Port 25GbE	Green: 25 GbE Amber: less than 25 GbE OFF: No link	Blinking: activity Off : No ativity
Dual Port 100GbE	Green: 100 GbE Amber: less than 100 GbE	Blinking: activity Off : No activity

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3278

Table 10: Intel NICs

NIC	Link (LNK) LED	Activity (ACT) LED
Quad port 10G BaseT	Green: 10 Gbps Yellow: 5/2.5/1Gbps OFF: 100 Mbps	Blinking green: Transmitting or receiving data Off : No link
Quad port 10G SFP+	Green: 10 Gbps Yellow: 1 Gbps	Blinking: Activity Off : No activity
Dual Port 25G	Green: 10 Gbps Amber: 10 Gbps	Green: SFP LAN port active

Table 11: Broadcom NICs

NIC	Link (LNK) LED	Activity (ACT) LED
Dual Port 25G	Green: Linked at 25 Gb/s Yellow: Linked at 10 Gb/s or 1 Gb/s Off: No link	Blinking green: Traffic Flowing Activity Off: No activity
Dual Port 10G	Green: Linked at 10 Gb/s Amber: Linked at 1 Gb/s Off: No link	Blinking green: Link up (traffic flowing) Off: No activity

Table 12: Mellanox NICs

NIC	Bi-color LED (Yellow/Green)	Single color LED (Green)	Indicates
Dual port CX-6 25G Dual port CX-6 100G	1 Hz blinking Yellow	Off	Beacon command for locating the adapter card
	4 Hz blinking Yellow Indicates an error with the link	ON	Error
	Blinking Green LED	Blinking	Physical Activity
	Solid Green LED	ON	Link Up

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3279

Power Supply Unit Redundancy and Node Configuration

Note: Carefully plan your AC power source needs, especially in cases where the cluster consists of mixed models. Nutanix recommends that you use 208 V - 240 V AC power source to ensure Power Supply Unit (PSU) redundancy.

Table 13: PSU Redundancy and Node Configuration

Nutanix model	Number of nodes	Redundancy at 110 V	Redundancy at 208-240 V
NX-1065-G9	1, 2, or 3	No	Yes
NX-3035-G9	1 or 2	No	Yes
NX-3060-G9	1, 2, 3, or 4	No	Yes
NX-1150S-G9	1	Yes	Yes
NX-1175S-G9	1	Yes	Yes
NX-3155-G9	1	No	Yes
NX-8150-G9	1	No	Yes
NX-8155-G9	1	No	Yes
NX-8155A-G9	1	No	Yes
NX-8170-G9	1	No	Yes
NX-9151-G9	1	Not supported	Yes (2+1 PSU redundancy) Two PSUs must remain functional at all times.

Caution:

For all G9 platforms except NX-1175S-G9 and NX-1150S-G9: When the input power source is 110 V, a single PSU failure will cause all nodes in a block to power off.

For NX-1175S-G9 and NX-1150S-G9: The block can tolerate a single PSU failure when connected to a 110 V input power source.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3280

3

MEMORY CONFIGURATIONS

Supported Memory Configurations

DIMM installation information for all Nutanix G9 platforms.

DIMM Restrictions

DIMM capacity

Each G9 node must contain only DIMMs of the same capacity. For example, you cannot mix 32 GB DIMMs and 64 GB DIMMs in the same node.

DIMM speed

G9 platforms that use Intel Sapphire Rapids processors support 4800 MT/s DIMMs. The speed of the CPU / DIMM interface is 4000 MT/s or 4800 MT/s based on the CPU SKU used.

G9 platforms that use Intel Emerald Rapids processors ship with 5600 MT/s DIMMs. The speed of the CPU / DIMM interface depends on the CPU class and on whether you have installed one DIMM per memory channel (1DPC) or two DIMMs per memory channel (2DPC).

- Platinum-8xxx: max 5600 MT/s at 1DPC; max 4400 MT/s at 2DPC.
- Gold-6xxx: max 5200 MT/s at 1DPC; max 4400 MT/s at 2DPC.
- Gold-5xxx: max 4800 MT/s at 1DPC; max 4400 MT/s at 2DPC.
- Silver-4xxx: max 4400 MT/s at both 1DPC and 2DPC.
- Bronze-3xxx (single socket boards only): max 4400 MT/s at both 1DPC and 2DPC.

If you install a 5600 MT/s DIMM in a G9 platform that uses Intel Sapphire Rapids processors, it runs at a max of 4800 MT/s.

DIMM manufacturer

Mixing of DIMMs from different manufacturers in a node is not allowed. You must use DIMMs from the same manufacturer in a node.

Memory Installation Order for Single-Node Hyper G9 Platforms

A *memory channel* is a group of DIMM slots.

For G9 single-node hyper platforms, each CPU is associated with eight memory channels. Each memory channel contains two DIMM slots, one blue slot and one black slot, for a total of 32 DIMM slots.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3281

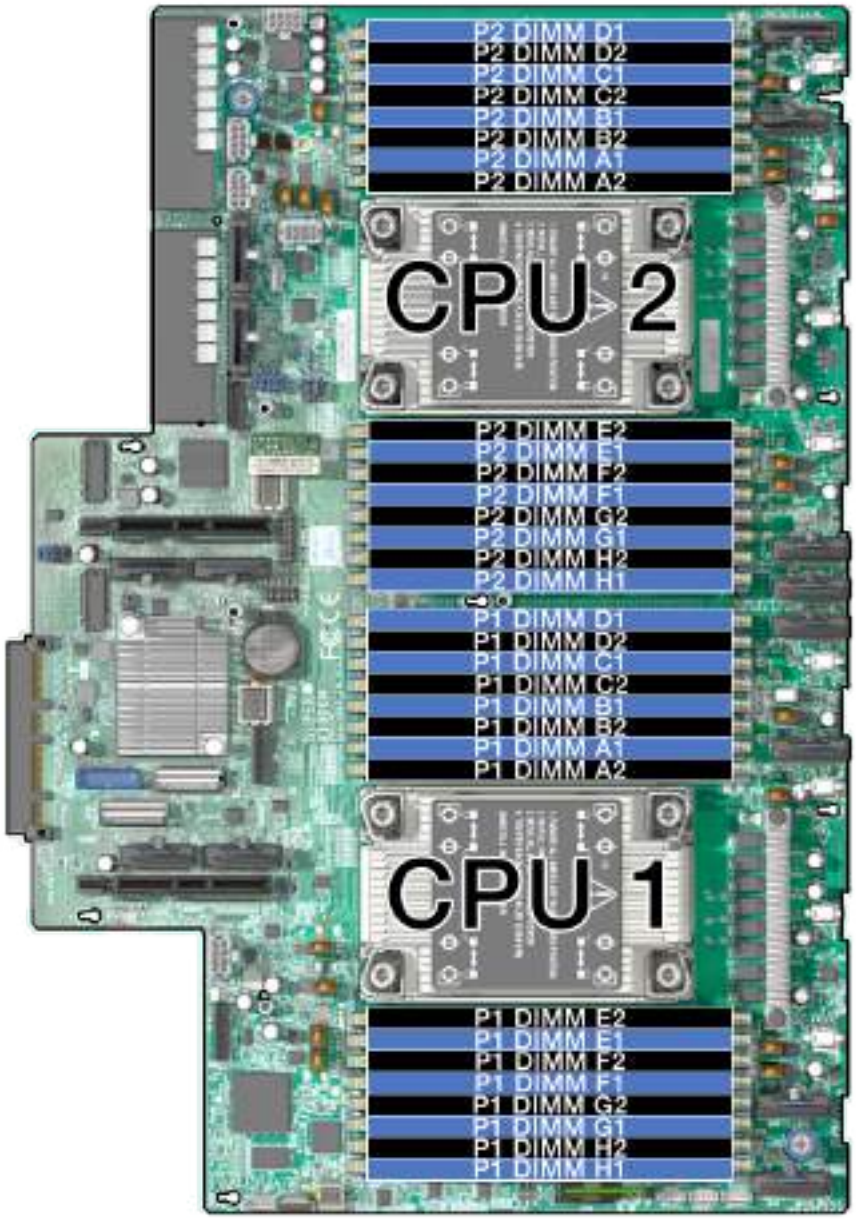


Figure 5: DIMM Slots for a Single-Node Hyper G9 Serverboard

Table 14: DIMM Installation Order for Single-Node Hyper G9 Platforms

Number of DIMMs	Slots to Use	Supported Capacities
4	CPU1: A1, G1 (blue slots) CPU2: A1, G1 (blue slots)	32 GB, 64 GB, 128 GB

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3282

Number of DIMMs	Slots to Use	Supported Capacities
8	CPU1: A1, C1, E1, G1 (blue slots) CPU2: A1, C1, E1, G1 (blue slots)	32 GB, 64 GB, 128 GB
12	CPU1: A1, C1, D1, E1, F1, G1 (blue slots) CPU2: A1, C1, D1, E1, F1, G1 (blue slots)	32 GB, 64 GB, 128 GB
16	CPU1: A1, B1, C1, D1, E1, F1, G1, H1 (blue slots) CPU2: A1, B1, C1, D1, E1, F1, G1, H1 (blue slots)	32 GB, 64 GB, 128 GB
24	CPU1: A1, B1, C1, D1, E1, F1, G1, H1 (blue slots) CPU1: A2, C2, E2, G2 (black slots) CPU2: A1, B1, C1, D1, E1, F1, G1, H1 (blue slots) CPU2: A2, C2, E2, G2 (black slots)	32 GB, 64 GB, 128 GB
32	Fill all slots.	32 GB, 64 GB, 128 GB

4

NUTANIX HARDWARE NAMING CONVENTION

Every Nutanix block has a unique name based on the standard Nutanix naming convention.

The Nutanix hardware model name uses the format prefix-*body*-*suffix*.

For all Nutanix platforms, the prefix is NX to indicate that the platform is sold directly by Nutanix and support calls are handled by Nutanix.

body uses the format *ABCD* | *Y*. The following table describes the body values.

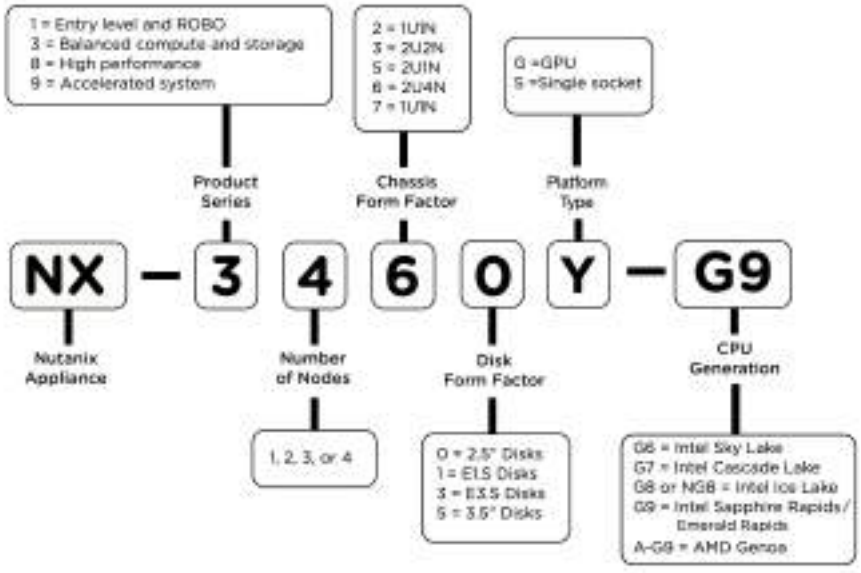


Figure 6: Nutanix Hardware Naming Convention

Table 15: Body

Body	Description
A	Indicates the product series and is one of the following values. • *1* – Entry-level & ROBO • *3* – Balanced compute and storage • *8* – High performance • *9* – Accelerated system

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3284

Body	Description
B	Indicates the number of nodes. • For single-node platforms, *B* is always 1. • For multi-node platforms, *B* can be 1, 2, 3, or 4. **Note:** For multi-node platforms, the documentation always uses a generic zero for *B*.
C	Indicates the chassis form factor and is one of the following values. • 1 – 1U1N (one rack unit high with one node) • 3 – 2U2N (two rack units high with two nodes) • 5 – 2U1N (two rack units high with one node) • 6 – 2U4N (two rack units high with four nodes) • 7 – 1U1N (one rack unit high with one node)
D	Indicates the drive form factor and is one of the following values. • *0* – 2.5 inch drives • *1* – E1.S drives • *3* – E3.S drives • *5* – 3.5 inch drives
Y	Indicates platform types, and takes one of the following values: • *S* – Single socket • *G* – GPU (Not used in G9 since GPU is available on multiple models)

Table 16: Suffix

Suffix	Description
G5	The platform uses the Intel Broadwell CPU.
G6	The platform uses the Intel Skylake CPU.
G7	The platform uses the Intel Cascade Lake CPU.
G8 or N-G8	The platform uses the Intel Ice Lake CPU.
G9	The platform uses the Intel Sapphire Rapids or Emerald Rapids CPU.
A-G9	The platform uses the AMD Genoa CPU.

COPYRIGHT

Copyright 2024 Nutanix, Inc.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Nutanix and the Nutanix logo are registered trademarks of Nutanix, Inc. in the United States and/or other jurisdictions. All other brand and product names mentioned herein are for identification purposes only and may be trademarks of their respective holders.

License

The provision of this software to you does not grant any licenses or other rights under any Microsoft patents with respect to anything other than the file server implementation portion of the binaries for this software, including no licenses or any other rights in any hardware or any devices or software that are used to communicate with or in connection with this software.

Conventions

Convention	Description
`variable_value`	The action depends on a value that is unique to your environment.
`ncli> command`	The commands are executed in the Nutanix nCLI.
`user@host$ command`	The commands are executed as a non-privileged user (such as nutanix) in the system shell.
`root@host# command`	The commands are executed as the root user in the vSphere or Acropolis host shell.
`> command`	The commands are executed in the Hyper-V host shell.
`output`	The information is displayed as output from a command or in a log file.

Default Cluster Credentials

Interface	Target	Username	Password
Nutanix web console	Nutanix Controller VM	admin	Nutanix/4u
vSphere Web Client	ESXi host	root	nutanix/4u
vSphere client	ESXi host	root	nutanix/4u
SSH client or console	ESXi host	root	nutanix/4u
SSH client or console	AHV host	root	nutanix/4u
SSH client	Nutanix Controller VM	nutanix	nutanix/4u
SSH client	Nutanix Controller VM	admin	Nutanix/4u

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3286

Interface	Target	Username	Password
SSH client or console	Acropolis OpenStack Services VM (Nutanix OVM)	root	admin

Version

Last modified: December 4, 2024 (2024-12-04T22:24:44+05:30)

NX-8155-G9 System Specifications

Platform ANY

NX-8155-G9

December 4, 2024

NUTANIX

Contents

1. System Specifications.....3
   Node Naming (NX-8155-G9).....3
      NX-8155-G9 System Specifications.....5

2. Component Specifications.....12
   Controls and LEDs for Single-node Platforms.....12
   Network Card LED Description.....14
   Power Supply Unit Redundancy and Node Configuration.....16

3. Memory Configurations.....17
   Supported Memory Configurations.....17

4. Nutanix Hardware Naming Convention.....20

Copyright.....22
   License.....22
   Conventions.....22
   Default Cluster Credentials.....22
   Version.....23

1

SYSTEM SPECIFICATIONS

Node Naming (NX-8155-G9)

Nutanix assigns a name to each node in a block, which varies by product type.

The NX-8155-G9 block contains a single node named Node A. It contains 12 drive slots and supports all-NVMe and hybrid NVMe + HDD configurations.

Figure 1: NX-8155-G9 Front Panel

Partial Population

The NX-8155-G9 supports partial population of drives according to the following restrictions:

- Partially populated configurations support only even numbers of drives.
- Populate the drive slots in order from bottom to top and left to right.

When partially populating a node, Nutanix recommends that you put an empty drive carrier in each unpopulated drive slot for proper airflow and to prevent dust contamination.

Hybrid NVMe + HDD Drive Configuration

Note: Hybrid NVMe + HDD configuration is available as a factory installation only. You cannot convert a hybrid NVMe + HDD node to an all-NVMe node in the field.

HDD 1 [SLOT3]	HDD 4 [SLOT6]	HDD 7 [SLOT9]	HDD 10 [SLOT12]
NVMe2 [SLOT2]	HDD 3 [SLOT5]	HDD 6 [SLOT8]	HDD 9 [SLOT11]
NVMe 1 [SLOT1]	HDD 2 [SLOT4]	HDD 5 [SLOT7]	HDD 8 [SLOT10]

Figure 2: Hybrid NVMe + HDD Configuration 1

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3290

- Two NVMe drives in slots 1 and 2; four HDDs in slots 3 through 6; all other slots empty
- Two NVMe drives in slots 1 and 2; six HDDs in slots 3 through 8; all other slots empty
- Two NVMe drives in slots 1 and 2; eight HDDs in slots 3 through 10; all other slots empty
- Two NVMe drives in slots 1 and 2; 10 HDDs in slots 3 through 12

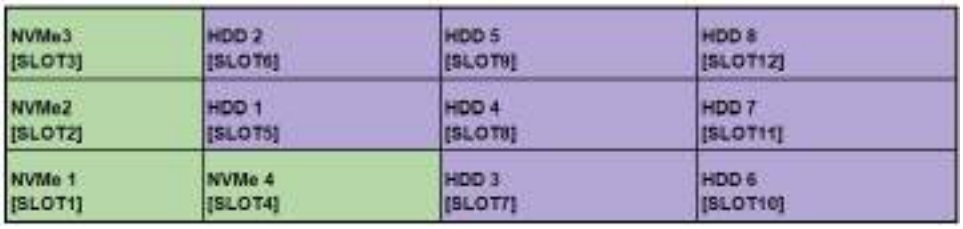


Figure 3: Hybrid NVMe + HDD Configuration 2

- Four SSDs in slots 1 through 4; eight HDDs in slots 5 through 12

All-NVMe Configuration

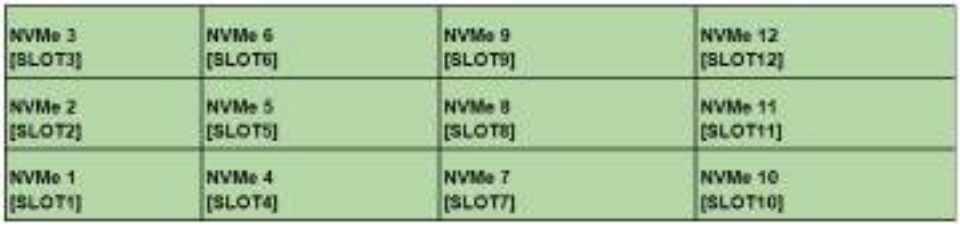


Figure 4: All-NVMe Configuration

Note: A minimum of four NVMe drives are mandatory for all-NVMe configuration.

- Four NVMe drives in slots 1 through 4; all other slots empty
- Six NVMe drives in slots 1 through 6; all other slots empty
- Eight NVMe drives in slots 1 through 8; all other slots empty
- 10 NVMe drives in slots 1 through 10; all other slots empty
- 12 NVMe drives in slots 1 through 12 (fill all slots)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3291

Figure 5: NX-8155-G9 Control Panel

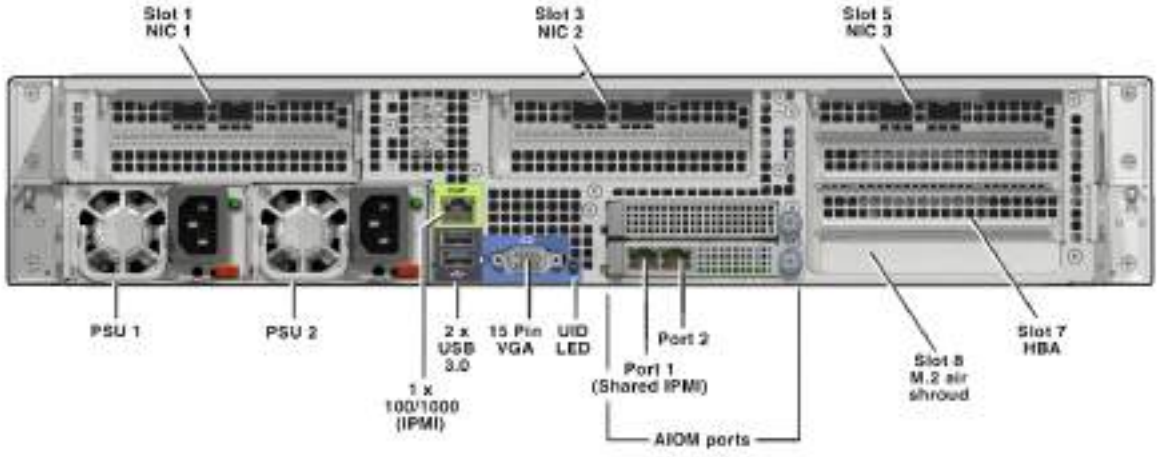


Figure 6: NX-8155-G9 Back Panel

NX-8155-G9 System Specifications

Table 1: System Characteristics

Boot Device	Boot Drive • 2 x 512GB M.2 Boot Device
Chassis	Chassis • 2U1N LFF Chassis

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3292

CPU	Processor Dual Intel Xeon® 5th Gen. (Emerald Rapids) • 2 x Intel Xeon® Silver 4509Y [8 cores / 2.60 GHz / 125 W] • 2 x Intel Xeon® Silver 4510 [12 cores / 2.40 GHz / 150 W] • 2 x Intel Xeon® Silver 4514Y [16 cores / 2.00 GHz / 150 W] • 2 x Intel Xeon® Silver 4516Y+ [24 cores / 2.20 GHz / 185 W] • 2 x Intel Xeon® Gold 5515+ [8 cores / 3.20 GHz / 165 W] • 2 x Intel Xeon® Gold 6526Y [16 cores / 2.80 GHz / 195 W] • 2 x Intel Xeon® Gold 6544Y [16 cores / 3.60 GHz / 270 W] • 2 x Intel Xeon® Gold 6542Y [24 cores / 2.90 GHz / 250 W] • 2 x Intel Xeon® Gold 5520+ [28 cores / 2.20 GHz / 205 W] • 2 x Intel Xeon® Gold 6548Y+ [32 cores / 2.50 GHz / 250 W] • 2 x Intel Xeon® Gold 6554S [36 cores / 2.20 GHz / 270 W] Dual Intel Xeon® 4th Gen. (Sapphire Rapids) • 2 x Intel Xeon® Silver 4410T [10 cores / 2.70 GHz / 150 W], Excluded from ENERGY STAR certification. • 2 x Intel Xeon® Silver 4410Y [12 cores / 2.00 GHz / 150 W] • 2 x Intel Xeon® Silver 4416+ [20 cores / 2.00 GHz / 165 W] • 2 x Intel Xeon® Gold 5415+ [8 cores / 2.90 GHz / 150 W], Excluded from ENERGY STAR certification. • 2 x Intel Xeon® Gold 5416S [16 cores / 2.00 GHz / 150 W] • 2 x Intel Xeon® Gold 5418Y [24 cores / 2.00 GHz / 185 W] • 2 x Intel Xeon® Gold 5420+ [28 cores / 2.00 GHz / 205 W] • 2 x Intel Xeon® Gold 6416H [18 cores / 2.20 GHz / 165 W] • 2 x Intel Xeon® Gold 6426Y [16 cores / 2.50 GHz / 185 W] • 2 x Intel Xeon® Gold 6434 [8 cores / 3.70 GHz / 195 W] • 2 x Intel Xeon® Gold 6442Y [24 cores / 2.60 GHz / 225 W] • 2 x Intel Xeon® Gold 6444Y [16 cores / 3.60 GHz / 270 W] • 2 x Intel Xeon® Gold 6454S [32 cores / 2.20 GHz / 270 W]

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3293

Memory	**Note:** • The 96 GB memory configurations are only available with Emerald Rapids processors. • The minimum memory configuration required for Energy STAR 4.0 certification is 512 GB. If memory is less than 512 GB, the platform is not Energy Star certified, even if the CPU is certified. 32GB DIMM • 4 x 32 GB = 128 GB • 8 x 32 GB = 256 GB • 12 x 32 GB = 384 GB • 16 x 32 GB = 512 GB • 24 x 32 GB = 768 GB • 32 x 32 GB = 1024 GB 64GB DIMM • 4 x 64 GB = 256 GB • 8 x 64 GB = 512 GB • 12 x 64 GB = 768 GB • 16 x 64 GB = 1024 GB • 24 x 64 GB = 1536 GB • 32 x 64 GB = 2048 GB 96GB DIMM • 16 x 96 GB = 1536 GB • 24 x 96 GB = 2304 GB • 32 x 96 GB = 3072 GB 128GB DIMM • 4 x 128 GB = 512 GB • 8 x 128 GB = 1024 GB • 12 x 128 GB = 1536 GB • 16 x 128 GB = 2048 GB • 24 x 128 GB = 3072 GB • 32 x 128 GB = 4096 GB

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3294

Network	Ports on Serverboard • 1x 1GbE Dedicated IPMI AIOM • 1 x 2P 10GBase-T (Port 1 is shared IPMI) • 1 x 2P 10GBase-T + 2P SFP+ (Port 1 is shared IPMI) Add on NICs in PCIe slots • 0, 1, 2 or 3 x 10GbE 4P NIC • 0, 1, 2 or 3 x 10GBaseT 2P NIC • 0, 1, 2 or 3 x 10GBaseT 4P NIC • 0, 1, 2 or 3 x 25GbE 2P NIC • 0, 1, 2 or 3 x 25GbE 4P NIC • 0, 1, 2 or 3 x 100GbE 2P NIC
Network Cables	Network Cable • 1M-QSFP28 • 1M-QSFP+ • 1M-SFP28 • 3M-QSFP28 • 3M-SFP28 • 3M-SFP+ • 5M-QSFP28 • 5M-QSFP+ • 5M-SFP28 • 5M-SFP+
Power Cable	Power Cable • C13/14 4ft Power Cable
Power Supply	Power Supply • 2 x PWS, 2000W
Server	Server • 1 x NX-8155-G9 Server
Storage	

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3295

All NVMe	4, 6, 8, 10 or 12 x NVMe • 1.92TB • 3.84TB • 7.68TB • 15.36TB
NVMe+HDD	2 x NVMe • 1.92TB • 3.84TB • 7.68TB • 15.36TB 4, 6, 8 or 10 x HDD • 8TB • 12TB • 18TB • 24TB
NVMe+HDD	4 x NVMe • 1.92TB • 3.84TB • 7.68TB • 15.36TB 8 x HDD • 8TB • 12TB • 18TB • 24TB
Storage Controller	Storage Controller • 1 x Broadcom 3816 Host Bus Controller (HBA), required for SATA/SAS based drive support
TPM	TPM • 0 or 1 x Unprovisioned Trusted Platform Module

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3296

Transceiver	Transceiver • SR SFP+ Transceiver
VGA	1 x VGA connector per node (15-pin female)
Chassis fans	4 x 80 mm heavy-duty fans with PWM fan speed controls.

Table 2: Block, power and electrical

Block	• Height : 88.1 mm • Depth : 799 mm • Width : 445.6 mm Maximum configuration (without rails and accessory kits) • Weight : 27.3 kg
Package	Package maximum weight with rails and accessory kits • Weight : 36.36 kg
Shock	10ms, half-sine, one shock on each side • Operating : 5 G 10ms, square wave, one shock on each side • Non-Operating : 20 G
Thermal Dissipation	• Typical : 3705 BTU/hr • Maximum : 4941 BTU/hr
Vibration (Random)	at 5 to 500 Hz, Approx. 15 min./axis • Operating : 0.1 Grms
Power consumption (calculated)	**Note:** • For the power consumption calculations, Max NIC and disk configurations are considered. Max Config • Maximum: 1448 VA • Typical: 1086 VA

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3297

Operating environment	Operating temperature : 10-30C Non-Operating temperature : -20-70C Operating relative humidity : 0-85% Non-operating relative humidity : 0-95%

Certifications

- BIS
- BSMI
- CE
- CSA
- CSAus
- EAC
- Energy Star
- FCC
- ICES
- KCC
- RCM
- Reach
- RoHS
- S-MARK
- SABS
- SII
- UKCA
- UKRSEPRO
- UL
- VCCI-A
- WEEE
- cUL

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3298

2

COMPONENT SPECIFICATIONS

Controls and LEDs for Single-node Platforms

Figure 7: Front Panel Controls and Indicators

Table 3: Front Panel Controls and Indicators

LED or Button	Function
Power button	Power button applies or removes primary power from the power supply to the system (System standby power maintains)
Power LED	Solid green: Indicates power is supplied to the system power supply units. This LED is illuminated when the system is operating normally.
UID/Reset button	Turns information LED *i* On/Off (Single press) Reboots the system (Press and hold for 6s)
Drive LED	Not used
NIC LED (AIOM Port 1)	Indicates network activity on AIOM 10Gbase-T port 1
NIC LED (AIOM Port 2)	Indicates network activity on AIOM 10Gbase-T port 2
Multiple Function *i* LED	Solid blue: UID activated locally Blinking blue: UID activated remotely

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3299

LED or Button	Function
	Solid red: Overheat condition
	Blinking red at 0.25Hz: Power supply failure
	Flashing red at 1Hz: Fan failure

Note: NIC1 and NIC2 LED in the table above are specific to the AIOM only. If it is a dual port AIOM, then NIC1 LED is controlled by one port and NIC2 LED is controlled by the other port.

Table 4: Drive LEDs

Top LED: Activity	Blue or green, blinking = I/O activity, off = idle
Bottom LED: Status	Red solid = failed drive, On five seconds after boot = power on

Back Panel Controls and Indicators

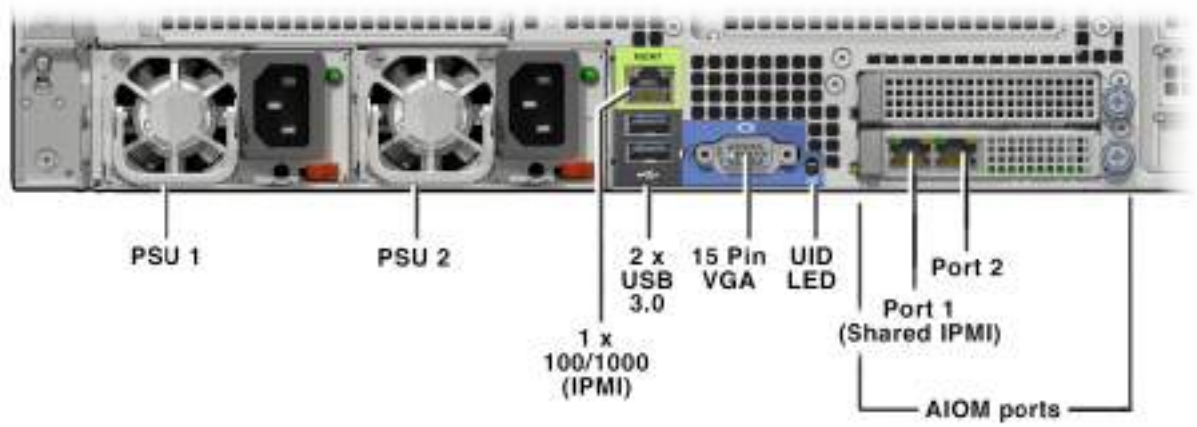


Figure 8: Back Panel Controls and Indicators

Table 5: Back Panel Controls and Indicators

Name	Color	Function
IPMI, Link LED (Left)	Solid Green	100 Mbps
	Solid Amber	1 Gbps
IPMI, Activity LED (Right)	Blinking Amber	Active
AIOM, Link LED (Left)	Off	No link
	Green	Linked at 10 Gb/s
	Amber	Linked at 1 Gb/s
AIOM, Activity LED (Right)	Off	No activity
	Blinking Green	Link up (traffic flowing)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3300

Name	Color	Function
Locator LED (UID)	Blue	Blinking - Node identified

Table 6: Power Supply LED Indicators

Power supply condition	LED status
No AC power to all power supplies	Off
Power supply critical events that cause a shutdown: **Failure**, **Over Current Protection**, **Over Voltage Protection**, **Fan Fail**, **Over Temperature Protection**, **Under Voltage Protection**.	Steady amber
Power supply warning events. Power supply continues to operate. High temperature, over voltage, under voltage and other conditions.	Blinking amber (1 Hz)
When AC is present only: 12VSB on (PS off) or PS in sleep state	Blinking green (1 Hz) minute
Output on and OK	Steady green
AC cord unplugged	Steady amber
Power supply firmware updating mode	Blinking green (2 Hz)

For add-on NIC LED indications, see Network Card LED Description on page 14.

Network Card LED Description

Different NIC manufacturers use different LED colors and blink states. Not all NICs are supported for every Nutanix platform. See the system specifications for your platform to verify which NICs are supported.

Table 7: SuperMicro NICs

NIC	Link (LNK) LED	Activity (ACT) LED
Dual/Quad Port 25GbE	Green: 25 GbE Amber: less than 25 GbE OFF: No link	Blinking: activity Off : No ativity
Dual Port 100GbE	Green: 100 GbE Amber: less than 100 GbE	Blinking: activity Off : No activity

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3301

Table 8: Intel NICs

NIC	Link (LNK) LED	Activity (ACT) LED
Quad port 10G BaseT	Green: 10 Gbps Yellow: 5/2.5/1Gbps OFF: 100 Mbps	Blinking green: Transmitting or receiving data Off : No link
Quad port 10G SFP+	Green: 10 Gbps Yellow: 1 Gbps	Blinking: Activity Off : No activity
Dual Port 25G	Green: 10 Gbps Amber: 10 Gbps	Green: SFP LAN port active

Table 9: Broadcom NICs

NIC	Link (LNK) LED	Activity (ACT) LED
Dual Port 25G	Green: Linked at 25 Gb/s Yellow: Linked at 10 Gb/s or 1 Gb/s Off: No link	Blinking green: Traffic Flowing Activity Off: No activity
Dual Port 10G	Green: Linked at 10 Gb/s Amber: Linked at 1 Gb/s Off: No link	Blinking green: Link up (traffic flowing) Off: No activity

Table 10: Mellanox NICs

NIC	Bi-color LED (Yellow/Green)	Single color LED (Green)	Indicates
Dual port CX-6 25G Dual port CX-6 100G	1 Hz blinking Yellow	Off	Beacon command for locating the adapter card
	4 Hz blinking Yellow Indicates an error with the link	ON	Error
	Blinking Green LED	Blinking	Physical Activity
	Solid Green LED	ON	Link Up

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3302

Power Supply Unit Redundancy and Node Configuration

Note: Carefully plan your AC power source needs, especially in cases where the cluster consists of mixed models. Nutanix recommends that you use 208 V - 240 V AC power source to ensure Power Supply Unit (PSU) redundancy.

Table 11: PSU Redundancy and Node Configuration

Nutanix model	Number of nodes	Redundancy at 110 V	Redundancy at 208-240 V
NX-1065-G9	1, 2, or 3	No	Yes
NX-3035-G9	1 or 2	No	Yes
NX-3060-G9	1, 2, 3, or 4	No	Yes
NX-1150S-G9	1	Yes	Yes
NX-1175S-G9	1	Yes	Yes
NX-3155-G9	1	No	Yes
NX-8150-G9	1	No	Yes
NX-8155-G9	1	No	Yes
NX-8155A-G9	1	No	Yes
NX-8170-G9	1	No	Yes
NX-9151-G9	1	Not supported	Yes (2+1 PSU redundancy) Two PSUs must remain functional at all times.

Caution:

For all G9 platforms except NX-1175S-G9 and NX-1150S-G9: When the input power source is 110 V, a single PSU failure will cause all nodes in a block to power off.

For NX-1175S-G9 and NX-1150S-G9: The block can tolerate a single PSU failure when connected to a 110 V input power source.

3

MEMORY CONFIGURATIONS

Supported Memory Configurations

DIMM installation information for all Nutanix G9 platforms.

DIMM Restrictions

DIMM capacity

Each G9 node must contain only DIMMs of the same capacity. For example, you cannot mix 32 GB DIMMs and 64 GB DIMMs in the same node.

DIMM speed

G9 platforms that use Intel Sapphire Rapids processors support 4800 MT/s DIMMs. The speed of the CPU / DIMM interface is 4000 MT/s or 4800 MT/s based on the CPU SKU used.

G9 platforms that use Intel Emerald Rapids processors ship with 5600 MT/s DIMMs. The speed of the CPU / DIMM interface depends on the CPU class and on whether you have installed one DIMM per memory channel (1DPC) or two DIMMs per memory channel (2DPC).

- Platinum-8xxx: max 5600 MT/s at 1DPC; max 4400 MT/s at 2DPC.
- Gold-6xxx: max 5200 MT/s at 1DPC; max 4400 MT/s at 2DPC.
- Gold-5xxx: max 4800 MT/s at 1DPC; max 4400 MT/s at 2DPC.
- Silver-4xxx: max 4400 MT/s at both 1DPC and 2DPC.
- Bronze-3xxx (single socket boards only): max 4400 MT/s at both 1DPC and 2DPC.

If you install a 5600 MT/s DIMM in a G9 platform that uses Intel Sapphire Rapids processors, it runs at a max of 4800 MT/s.

DIMM manufacturer

Mixing of DIMMs from different manufacturers in a node is not allowed. You must use DIMMs from the same manufacturer in a node.

Memory Installation Order for Single-Node Hyper G9 Platforms

A *memory channel* is a group of DIMM slots.

For G9 single-node hyper platforms, each CPU is associated with eight memory channels. Each memory channel contains two DIMM slots, one blue slot and one black slot, for a total of 32 DIMM slots.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3304

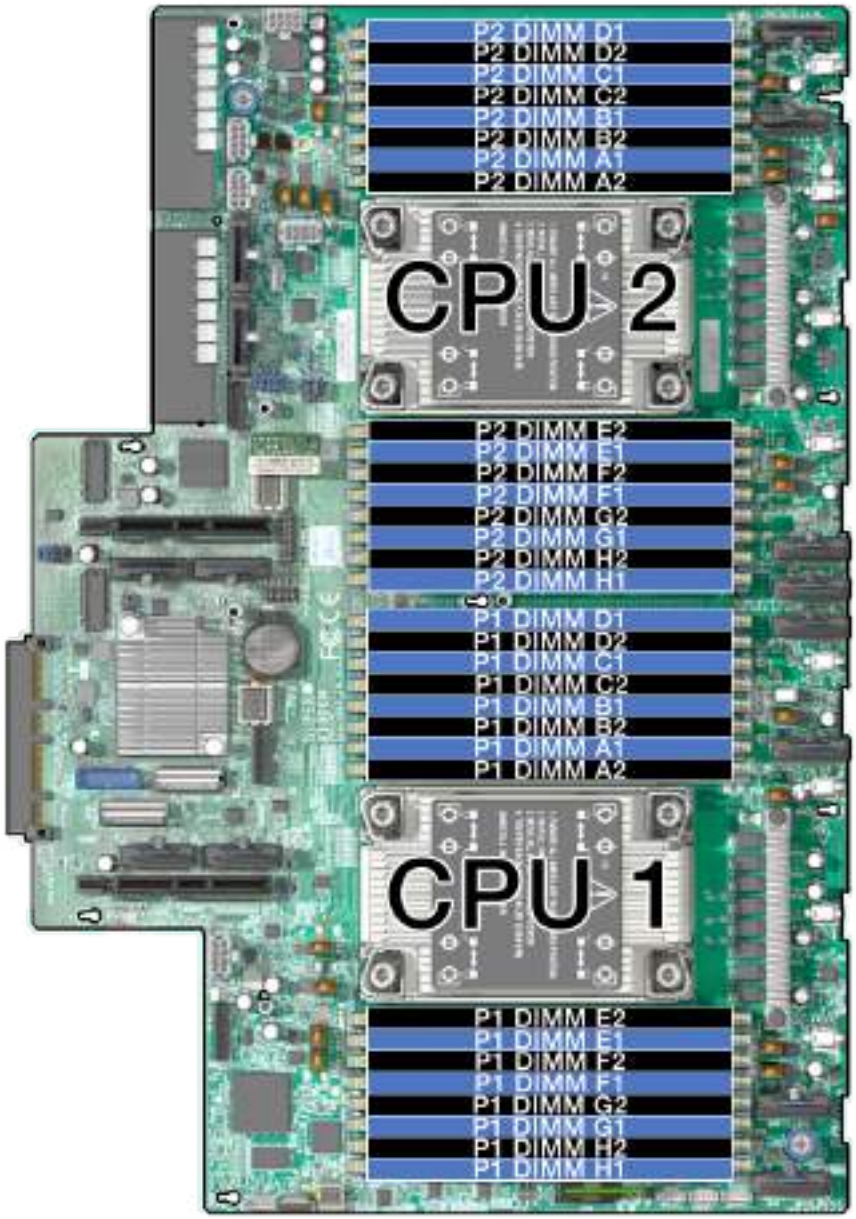


Figure 9: DIMM Slots for a Single-Node Hyper G9 Serverboard

Table 12: DIMM Installation Order for Single-Node Hyper G9 Platforms

Number of DIMMs	Slots to Use	Supported Capacities
4	CPU1: A1, G1 (blue slots) CPU2: A1, G1 (blue slots)	32 GB, 64 GB, 128 GB

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3305

Number of DIMMs	Slots to Use	Supported Capacities
8	CPU1: A1, C1, E1, G1 (blue slots) CPU2: A1, C1, E1, G1 (blue slots)	32 GB, 64 GB, 128 GB
12	CPU1: A1, C1, D1, E1, F1, G1 (blue slots) CPU2: A1, C1, D1, E1, F1, G1 (blue slots)	32 GB, 64 GB, 128 GB
16	CPU1: A1, B1, C1, D1, E1, F1, G1, H1 (blue slots) CPU2: A1, B1, C1, D1, E1, F1, G1, H1 (blue slots)	32 GB, 64 GB, 128 GB
24	CPU1: A1, B1, C1, D1, E1, F1, G1, H1 (blue slots) CPU1: A2, C2, E2, G2 (black slots) CPU2: A1, B1, C1, D1, E1, F1, G1, H1 (blue slots) CPU2: A2, C2, E2, G2 (black slots)	32 GB, 64 GB, 128 GB
32	Fill all slots.	32 GB, 64 GB, 128 GB

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3306

4

NUTANIX HARDWARE NAMING CONVENTION

Every Nutanix block has a unique name based on the standard Nutanix naming convention.

The Nutanix hardware model name uses the format prefix-*body*-*suffix*.

For all Nutanix platforms, the prefix is NX to indicate that the platform is sold directly by Nutanix and support calls are handled by Nutanix.

body uses the format *ABCD* | *Y*. The following table describes the body values.

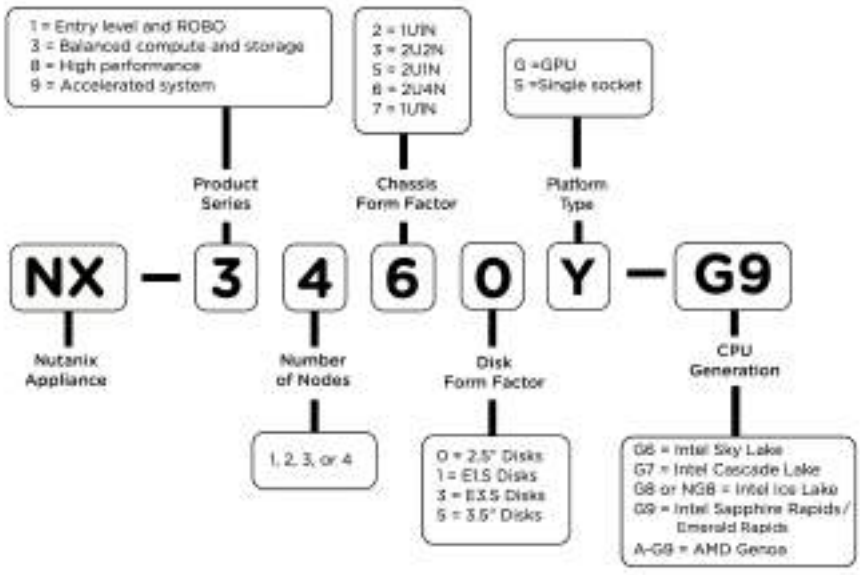


Figure 10: Nutanix Hardware Naming Convention

Table 13: Body

Body	Description
A	Indicates the product series and is one of the following values. • *1* – Entry-level & ROBO • *3* – Balanced compute and storage • *8* – High performance • *9* – Accelerated system

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3307

Body	Description
B	Indicates the number of nodes. • For single-node platforms, *B* is always 1. • For multi-node platforms, *B* can be 1, 2, 3, or 4. **Note:** For multi-node platforms, the documentation always uses a generic zero for *B*.
C	Indicates the chassis form factor and is one of the following values. • 1 – 1U1N (one rack unit high with one node) • 3 – 2U2N (two rack units high with two nodes) • 5 – 2U1N (two rack units high with one node) • 6 – 2U4N (two rack units high with four nodes) • 7 – 1U1N (one rack unit high with one node)
D	Indicates the drive form factor and is one of the following values. • *0* – 2.5 inch drives • *1* – E1.S drives • *3* – E3.S drives • *5* – 3.5 inch drives
Y	Indicates platform types, and takes one of the following values: • *S* – Single socket • *G* – GPU (Not used in G9 since GPU is available on multiple models)

Table 14: Suffix

Suffix	Description
G5	The platform uses the Intel Broadwell CPU.
G6	The platform uses the Intel Skylake CPU.
G7	The platform uses the Intel Cascade Lake CPU.
G8 or N-G8	The platform uses the Intel Ice Lake CPU.
G9	The platform uses the Intel Sapphire Rapids or Emerald Rapids CPU.
A-G9	The platform uses the AMD Genoa CPU.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3308

COPYRIGHT

Copyright 2024 Nutanix, Inc.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Nutanix and the Nutanix logo are registered trademarks of Nutanix, Inc. in the United States and/or other jurisdictions. All other brand and product names mentioned herein are for identification purposes only and may be trademarks of their respective holders.

License

The provision of this software to you does not grant any licenses or other rights under any Microsoft patents with respect to anything other than the file server implementation portion of the binaries for this software, including no licenses or any other rights in any hardware or any devices or software that are used to communicate with or in connection with this software.

Conventions

Convention	Description
`variable_value`	The action depends on a value that is unique to your environment.
`ncli> command`	The commands are executed in the Nutanix nCLI.
`user@host$ command`	The commands are executed as a non-privileged user (such as nutanix) in the system shell.
`root@host# command`	The commands are executed as the root user in the vSphere or Acropolis host shell.
`> command`	The commands are executed in the Hyper-V host shell.
`output`	The information is displayed as output from a command or in a log file.

Default Cluster Credentials

Interface	Target	Username	Password
Nutanix web console	Nutanix Controller VM	admin	Nutanix/4u
vSphere Web Client	ESXi host	root	nutanix/4u
vSphere client	ESXi host	root	nutanix/4u
SSH client or console	ESXi host	root	nutanix/4u
SSH client or console	AHV host	root	nutanix/4u
SSH client	Nutanix Controller VM	nutanix	nutanix/4u
SSH client	Nutanix Controller VM	admin	Nutanix/4u

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3309

Interface	Target	Username	Password
SSH client or console	Acropolis OpenStack Services VM (Nutanix OVM)	root	admin

Version

Last modified: December 4, 2024 (2024-12-04T22:25:52+05:30)

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3310

v3.4 | September 2023 | TN-2027

SOLUTIONS DOCUMENT

Data Protection and Disaster Recovery

NUTANIX

Legal

© 2024 Nutanix, Inc. All rights reserved. Nutanix, the Enterprise Cloud Platform, the Nutanix logo and the other Nutanix products, features, and/or programs mentioned herein are registered trademarks or trademarks of Nutanix, Inc. in the United States and other countries. All other brand and product names mentioned herein are for identification purposes only and are the property of their respective holder(s), and Nutanix may not be associated with, or sponsored or endorsed by such holder(s). This document is provided for informational purposes only and is presented "as is" with no warranties of any kind, whether implied, statutory or otherwise.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

Contents

1. Executive Summary....4
Document Version History....5

2. Nutanix Disaster Recovery Snapshots....6
Nutanix Snapshot Implementation....8
Cloning and Recovery from Granular Snapshots....10

3. Remote Backup and Disaster Recovery with Nutanix....12
Single-Node Backup....13
Hybrid Cloud Deployments with Cloud Connect....14
Self-Service Restore....16

4. NearSync Replication Powered by Lightweight Snapshots....18

5. Nutanix Disaster Recovery Orchestration....20
Protection Policies....21
Recovery Plans....24

6. Metro Availability....28

7. Third-Party Integration with Nutanix....31
REST APIs....31

8. Conclusion....33

About Nutanix....34

List of Figures....35

1. Executive Summary

Enterprises are increasingly vulnerable to data loss and downtime during disasters as they come to rely on virtualized applications and infrastructure that their legacy data protection and disaster recovery solutions can't adequately support. This tech note discusses the data protection and disaster recovery functionalities of Nutanix software. We also recommend reading the Infrastructure Resilience tech note to learn more about our resilience features, including how we handle hardware and software failures.

The Nutanix architecture runs a virtual storage controller (Controller VM, or CVM) on each Nutanix node on the platform, forming a distributed system. The nodes aggregate storage resources into a single global pool that all components can use. Nutanix storage manages resources to preserve data and system integrity in the event of node, disk, application, or hypervisor software failure. The distributed storage also delivers data protection and high availability to keep critical data and VMs secure and applications running.

Nutanix provides simplicity and flexibility to address ever-changing business requirements. Nutanix offers fast and efficient snapshots, which allow quick recovery from application errors, and protection policies that safeguard complex applications without the need to worry about LUNs and storage mapping between sites. The ability to protect discrete components precisely as needed promotes the best possible use of physical resources and supports replication to multiple locations. Whether you're quickly restoring a file through a self-service recovery, backing up to a single-node target, or using NearSync or Metro Availability to replicate another Nutanix cluster on-premises or in the cloud, Nutanix provides several geographical availability options to ensure that your data is safe.

Nutanix also offers Nutanix Disaster Recovery as a Service (DRaaS), which uses the same disaster recovery orchestration features as the on-premises product, including protection policies and recovery plans.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3314

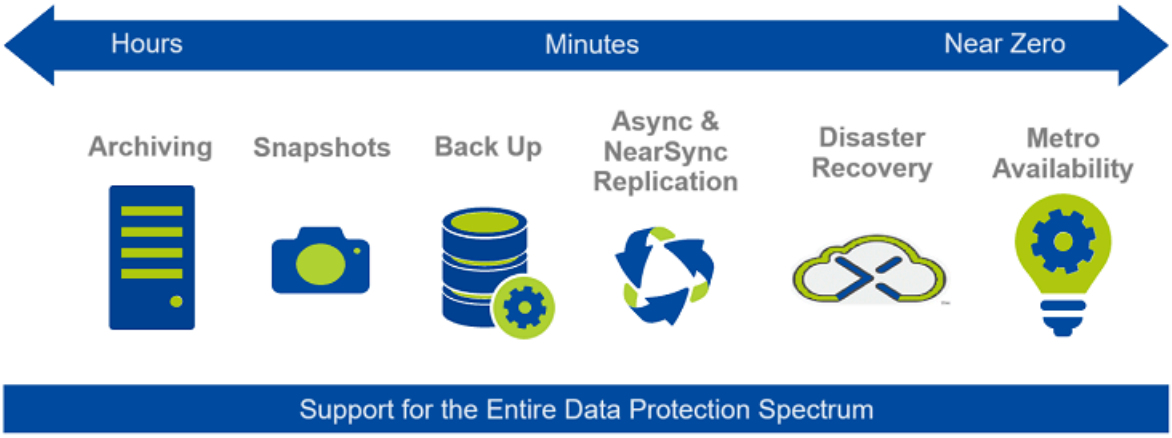


Figure 1: Overall Availability Features

Document Version History

Version Number	Published	Notes
1.0	June 2016	Original publication.
1.1	December 2016	Updated for AOS 5.0.
1.2	December 2017	Updated for AOS 5.5.
2.0	November 2018	Updated for AOS 5.10 and Xi Leap.
2.1	March 2018	Updated for AOS 5.11 and ESXi support for Leap.
2.2	April 2019	Added information about ESXi support for disaster recovery.
3.0	May 2020	Updated for AOS 5.17.
3.1	September 2020	Updated for AOS 5.18 and Nutanix Clusters on Amazon Web Services (AWS).
3.2	November 2021	Refreshed content.
3.3	September 2022	Updated product naming.
3.4	September 2023	Refreshed content.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3315

2. Nutanix Disaster Recovery Snapshots

Fine-grained snapshots are the foundation of Nutanix data protection. VM-centric snapshots can provide data protection at the scale of an individual virtual hard drive. Nutanix also offers snapshot protection for volume groups that provide in-guest iSCSI storage to cover a variety of specific application requirements. To understand the advantages of the Nutanix snapshot functionality, you must first understand the different types of snapshots available.

Snapshots represent a significant advance in the traditional backup process. The storage system generates a snapshot by creating a full or virtual copy of the metadata or index of the stored data, rather than copying the entire pool of stored data. Because snapshots copy only the metadata or index, they can be nearly instantaneous, have minimal performance impact, and require little incremental space. IT organizations can take snapshot-based backups more frequently to improve their recovery point objective (RPO). Backup vendors and analysts widely acknowledge snapshots as the most practical option for faster recovery.

Each snapshot implementation has different storage requirements and use restrictions. The preferred implementation for snapshots is redirect-on-write (ROW). This method redirects any updates to existing protected data to a new location. You don't need to copy or move any of the existing metadata or data in the snapshots. As a result, ROW snapshots don't suffer the performance impact of copy-on-write snapshots. Instead of updating pointers in the metadata, copy-on-write snapshots copy the metadata itself, which causes additional latency during snapshot creation and creates metadata bloat, which uses more of the storage system's performance tier. Nutanix refers to its version of ROW as vDisk-based snapshots.

Nutanix improved its snapshots by incorporating lightweight snapshots (LWS) to provide NearSync replication. Using LWS, you can achieve an RPO between fifteen minutes and one minute by using markers instead of creating full snapshots. LWS further reduces metadata management overhead and increases storage performance by decreasing the high number of storage I/O operations that long snapshot chains can cause. The administrator doesn't have to worry about setting a policy to determine whether the system uses vDisk snapshots or LWS; Nutanix AOS automatically transitions

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3316

between the two forms of replication based on the RPO and available bandwidth. If the network can't handle the low RPO, replication changes to vDisk snapshots. When the network can meet the requirements for NearSync again, AOS returns to using LWS. In oversubscribed networks, NearSync can provide almost the same level of protection as synchronous replication while avoiding network latency on the running workload.

Another consideration with snapshots is the granularity of data you can protect. Granularity determines the snapshot's space overhead. When you take a snapshot of a large block, a change to a small portion of that block creates a full new block with mostly duplicate data, causing the snapshot to be much larger than the amount of data changed. Smaller block sizes result in more data shared between snapshots and greater space efficiency.

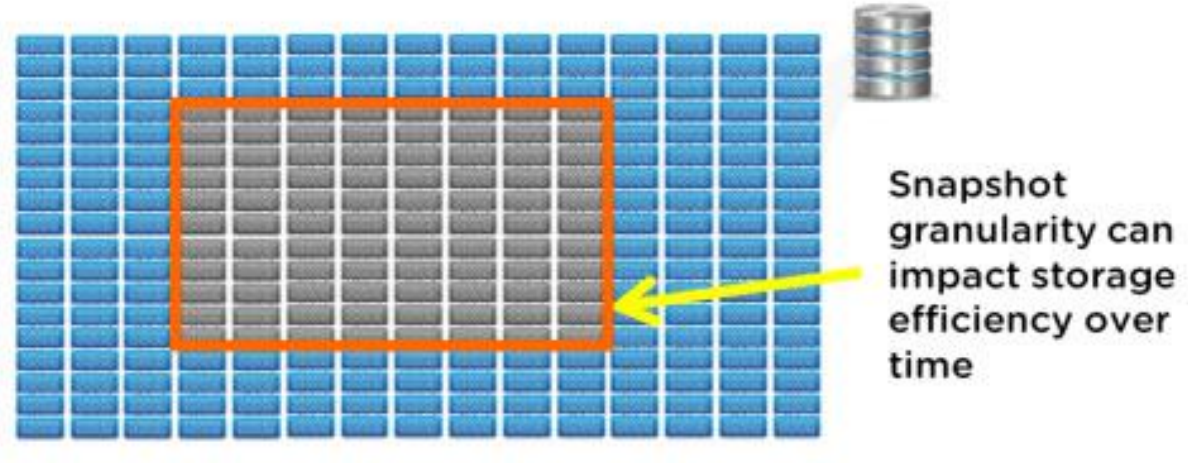


Figure 2: Volume- or LUN-Level Snapshot Granularity

The last aspect of snapshot design to consider is the unit of data that the storage system can protect and restore. Traditional storage deployments typically operate at the storage object level or volume or LUN level, with little to no understanding of what those containers store. In a virtualized environment, this organization results in a simultaneous snapshot of dozens to hundreds of VMs, each with varying change rates. Consequently, administrators bear the burden of mapping the different VMs to storage objects such as LUNs or volumes. This required intervention results in additional steps and greater system complexity, especially when recovering individual VMs. In the traditional approach, you can only set snapshot schedules at the LUN or volume level,

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3317

leading to practices such as creating one LUN per VM as a workaround in order to create individualized snapshot VM schedules.

As an alternative to the volume- or LUN-level method, you can take an application-centric approach to storage and data protection with VM and volume group granularity. In an application- or VM-centric scenario, storage operates at the virtual disk or VM level—the level at which the system takes snapshots. Based on this structure, administrators can set schedules and retention periods for the individual components to meet service requirements. Recovery is simple, as administrators can restore individual VMs without dealing with the underlying storage objects.

Nutanix Snapshot Implementation

This application-centric approach is how Nutanix implements ROW, application-granular, vDisk-based snapshots. When the system initially takes a snapshot of a VM or volume group, it creates a read-only, zero-space clone of the metadata (in other words, an index to the data) and makes the underlying VM data immutable or read-only—it doesn't actually copy or move any data or virtual disks. The system thus creates a read-only copy of the VM you can access the same way as its active counterpart. Nutanix snapshots only take a few seconds to create, eliminating application and VM backup windows.

After the system takes a snapshot and as the application continues to run, the system redirects any new writes and updates to existing data. The original data in the snapshot remains unchanged and the system shares the unchanged data across the snapshots and active VM. AOS handles the snapshot process transparently, so there is no change to how applications and the virtualization stack access the VM.

From an efficiency standpoint, you can take Nutanix snapshots with byte-level resolution. This resolution captures only the changed data between successive snapshots. For even greater efficiency, you can compress and deduplicate all the data stored on AOS, including the snapshot. Although individual deployment savings vary with the specific workloads, average deployments have seen anywhere from 25 to 75 percent reduction in the amount of space needed.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3318

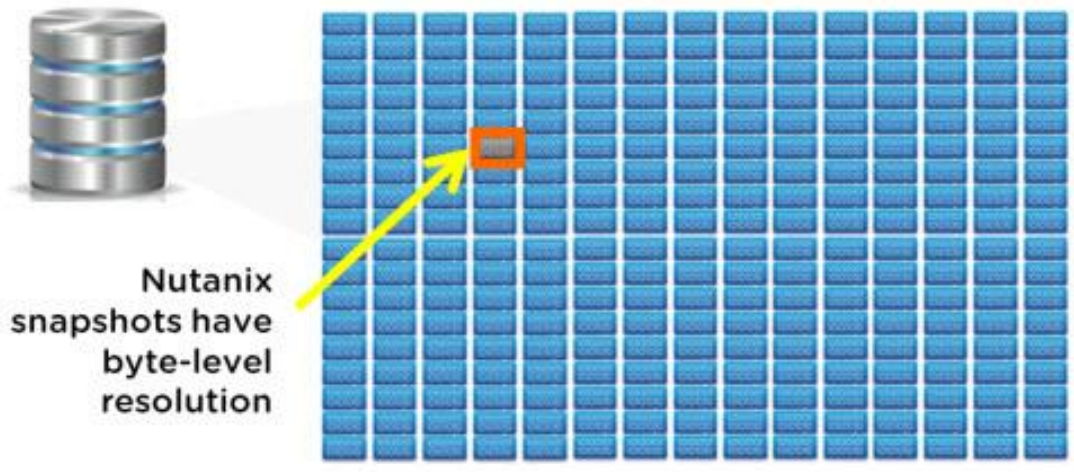


Figure 3: Byte-Level Nutanix Snapshots

You also have flexibility in the types of snapshots available. You can set VM-granular snapshots to be either crash-consistent or application-consistent. Volume group snapshots must be crash-consistent. Crash-consistent snapshots are instantaneous and help workloads recover if the operating system (OS) or VM crashes.

Application-consistent snapshots use the Nutanix framework and services like Microsoft Volume Shadow Copy Service (VSS) to quiesce the VM and supported applications, rendering them into a known or consistent state. For systems using ESXi or AHV and running Microsoft Windows guests, the Nutanix Guest Agent that runs in the guest OS provides VSS support. Using the native Nutanix VSS software provider, the Nutanix Guest Agent is called to quiesce the OS and supported applications, such as Microsoft Exchange and SQL Server, before the system takes an application-consistent snapshot of the VM. Because these VSS-supported snapshots have a software provider, application quiescence times are shorter than what previous hypervisor-based snapshot tools could deliver. Shorter quiescence times help keep application performance constant and reduce the I/O required when collapsing a hypervisor-based snapshot.

Depending on your RPOs and retention needs, you can schedule both VM and volume group snapshots on an hourly, daily, weekly, or monthly basis. Additionally, you can group multiple VMs and volume groups in a Nutanix protection domain to operate on them as a single entity with one RPO. This structure is particularly useful when you're protecting complex applications such as Microsoft SQL Server–based applications or

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3319

Microsoft Exchange. We discuss protecting applications across multiple Nutanix clusters using protection policies later in this document.

The main advantage of using protection domains to group VMs and volume groups versus the traditional SAN approach of consolidating different VMs onto a LUN is VM portability. VMs and volume groups can move between different AOS protection domains without needing to move or copy any data and without revising the business continuity design. For traditional SANs, changing an application's SLA typically requires migrating the application to another LUN or volume. Once changed, both the storage and the hypervisor layer for the application need updating, and you have to account for the configuration time and effort involved in setup.

Because the unique storage design uses a shared-nothing distributed approach to metadata, the system's limits scale with the cluster size. This scalable method eliminates the need for separate storage systems for backup and long-term archiving, as the snapshots are stored across the entire cluster.

Data Optimization with Nutanix AOS

AOS runs a distributed data management service in the background. This service is responsible for running the following tasks with minimal performance impact:

- Metadata optimization
- Garbage collection of deleted VMs
- Data reduction
- Tiering
- Consistency checking
- Rebalancing to optimize data across nodes, flash, and disks

Cloning and Recovery from Granular Snapshots

Nutanix snapshot technology forms the basis of a unique ecosystem of functionality for high availability and DR. One feature that builds on the Nutanix snapshot capability is application-granular cloning.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3320

You can use cloning for a variety of purposes, including deployment and recovery. By integrating your virtualization stack with functionalities like VMware vStorage APIs for Array Integration (VAAI) and VMware View Composer API for Array Integration (VCAI), you can simplify VM deployment using cloning. Nutanix offers the same native functionality for AHV and provides a quick clone plug-in for Hyper-V. You can also clone individual volume groups as rollback support before application upgrades.

With AOS, you can recover individual VMs and volume groups from snapshots. You can either replace the existing active VM with the snapshot copy or create a separate clone of a snapshot, preserving the active VM. Depending on the snapshot settings you use, the recovered VM is either crash-consistent or application-consistent when it comes back online. Restored volume groups come up in a crash-consistent state. When you restore a volume group, reattachment is easy because it maintains its application-specific settings.

If needed, you can create a Nutanix VM-centric snapshot clone to test a new software package or update. Application owners can use file-level recovery directly from the VM to restore individual files with minimal infrastructure operations involvement. Compared to a traditional LUN- or volume-based approach, a VM-centric snapshot strategy eliminates cumbersome steps: it recovers the storage object (LUN or volume), identifies and mounts the VM, then recovers the file. The ability to perform your own restoration helps speed up the process of getting your file back.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3321

3. Remote Backup and Disaster Recovery with Nutanix

With Nutanix snapshots, you can efficiently replicate individual VMs and volume groups from a primary Nutanix cluster to one or more secondary Nutanix clusters. By supporting a fan-out and fan-in or multiway model for replication, AOS creates a flexible, multimaster virtualization environment for backup and disaster recovery. Deployments involving the cloud and numerous branch offices benefit the most from this elastic organization.

Figure 4: Multiway Protection Domains

Because Nutanix's software-defined replication builds on application-granular snapshots, policies for replication are also set at the individual protection-domain level rather than at the LUN or volume level. All nodes in the cluster participate in replication, and only byte-level changes between snapshots of individual VMs move over the network to the remote cluster. While one host serves I/O on the active virtual disk, another host in the cluster can calculate the changed blocks, which eliminates performance bottlenecks for critical VMs and their corresponding hosts.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3322

Figure 5: Use All Cluster Resources for Replication

To get the most out of WAN connectivity, you can deduplicate and compress data before sending it over the wire. First, the primary system sends the fingerprints of changed blocks to the remote destinations. The different destination systems report back with the unique blocks they need to complete the replication; the primary system then sends only those blocks to the destinations. Deduplicating data over the wire can effectively reduce the bandwidth required by 75 percent as opposed to host-based full-copy backup solutions.

The Nutanix converged compute and storage approach, along with application-centric replication, makes creating a disaster recovery solution simple. Using protection domains, you can replicate volume groups and sets of related VMs together and, when the primary site is down, bring them up on the secondary site with a single command. Cross-hypervisor disaster recovery provides true VM mobility; you can replicate VMs between ESXi and AHV Nutanix clusters, and they provide full asynchronous disaster recovery and backup for each other.

Nutanix application-granular replication also makes disaster recovery more affordable. Because replication isn't hardware-dependent for virtualized workloads, the secondary site can be different from the primary cluster. This ability is especially useful for remote site deployments with centralized backup and disaster recovery that use Nutanix storage-only nodes to optimize costs.

Single-Node Backup

Nutanix supports single-node backups as a cost-efficient solution for providing full native backups to branch offices and small and medium-sized businesses. Using the same

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3323

underlying disaster recovery technology, the single node can be either on-site or remote. Nutanix protects the node's data from single-drive failure and provides native backups from end to end.

Nutanix only supports single-node backup on NX-1155 and NX-1175 hardware models. These models are dual-node SSD appliances. Both these appliances and their OEM counterparts can run VMs in the event of a failure.

Hybrid Cloud Deployments with Cloud Connect

With Cloud Connect, customers can use the public cloud as a destination and seamlessly back up and recover their VMs and volume group data. Cloud Connect uses all the existing protection and recovery features discussed earlier and extends them to the public cloud. All nodes participate in replication when they connect to the public cloud, so replication doesn't affect the running workloads. Customers can tune their backup schedules and retention periods depending on the workload and associated SLAs. Cloud Connect works with Amazon Web Services (AWS) and Azure to provide multiple geographical failure domains.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3324

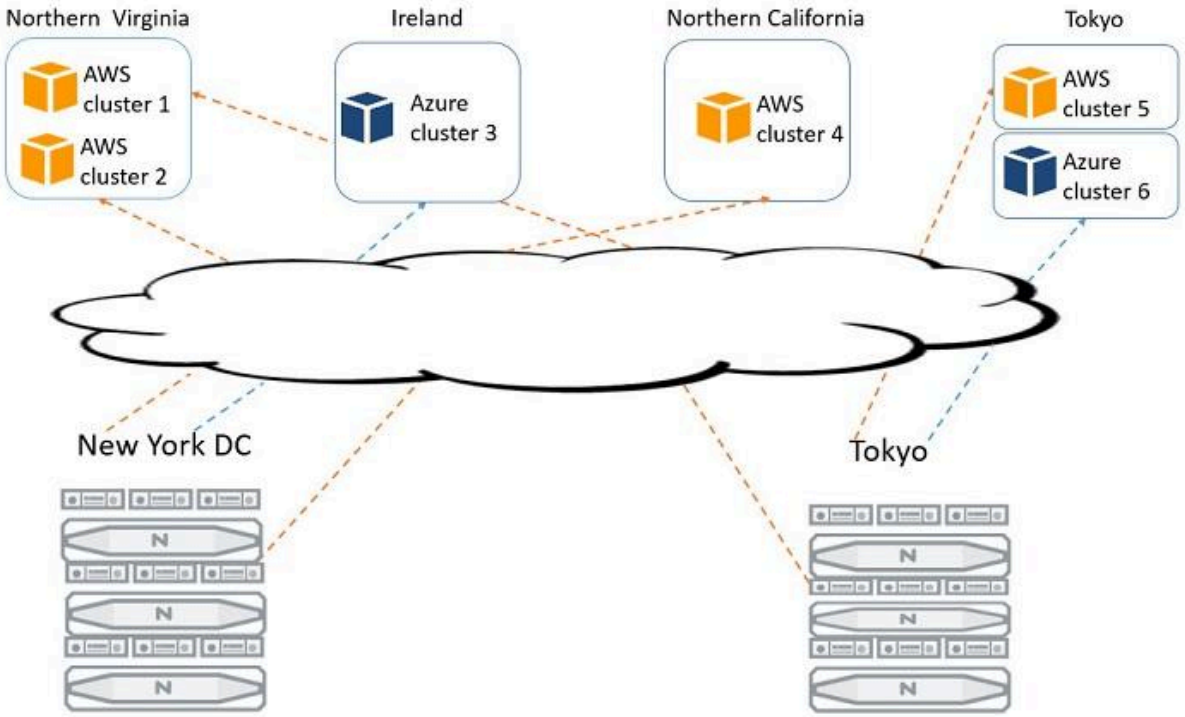


Figure 6: Sample Deployment for Cloud Connect

Nutanix Prism provides a single console for managing storage, compute, backup, and disaster recovery. With Nutanix Prism, administrators can set up Cloud Connect, back up workloads to the public cloud or to a remote site, parse through protected items, perform quick recovery, and make changes to protection schedules. This streamlined interface greatly reduces management clutter.

When you enter public cloud credentials in Prism, a Nutanix CVM cluster deploys in the public cloud. The Nutanix CVM cluster in the private cloud then transfers data to the CVM cluster in the public cloud as if it were communicating with a remote cluster. You can compress the data you send across the WAN, and the granularity of what you send is at the byte level. In other words, if you have 32 KB of data that has changed, Nutanix sends all 32 KB. However, if only 4 KB of your data has changed, Nutanix only sends 4 KB.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3325

Self-Service Restore

Recovering from issues such as accidentally deleting files or overwriting important configuration information can be cumbersome, especially when you're the storage or virtualization administrator in a larger company. Such recovery often requires the assistance of a backup or virtualization administrator who might not work on your team, and getting a response can take hours or days.

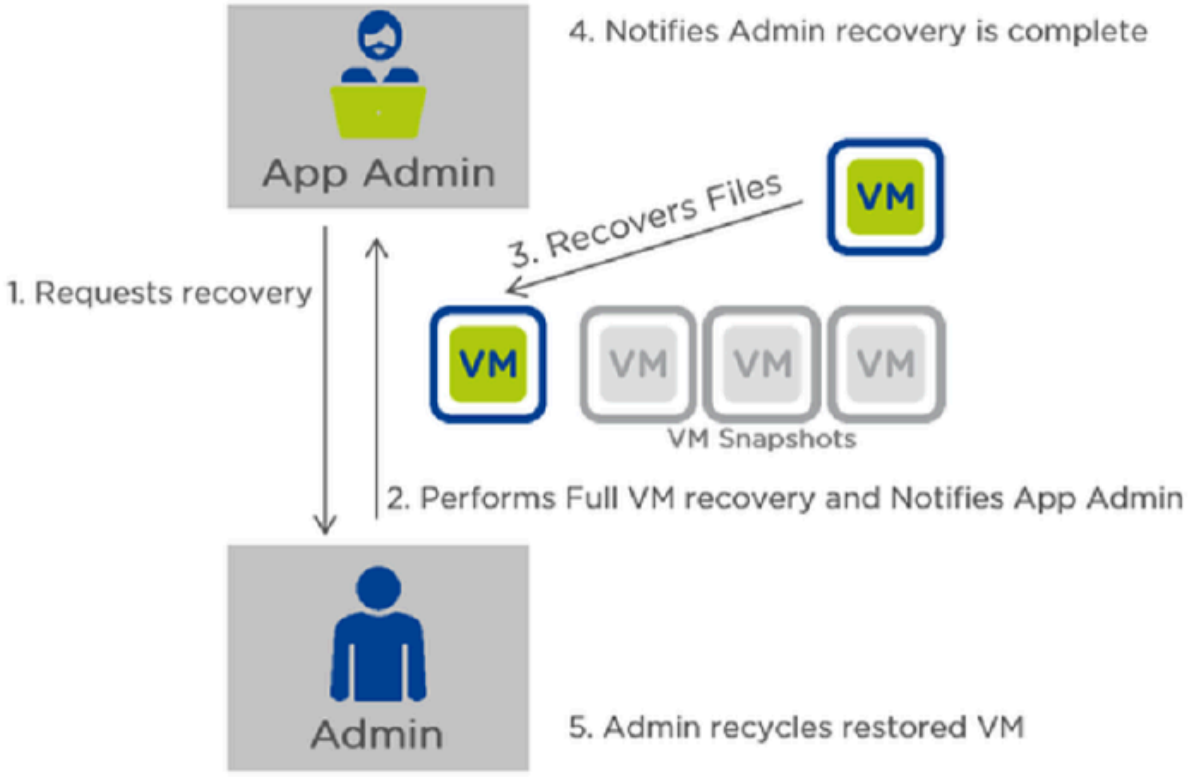


Figure 7: Traditional Restore Process

Nutanix administrators can enable a robust self-service feature, Nutanix Self-Service Restore (SSR), on a per-VM basis to allow trusted application administrators to recover their own files.

Once you enable SSR in a VM, an application administrator can easily manage snapshots from within it, listing available snapshots and mounting or unmounting a

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3326

particular snapshot. Once mounted, a snapshot appears as a new drive in the Windows guest OS. Administrators can copy the files they need from this drive and then unmount the snapshot. To avoid mounted snapshot congestion, SSR automatically cleans up snapshots left mounted for more than 24 hours. Administrators can also connect multiple snapshots to the VM at the same time if they need to search the snapshot history.

SSR requires that you install Nutanix Guest Tools (NGT) in the guest OS. NGT controls tasks like securing communication with the Nutanix CVM from within the guest for control plane operations, handling disk signature clashing, and hiding any system-reserved partitions. We fully support SSR on both VMware vSphere and AHV. A machine's administrator simply opens a web browser to `http://<localhost>:5000` to find what they want to restore and begin the restoration process.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3327

4. NearSync Replication Powered by Lightweight Snapshots

Nutanix uses the lightweight snapshots (LWS) feature to handle a high rate of snapshots without affecting the running application. LWS tracks changes with markers instead of creating new vDisks for every snapshot. With markers, you don't need to maintain metadata or collapse long snapshot chains; however, when you enable NearSync, LWS handles all changes in SSD. To accommodate this trade-off, Nutanix reserves a percentage of SSD space for LWS when you enable it.

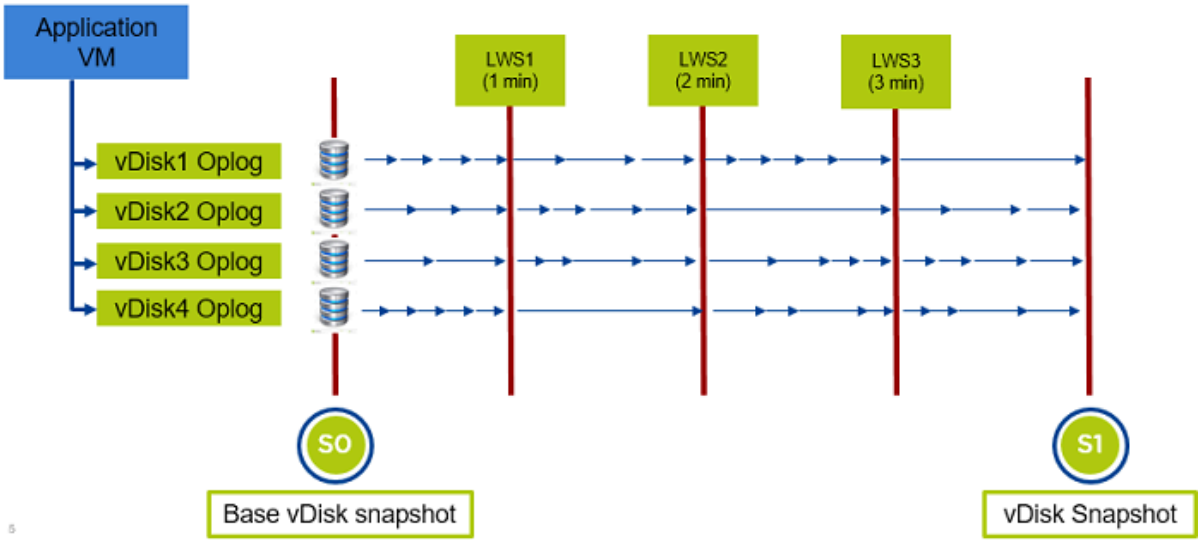


Figure 8: LWS Creation on the Oplog

In the previous diagram, the system first takes a vDisk-based snapshot and replicates it to the remote site. Once the initial full replication is complete, LWS begins at the set schedule. If you haven't set up the remote site, LWS begins locally right away. With sufficient bandwidth available, this process proceeds seamlessly. If you miss your RPO target repeatedly, the system automatically goes back to vDisk-based snapshots. Once the vDisk-based snapshots finish quickly enough to meet requirements, the system automatically returns to NearSync.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3328

At the destination site, AOS creates hydration points, which help LWS transition into vDisk-based snapshots. Hydration points also free SSD space for new incoming replications. Inline hydration works as follows:

1. Create a staging area for each VM consistency group protected by the protection domain.

   A consistency group is a subset of the entities in a protection domain. Consistency groups snapshot a group of VMs or volume groups in a crash-consistent manner. The staging area is essentially a directory with a set of vDisks for the VM that are clones from the last vDisk-based snapshot.
2. The system applies any new incoming LWS (set of oplog episodes) to the same set of vDisks.
3. The system clones the vDisks from the previous step every hour.

   This process provides a snapshot you can use for quick recovery.

The source side doesn't need to hydrate because it takes a vDisk-based snapshot every hour.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3329

5. Nutanix Disaster Recovery Orchestration

Prism Central provides a single web console for monitoring and managing multiple clusters. With AOS versions 5.11 and later, Nutanix protection policies and recovery plans are available in Prism Central for AHV and ESXi to orchestrate operations around migrations and unplanned failures. You can apply orchestration policies from a central location, ensuring consistency across all your sites and clusters.

Nutanix uses a construct called availability zones to manage these new protection policies and recovery plans. On-premises availability zones include all the Nutanix clusters managed by one Prism Central instance. An availability zone can also represent a region in Nutanix DRaaS. For disaster recovery, availability zones exist in pairs—either on-premises to on-premises or on-premises to the cloud. Clusters deployed in a cloud provider like AWS work the same way as on-premises availability zones. Once you pair your on-premises environment to a cloud-based availability zone, you can take advantage of Nutanix DRaaS. There are multiple Nutanix DRaaS subscription plans available, so you don't have to pay the full cost associated with buying a secondary cluster up-front, and you save the time it takes to manage and operate additional infrastructure.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3330

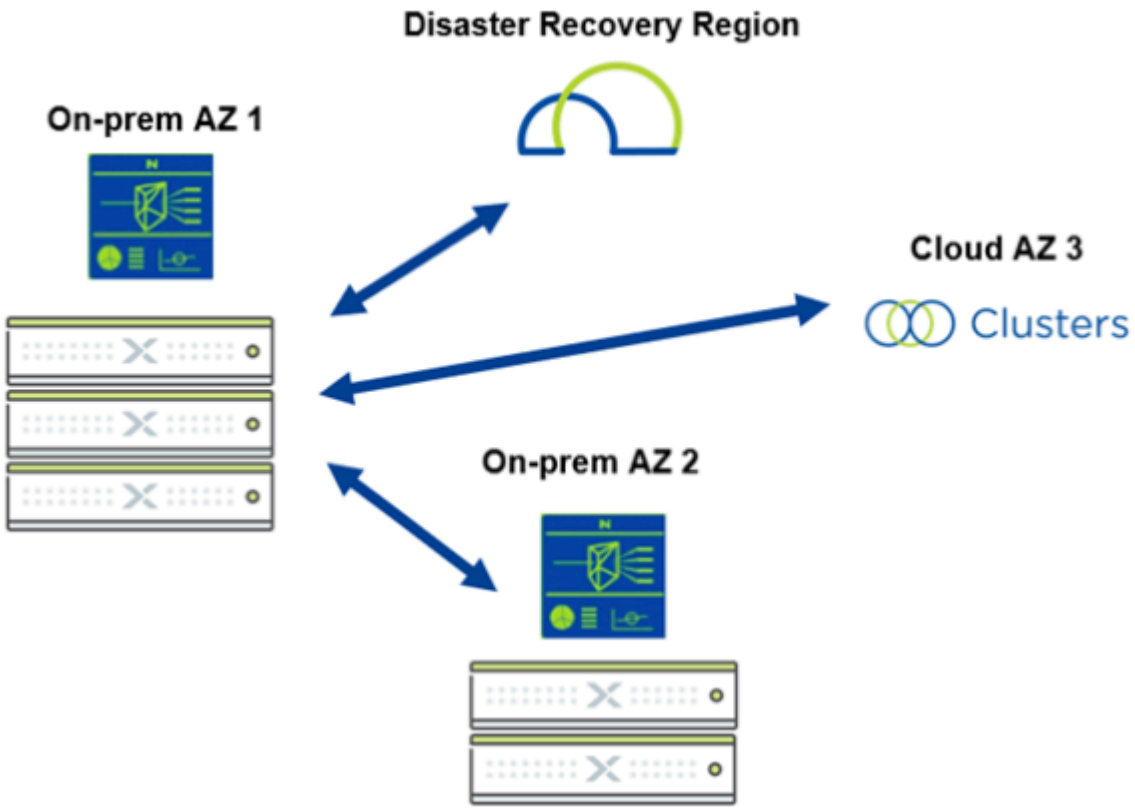


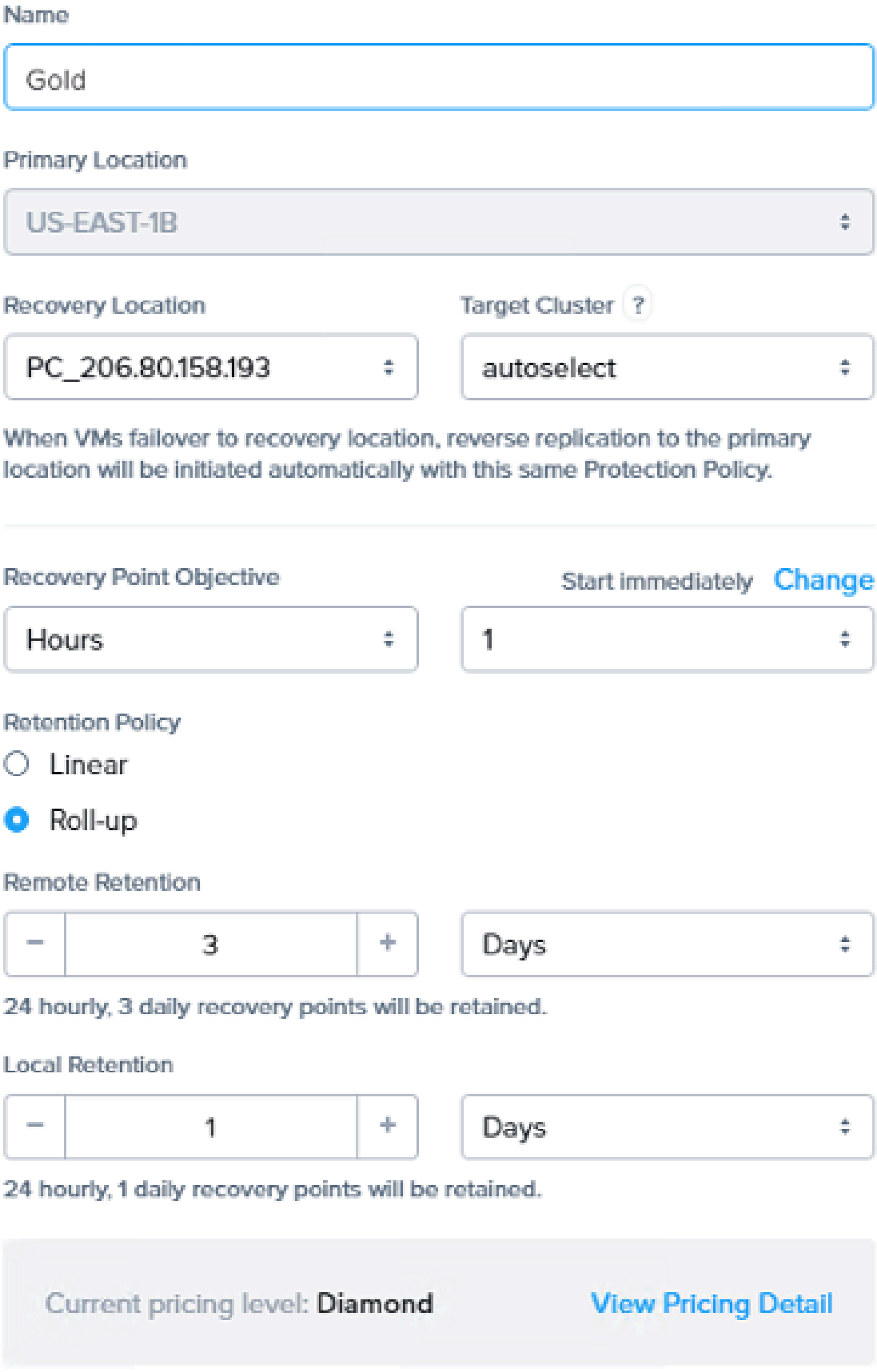
Figure 9: On-Premises and Nutanix-Based Availability Zones

Protection Policies

A protection policy automates the creation and replication of snapshots across all the clusters managed by Prism Central. When you configure a protection policy to create local snapshots, you just specify the RPO, retention policy, and the entities you want to protect. If you want to automate snapshot replication to a remote location, you can also specify the remote location.

Nutanix synchronizes protection policies between paired availability zones. After you perform a failover to the recovery location, that location becomes the primary, and snapshot replication automatically resumes to the former primary location (which has become the new recovery location). If the VPN is connected, your workloads are protected automatically; you don't need to take action to ensure that the two datacenters remain in sync.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3331



© 2024 Nutanix, Inc. All rights reserved |

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3332

To apply protection policies, either use categories or add VMs individually to the policy. Prism Central includes built-in categories for popular applications, such as Microsoft Exchange and Oracle. You can also create your own categories. To add a custom category or value to a policy, create that tag first, so it's available when you create the protection policy. You can add VMs to the category either before or after you configure the protection policy.

When applying your retention policy to meet the required RPO, you have two options: linear and roll-up retention.

Linear Retention

Linear retention implements a retention scheme at both sites (local and remote). If you set the retention number for a given site to n, the site retains the n most recent snapshots. For example, if the RPO is one hour and the retention number for the local site is 48, the 48 most recent snapshots are retained at any given time.

Roll-Up Retention

Roll-up retention combines the oldest snapshots for the specified RPO interval into a single snapshot when the next higher interval is reached, all the way up to the retention period specified for a site. For example, if you select roll-up retention, set the RPO to one hour, and set the retention time at a site to one year, the system retains snapshots in the following ways:

- The 24 oldest hourly snapshots roll up into a single daily snapshot every 24 hours.
- The 7 oldest daily snapshots roll up into a single weekly snapshot at the end of every week.
- The 4 oldest weekly snapshots roll up into a single monthly snapshot at the end of every month
- The 12 oldest monthly snapshots roll up into a single annual snapshot at the end of every year.

At the end of one year, the site has 24 of the most recent hourly snapshots, 7 of the most recent daily snapshots, 4 of the most recent weekly snapshots, 12 of the most recent monthly snapshots, and 1 yearly snapshot. The system discards the snapshots used to create a rolled-up snapshot.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3333

Recovery Plans

A recovery plan orchestrates restoring protected VMs at a backup location, whether that location is on-premises or Nutanix DRaaS–based. Recovery plans can either recover all specified VMs at once or, with what is essentially a runbook functionality, use power-on sequences with optionally configurable interstage delays to recover applications gracefully and in the required order. Recovery plans that restore applications in Nutanix DRaaS can also create the required networks during failover and can assign public-facing IP addresses to VMs.

Recovery plans also allow protected VMs to run custom embedded scripts. If you have NGT installed, you can use a custom script to perform a variety of customizations, like changing desktop wallpaper or even updating existing management software after the failover. On failover, the recovery plan provides a variety of options to change or maintain VM IP addresses. The plan shows you the last four digits of the VM's new IP address beforehand so you can take action on it.

Offset-Based IP Mapping

Offset-based IP mapping tracks the last octet of VM IP addresses so you can automatically maintain or change them based on the subnet configuration in the recovery plan. If you keep the source and destination subnets the same, you can maintain the IP address. If you change the destination subnet to a new value, the new subnet keeps the last four digits. The following example migrates a SQL server with the IP address 192.168.0.100 to a new subnet with the IP address 192.168.1.1/24. When the SQL server fails over to the new subnet, the server's IP address is 192.168.1.100. Because you know the new IP address, you can plan any changes (like updating DNS records) before the failover happens.

- The IP address for the Production1 subnet is 192.168.0.1/24.
- The IP address for the Production2 subnet is 192.168.1.1/24.
- The IP address for the SQL server in the Production1 subnet is 192.168.0.100.
- The extract host offset of the VM is 0.0.0.100.
- The extract network offset of the Production100subnet is 192.168.1.0.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3334

- The mapped SQL Server IP address is 192.168.1.0. Add 0.0.0.100 to get the IP address after it fails over to a new subnet: 192.168.1.100.

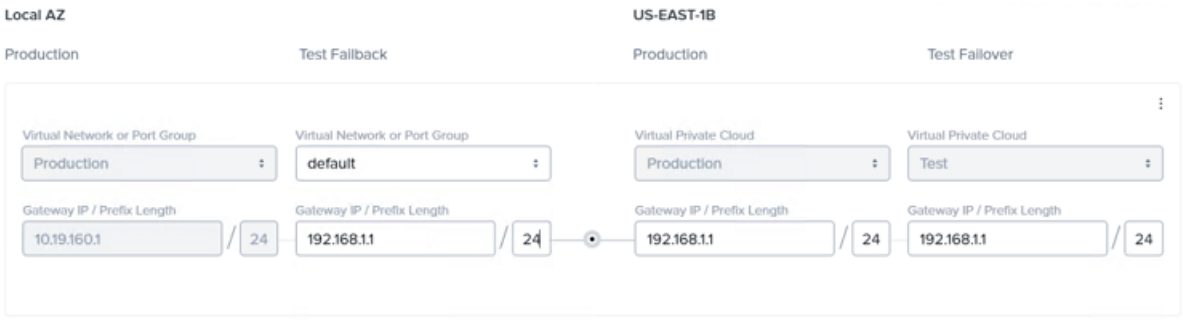


Figure 11: Offset Networking Mapping

If you want to manually assign static IP addresses to your VMs on failover, you can use custom IP mapping to do so as part of the recovery plan.

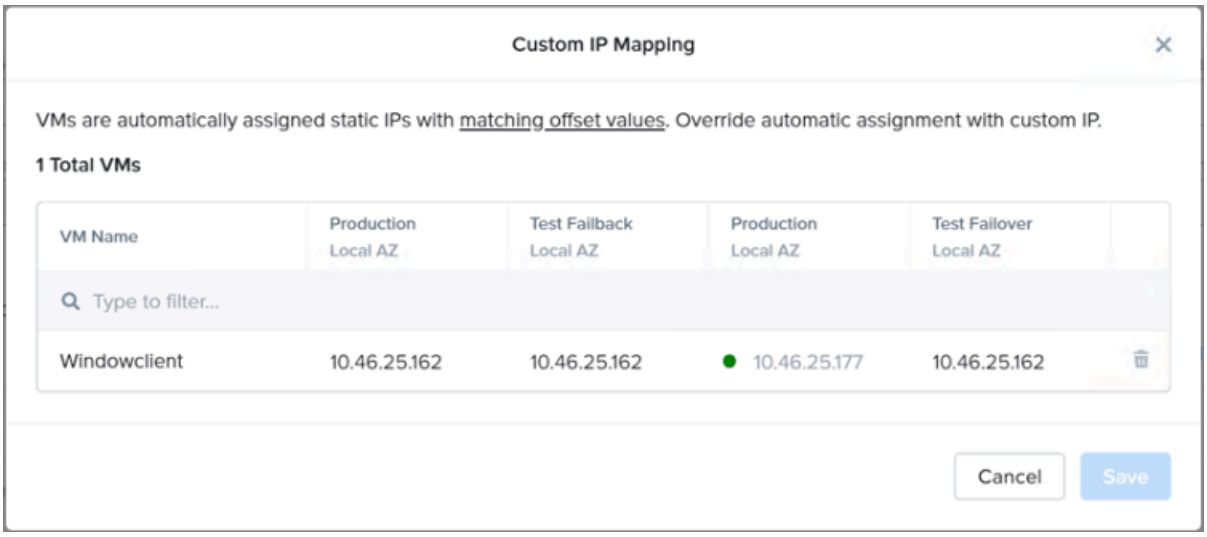


Figure 12: Custom IP Mapping

Recovery plans created at one location synchronize with the paired location and work bidirectionally. After VMs fail over from the primary location to the recovery location, you can use the same recovery plan to return the VMs to the original primary location using a failback mechanism. After you create a recovery plan, you can validate and test it to make sure the system can recover smoothly if it needs to fail over. Nutanix DRaaS includes a built-in virtual network for testing failover. The test network in the

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3335

cloud is isolated, so you can have workloads running on the source side and live-test your applications without affecting production. If you're replicating to an on-premises availability zone, your network team can create a nonroutable network for the test network to achieve the same kind of segmentation as Nutanix DRaaS.

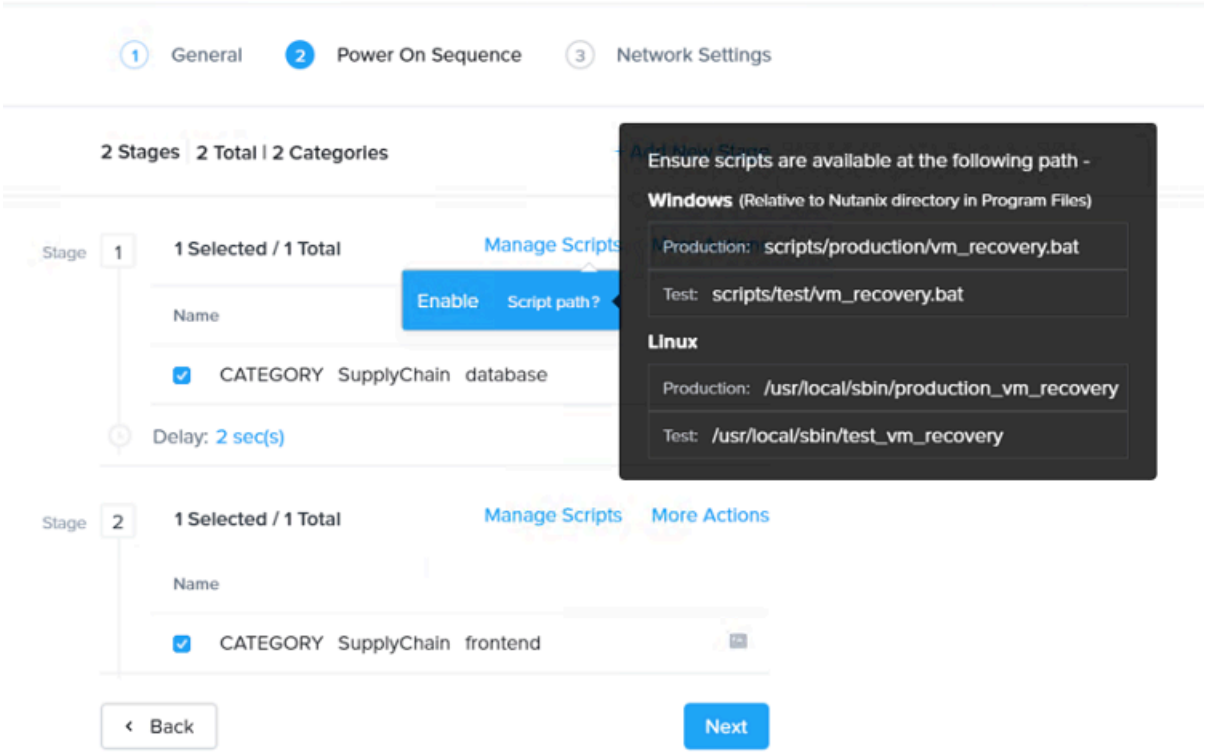


Figure 13: Recovery Plan Configuration

Because they operate independently of protection policies, recovery plans don't reference protection policies in their configuration information or create snapshots. However, during an unplanned failover, recovery plans rely on the availability of snapshots at the designated recovery location. You can either manually replicate snapshots or automate snapshot creation and replication using protection policies. (A planned failover doesn't require snapshots to be present at the recovery location in advance.)

The network mapping portion of the recovery plan allows for full and partial subnet failover for Nutanix DRaaS. If the source and destination availability zones have the

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3336

same network mapping, the full subnet fails over so applications can retain their IP addresses and you don't have to script and update the DNS. When an administrator runs a planned full subnet failover, even the MAC addresses are retained, which can be crucial when dealing with applications licensed through MAC and IP addresses. If you're using AHV's built-in IPAM, you don't have to install anything in the guest VM to retain the addresses. If you're using your own DHCP server or setting up your VMs with manual IP addresses, you can simply install the NGT software package. NGT helps maintain the network information regardless of the hypervisor.

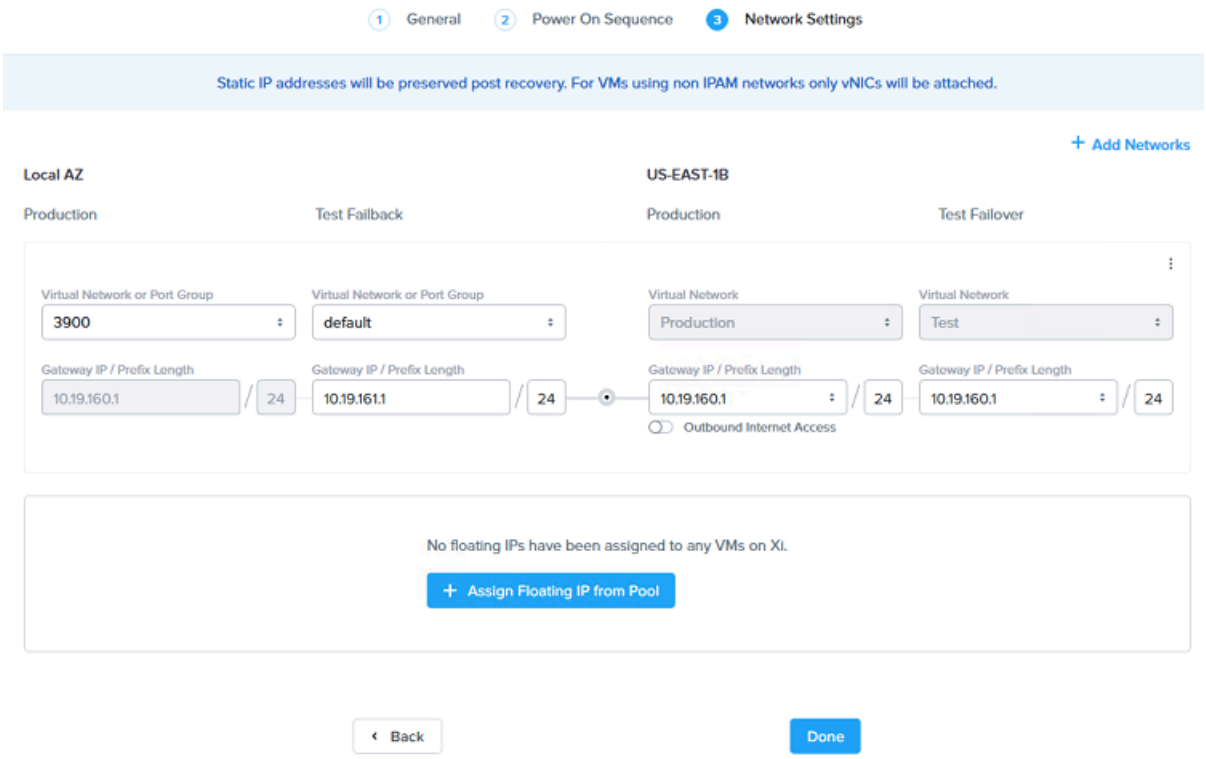


Figure 14: Network Mapping

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3337

6. Metro Availability

Metro Availability synchronously replicates data to another site, ensuring that a real-time copy of the data exists at a different location. During a disaster or planned maintenance, VMs can fail over from a primary site to a secondary site, guaranteeing nearly 100 percent uptime for applications.

Metro Availability is a continuous availability solution that provides a global file system namespace across a container stretched between Nutanix clusters. Synchronous storage replication across independent Nutanix clusters supports the stretched container using the protection domain and remote site constructs. You enable synchronous replication at the container level, and all VMs and files stored in that container replicate concurrently to another Nutanix cluster.

Each protection domain maps to one container. You can create multiple protection domains to enable different policies, including bidirectional replication, in which each Nutanix cluster replicates synchronously to another. Metro Availability currently supports a one-to-one relationship between protection domains, meaning that each container can replicate to one other remote site. Containers have two primary roles while enabled for Metro Availability: active and standby. Active containers replicate data synchronously to standby containers.

Failover between sites can be manual or automatic with the use of a witness. While the connection between site 1 and site 2 must have a round-trip time (RTT) of 5 milliseconds or less, the witness between sites can have an RTT of up to 200 ms. The witness is simply a VM deployed in a separate failure domain. The witness uses only a small amount of resources and must reside on a different network than site 1 and site 2. The witness helps protect against network partitions and primary and secondary site failures.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3338

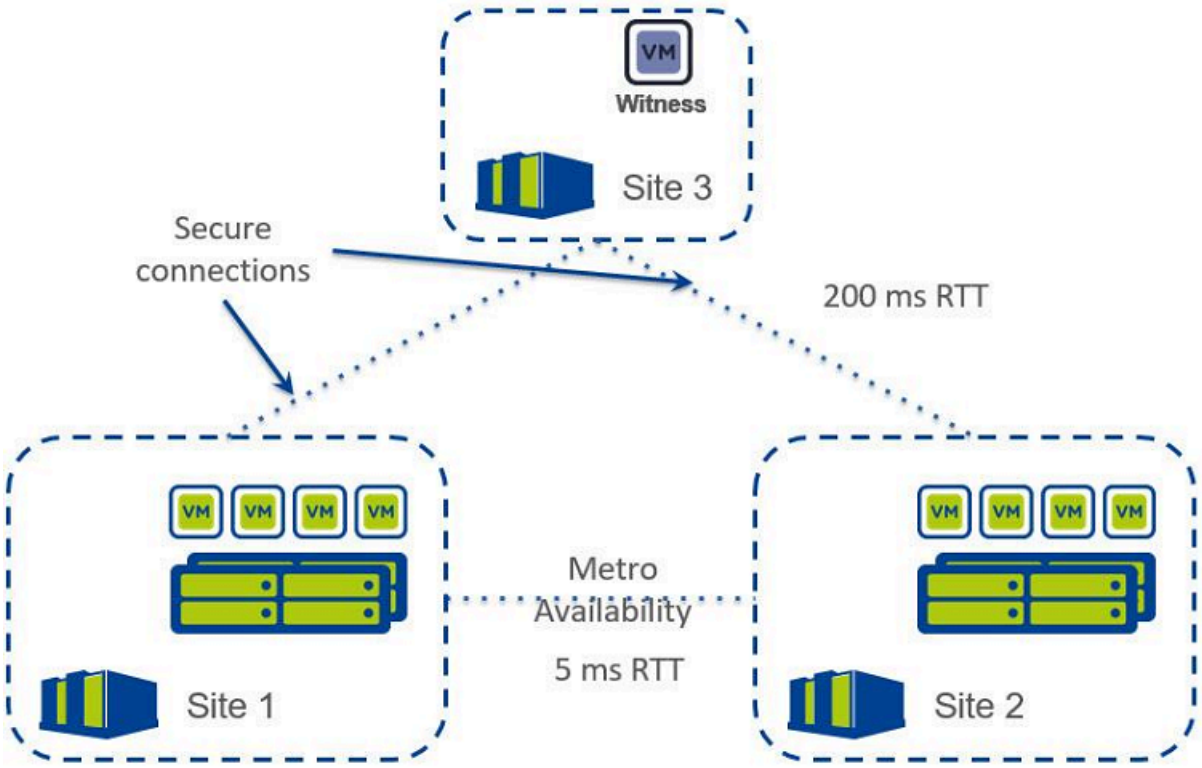


Figure 15: Metro Availability Overview

Metro Availability works in conjunction with existing Nutanix data management features, including compression, erasure encoding, deduplication, and tiering. Metro Availability also enables compression over the network for synchronous replication traffic between sites, reducing the total bandwidth required.

A version of synchronous replication that's very similar to Metro Availability is also available for AHV, ESXi, and Hyper-V environments, but the feature doesn't have disaster recovery workflows in these environments.

Some customers (for example, stock exchanges and clearing houses) have very stringent requirements and need to protect their data across multiple sites. Nutanix offers the following Metro Availability topology for customers who can't afford to lose any piece of data even in the most severe outages.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3339

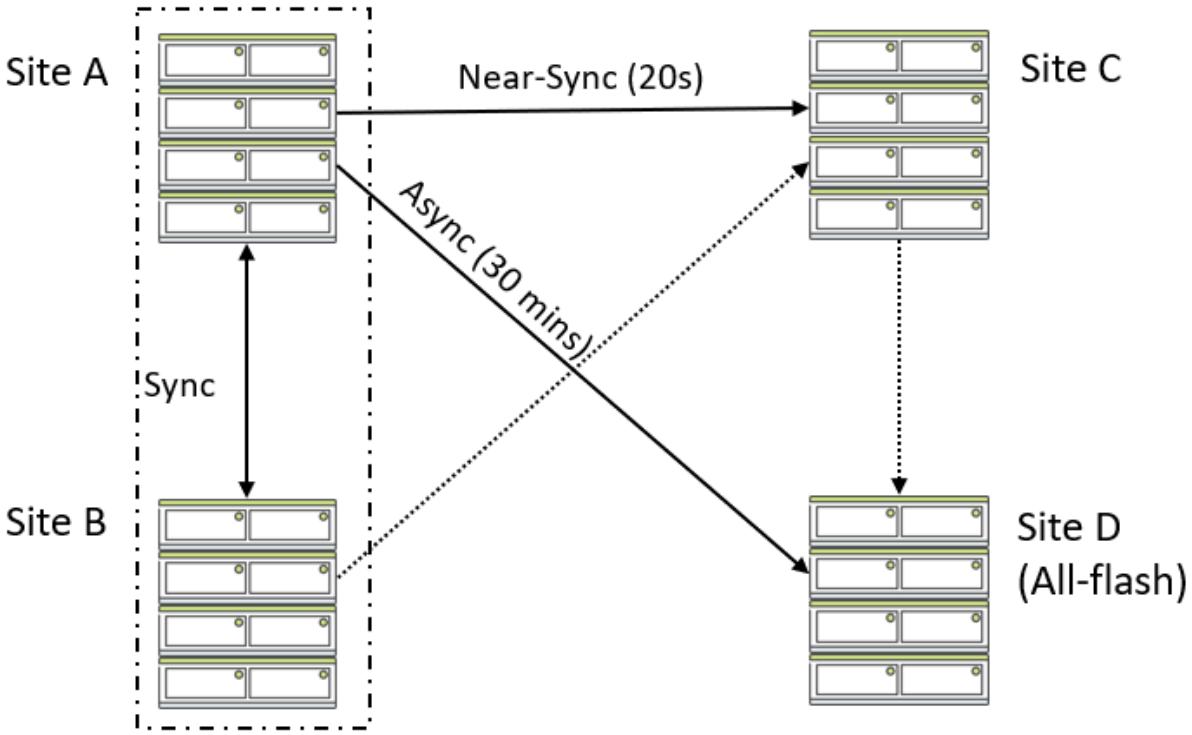


Figure 16: Metro Availability with NearSync and Asynchronous Replication

As shown in the previous figure, you can use Metro Availability between Site A and Site B, then use NearSync replication to Site C with an RPO as low as 20 seconds. You can use asynchronous replication between Site A and Site D, and if you're using an all-flash cluster in Site D, the RPO can be as low as 30 minutes. Because NearSync and asynchronous replication can cover great distances, you can have multiple copies for availability in the worst-case scenarios. Typically, a configuration this complex takes weeks to set up, but with Nutanix you can configure this setup in the Prism UI. When the system fails, you're protected and can restore services without much prior knowledge.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3340

7. Third-Party Integration with Nutanix

Nutanix integrates with popular offload capabilities such as VAAI and Microsoft Offloaded Data Transfer (ODX) to create clones in a matter of seconds with minimal overhead.

Additionally, with support for vStorage API for Data Protection (VADP) and by using VSS for application-level consistent snapshots, Nutanix backup and disaster recovery capabilities fully integrate with third-party tools such as Commvault, Druva, Symantec NetBackup, Veeam, and VMware SRM.

REST APIs

Nutanix provides an exhaustive list of REST APIs for various functions, including data protection and disaster recovery. These REST APIs are the foundation for the Nutanix Prism management interface and can be explored through the Nutanix Prism API explorer.

Nutanix Prism APIs can automate workflows using snapshots and replication for backup and disaster recovery through scripting languages or workflow engines. Prism APIs can also create runbook automation for failover, automatically registering VMs at the disaster recovery site in VMware vCenter and starting them. For example, you can use the Prism APIs to create a custom script that triggers the system to take and replicate a snapshot of the group of critical VMs making up an order-entry system, based on the number of transactions running.

Nutanix also offers a REST API for third-party backup vendor integration with changed-region tracking. This API uses the customized web-scale NoSQL implementation that handles metadata in the storage fabric. Given any two snapshots of a disk or file, the API responds with metadata that describes the regions that have changed between those snapshots, including the offset and length of the change. Changed-region tracking runs by default, so you don't need to configure it.

Changed-region tracking leads to faster backups and the ability to perform both differential and incremental backups across any hypervisor. The API is even beneficial

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3341

for full backups, as it reports which regions contain zeros, saving storage controller resources you might otherwise spend just reading zeros.

© 2024 Nutanix, Inc. All rights reserved |

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3342

8. Conclusion

Many enterprise workloads are either unprotected or underprotected. Budget constraints and deployment complexity can keep enterprises from protecting their applications, resulting in significant downtime caused by software and hardware glitches and user errors. As businesses virtualize more of their critical workloads, deploying data protection and disaster recovery becomes essential. Using application-granular snapshots and recovery, policy-based protection domains, asynchronous multisite replication, synchronous replication, Metro Availability, and centralized Prism management, Nutanix provides the tools to back up critical data, protect applications, and survive disasters efficiently without specialized skill or investment.

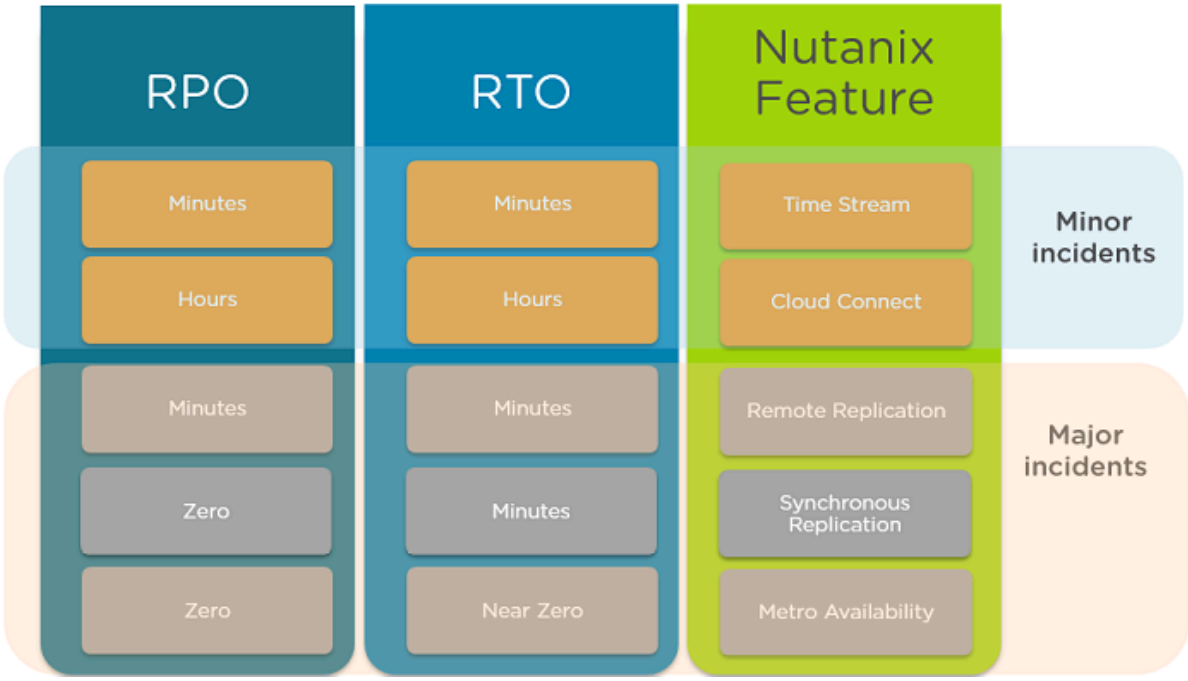


Figure 17: Nutanix Feature Matrix

© 2024 Nutanix, Inc. All rights reserved

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3343

About Nutanix

Nutanix offers a single platform to run all your apps and data across multiple clouds while simplifying operations and reducing complexity. Trusted by companies worldwide, Nutanix powers hybrid multicloud environments efficiently and cost effectively. This enables companies to focus on successful business outcomes and new innovations. Learn more at Nutanix.com.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3344

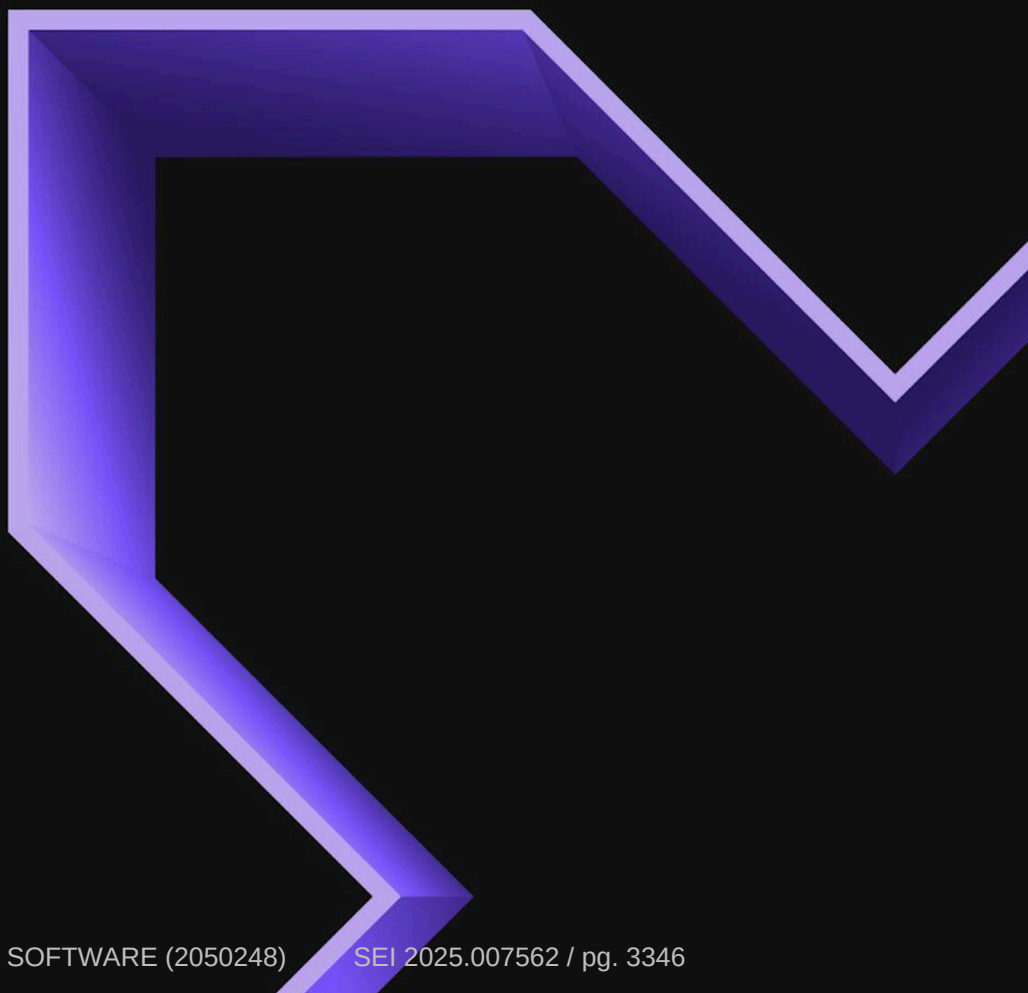
List of Figures

Figure 1: Overall Availability Features..... 5
Figure 2: Volume- or LUN-Level Snapshot Granularity..... 7
Figure 3: Byte-Level Nutanix Snapshots..... 9
Figure 4: Multiway Protection Domains..... 12
Figure 5: Use All Cluster Resources for Replication..... 13
Figure 6: Sample Deployment for Cloud Connect..... 15
Figure 7: Traditional Restore Process..... 16
Figure 8: LWS Creation on the Oplog..... 18
Figure 9: On-Premises and Nutanix-Based Availability Zones..... 21
Figure 10: Protection Policy Options..... 22
Figure 11: Offset Networking Mapping..... 25
Figure 12: Custom IP Mapping..... 25
Figure 13: Recovery Plan Configuration..... 26
Figure 14: Network Mapping..... 27
Figure 15: Metro Availability Overview..... 29
Figure 16: Metro Availability with NearSync and Asynchronous Replication..... 30
Figure 17: Nutanix Feature Matrix..... 33

v1.6 | January 2025 | TN-2032

SOLUTIONS DOCUMENT

Data Efficiency



NUTANIX

Legal

© 2025 Nutanix, Inc. All rights reserved. Nutanix, the Enterprise Cloud Platform, the Nutanix logo and the other Nutanix products, features, and/or programs mentioned herein are registered trademarks or trademarks of Nutanix, Inc. in the United States and other countries. All other brand and product names mentioned herein are for identification purposes only and are the property of their respective holder(s), and Nutanix may not be associated with, or sponsored or endorsed by such holder(s). This document is provided for informational purposes only and is presented "as is" with no warranties of any kind, whether implied, statutory or otherwise.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

Contents

1. Executive Summary....4

2. Nutanix Data Efficiency....6
Data Avoidance....6
Data Reduction....9

3. Conclusion....19

About Nutanix....20

List of Figures....21

1. Executive Summary

In this document, we describe how Nutanix AOS storage provides data avoidance and efficiency using techniques such as thin provisioning, intelligent cloning, compression, deduplication, and erasure coding (EC-X). These techniques accelerate application performance and optimize storage capacity. Unlike traditional storage architectures, the Nutanix web-scale design ensures that data efficiency techniques scale as the cluster grows—node by node, with no bottlenecks, single points of failure, or expensive proprietary hardware and software.

This document describes how the Nutanix Cloud Platform achieves data efficiency, including an introduction to the following features:

- Data transformations and utilization
- Thin provisioning
- Intelligent cloning
- Compression
- Deduplication
- EC-X

Table: Document Version History

Version Number	Published	Notes
1.0	November 2017	Original publication.
1.1	July 2019	Updated Nutanix overview.
1.2	April 2021	Updated Nutanix overview.
1.3	April 2022	Refreshed content.
1.4	June 2023	Updated the Nutanix Data Efficiency, Intelligent Cloning, and Data Reduction sections.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3349

Version Number	Published	Notes
1.5	November 2023	Added the Zero Suppression section. Updated the Erasure Coding section.
1.6	January 2025	Updated the Nutanix Data Efficiency section.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3350

2. Nutanix Data Efficiency

Nutanix incorporates a wide range of data and storage optimization technologies that work together to efficiently use the available capacity for any workload. These software-based technologies are massively scalable and adaptive to workload characteristics, eliminating the need for manual configuration and fine-tuning. The native compression, encoding, and deduplication features substantially increase storage efficiency and improve performance because of larger effective cache sizes in the performance tier.

Nutanix data efficiency capabilities are entirely software-based, and the Nutanix Cloud Platform doesn't rely on special networking hardware, such as custom application-specific integrated circuits or field-programmable gate arrays. It performs all data efficiency computation using an industry-standard server architecture. This approach facilitates regular product version upgrades so that Nutanix can deliver improved capabilities and future enhancements as a simple software update.

You can enable deduplication, compression, and EC-X on the same container or different containers as required. AOS 6.1 also introduced the ability to set compression on individual VMs or groups of VMs using storage policies in Prism Central.

To view capacity optimization and storage overprovisioning metrics, go to **Hardware** > **Clusters** in Prism Central or **Storage** in Prism Element. You can also view the following stats for individual storage containers on their summary pages:

- Data reduction ratio
- Data reduction savings (in TiB)
- Overall efficiency ratio
- Storage overprovisioning ratio

Data Avoidance

Data avoidance technologies typically contribute the most to data efficiency. They prevent unnecessary data creation and minimize the need for more resource-demanding data reduction technologies. With fewer back-end operations, more resources are

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3351

available for front-end (or user-driven) operations and applications. Because Nutanix data avoidance technologies are on by default, you don't need to manually configure or fine-tune your environment.

Zero Suppression

Zero suppression ensures efficient storage capacity usage by omitting zeros from writes. If write I/O from a VM or application contains zeros, AOS doesn't write those zeros to storage. It only updates the metadata to imply that the written data contains zeros.

Thin Provisioning

Thin provisioning is a simple and broadly adopted technology for increasing data capacity usage by overcommitting resources. Nutanix enables this feature in all containers by default. In deployments using VMware ESXi, the system presents containers to hosts as natively thin-provisioned NFS datastores. Thin provisioning on Nutanix outperforms thick provisioning, and we recommend it for all workloads.

Some applications, such as Oracle RAC and vSphere Fault Tolerance, require thick provisioning. Nutanix storage supports thick-provisioned (eager zero or lazy zero) VMDKs using the VMware API for Array Integration (VAAI) NAS reserve space primitive. Eager-zeroed thick VMDKs guarantee space reservations but don't write data: AOS storage acknowledges every I/O operation and performs a simple metadata update.

The storage overprovisioning widget shows the ratio of provisioned storage to available raw storage. Calculations for the overall efficiency metric account for savings from thin provisioning. You can view the current thick-provisioned capacity in Prism on the Storage Container Details page.

Intelligent Cloning

Nutanix storage provides native support for space-efficient, offloaded VM clones. You can choose to provision clones automatically using VAAI, View Composer for Array Integration (VCAI), and Microsoft Offloaded Data Transfer (ODX) or interactively using nCLI, REST, or Nutanix Prism. Nutanix clones are based on Nutanix snapshots that use a redirect-on-write algorithm, which is the most effective and space-efficient virtual disk (vDisk) sharing technique.

On the Nutanix platform, VMs store data as vDisk files. Each vDisk is composed of logically contiguous data chunks called extents. The platform stores these extents in

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3352

physically contiguous groups as files on storage devices. When you clone a VM, the system marks the base vDisk read-only and creates another vDisk for reads and writes. Both vDisks have the same block map, which is a metadata mapping of the vDisk to its corresponding extents.

The following figure shows what happens when you clone a VM.

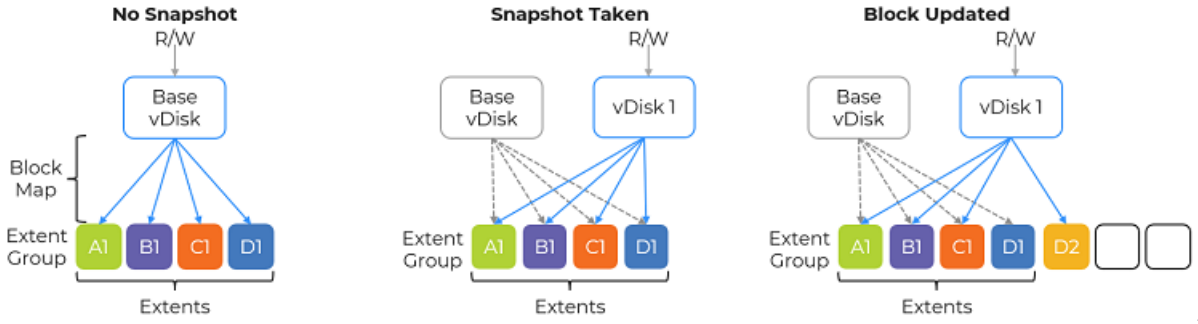


Figure 1: Example Clone Block Map

The system uses the same method for multiple clones of a VM or vDisk. Clone operations update metadata only, so no I/O takes place, and the clones occupy very little additional space. You can also replicate clones the same way; essentially, the previously cloned VM acts as the base vDisk. On cloning, the system locks the base vDisk's block map and creates two clones, with one block map for the previously cloned VM and another block map for the new clone. Any new metadata writes or updates occur in the new individual block maps. Any subsequent clones lock the original block map and create a new one for read and write access.

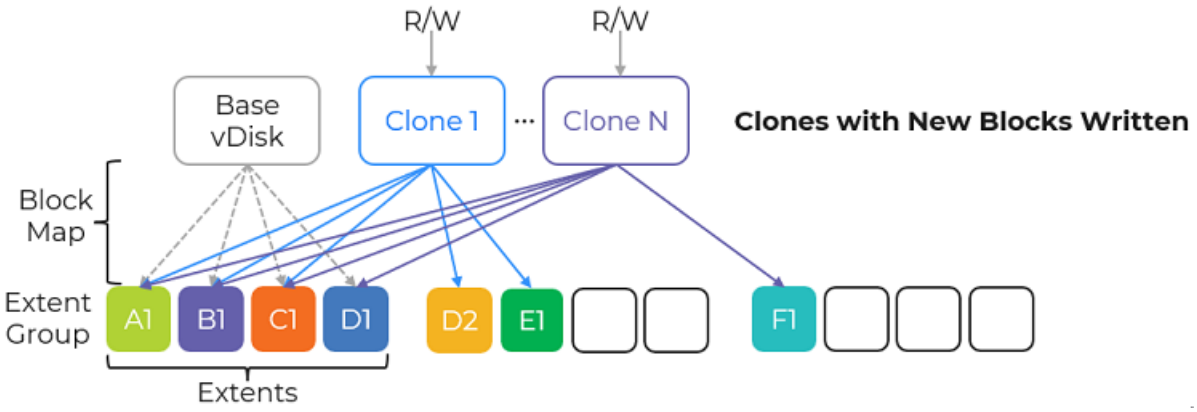


Figure 2: Clone Block Maps: New Write

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3353

You can make as many clones as you need.

Calculations for the overall efficiency metric account for intelligent cloning savings. You can view this metric in Prism on the Storage Container Details page.

Data Reduction

The Nutanix AOS Capacity Optimization Engine (COE) transforms data to increase data efficiency on disk. The engine increases the effective cluster storage capacity by eliminating repetitive data as it's written to the system or by transforming it using mathematical functions postprocess as a series of MapReduce jobs. Compression, deduplication, and EC-X are easy to configure on the container and give you the flexibility to fine-tune data reduction techniques.

Compression

Nutanix storage provides both inline and postprocess compression to suit your data types and application usage patterns. The inline method compresses sequential data streams or large I/O sizes (more than 64 KB) as they're written to the capacity store (extent store). Postprocess compression initially writes the data in an uncompressed state and uses the Curator framework to compress it clusterwide. AOS compresses all incoming write I/O operations over 4 KB inline in the persistent write buffer (oplog), so you can use oplog capacity more efficiently and sustain performance. Supported versions of AOS enable inline compression (compression delay=0) by default for all new containers.

Nutanix uses LZ4 and LZ4HC algorithms for data compression in supported AOS versions. On initial ingest, LZ4 compresses regular data, which provides a very good balance between compression and performance. As data cools, LZ4HC further compresses it to improve the compression ratio.

We define cold data with two main categories:

- Regular data: No read or write access for three days
- Immutable data (snapshots): No read or write access for one day

The following figure shows how inline compression interacts with the write I/O path.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3354

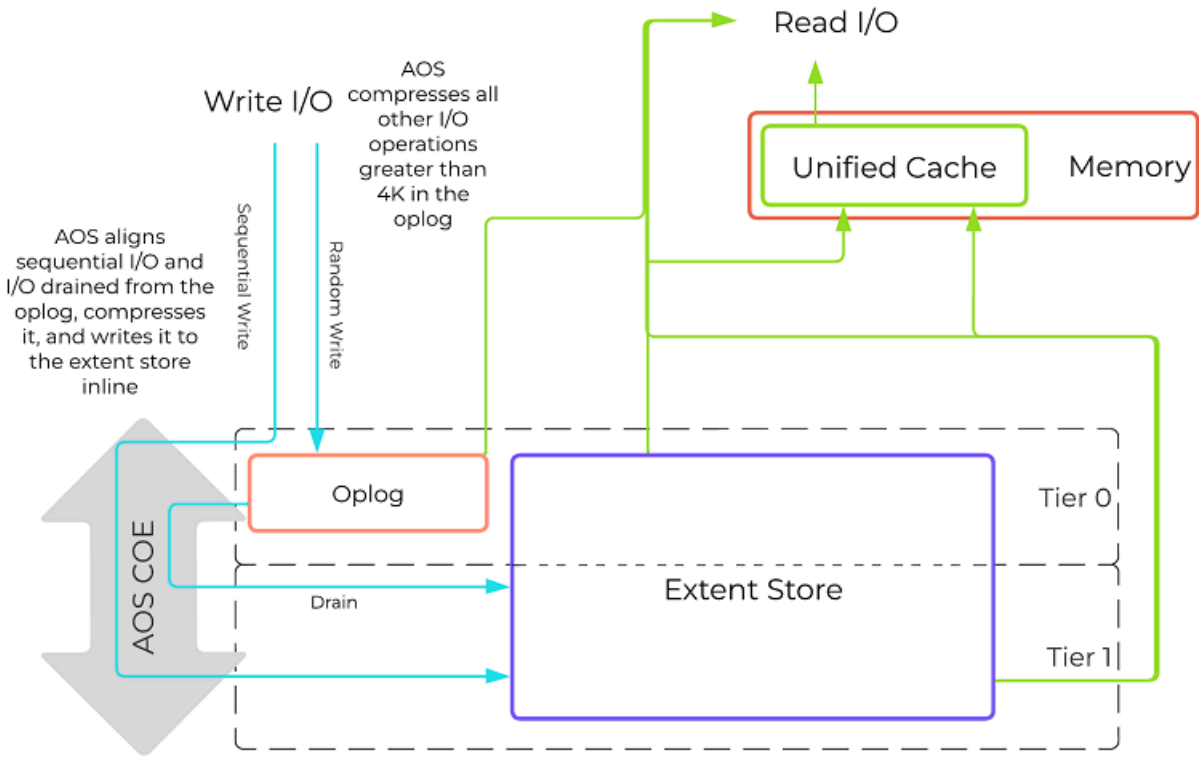


Figure 3: Inline Compression I/O Path

In most cases, we recommend inline compression (compression delay=0) because it only compresses large or sequential writes and doesn't affect random write performance. Inline compression can improve performance by increasing the usable size of the SSD tier. In addition, when the system replicates large or sequential data for protection, it can send compressed data, improving performance because less data travels across the network. Inline compression also pairs well with EC-X.

When you enable postprocess compression, all new write I/O follows the normal I/O path without compression. After the data meets the compression delay setting (which you can configure in Nutanix Prism), it can be compressed in the extent store. Postprocess compression tasks use the Curator MapReduce framework to distribute work across all nodes. Automatic resource adjustments between front- and back-end operations ensure that postprocess compression tasks don't limit user application performance.

The following figure shows how postprocess compression interacts with the write I/O path.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3355

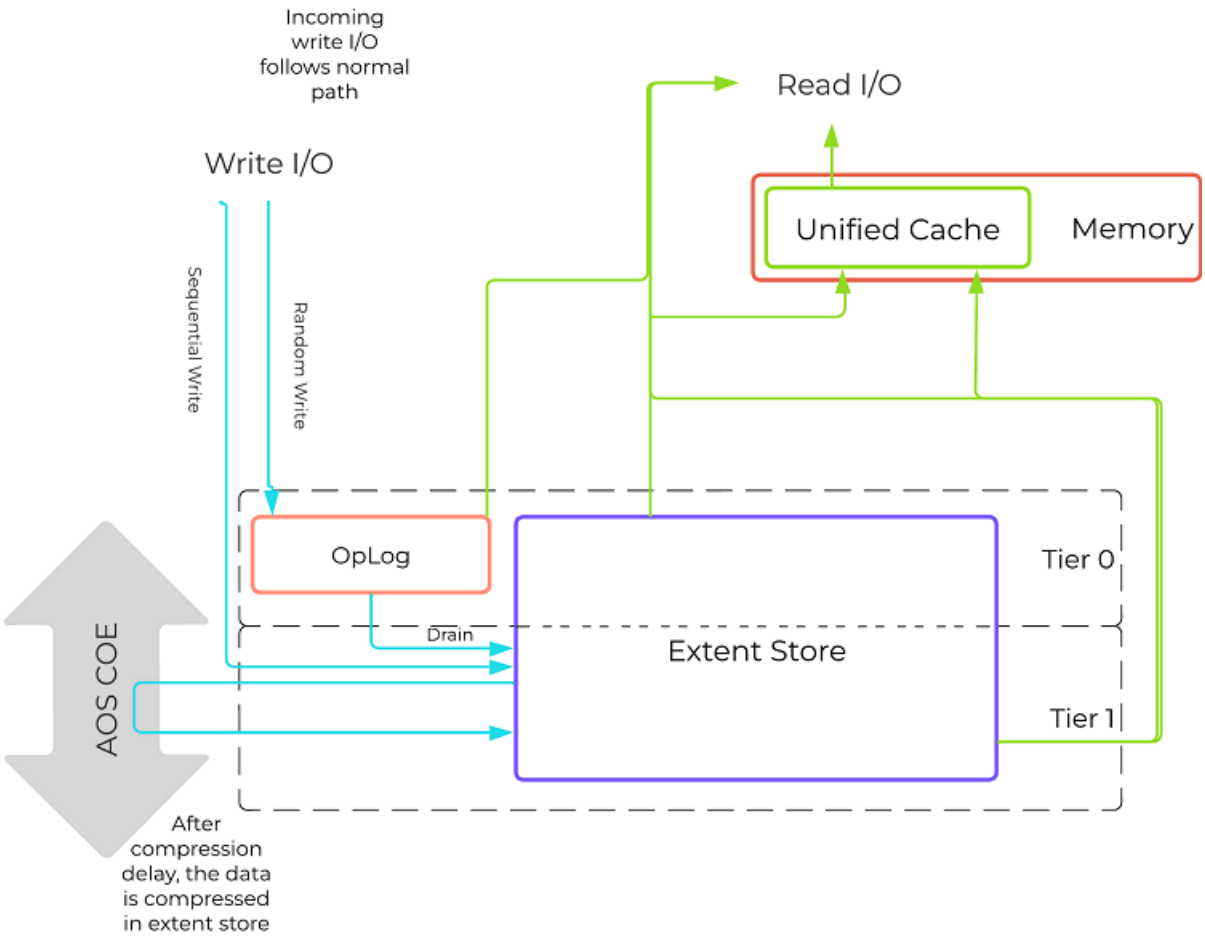


Figure 4: Postprocess Compression I/O Path

For read I/O operations on compressed data, the system first decompresses the data in memory and then serves the I/O. The system decompresses heavily accessed data in the extent store and then moves it to the cache.

> **Note:** To view current compression rates in Prism, hover over the **Compression** setting on the Storage Container Details page.

We recommend compression for almost all use cases except the following workloads:

- Encrypted datasets
- Compressed datasets (images, audio, and video)

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3356

Erasure Coding

The Nutanix platform relies on a replication factor for data protection and availability. This method provides the highest degree of availability because it doesn't require data recomputation on failure or reading from more than one storage location. Replication factor 2 (also called fault tolerance 1) creates two data copies, and replication factor 3 (also called fault tolerance 2) creates three data copies. Because the replication factor creates full copies of data, replication factor 2 decreases effective storage capacity to 50 percent, and replication factor 3 decreases effective storage capacity to 33 percent.

To provide a balance between availability and storage capacity consumption, Nutanix storage offers EC-X. Like RAID (levels 4, 5, 6, and so on), EC-X encodes a strip of data blocks on different nodes and calculates parity. In the event of a host or disk failure, the system can use parity to decode any missing data blocks. In AOS, a data block is an extent group between 1 MB and 4 MB in size.

You can configure the number of data and parity blocks in a strip based on how many failures you can tolerate. AOS dynamically calculates the erasure coding strip sizes depending on the number of nodes, blocks, and racks. The configuration is the number of data blocks divided by the number of parity blocks.

Replication factor 2–like availability (n + 1) consists of two, three, or four data blocks and one parity block in a strip (in other words, 2:1, 3:1 or 4:1). Replication factor 3–like availability (n + 2) consists of two, three, or four data blocks and two parity blocks in a strip (in other words, 2:2, 3:2 or 4:2). We support and recommend maximum strip sizes of 4:1 for replication factor 2–like availability and 4:2 for replication factor 3–like availability.

We recommend that you size your clusters with at least one more node than the combined strip size (data and parity) for replication factor 2 availability and at least two more nodes than the combined strip size for replication factor 3 availability.

Replication factor 2 uses twice as much storage as replication factor 1, and replication factor 3 uses three times as much storage as replication factor 1. You can calculate the expected EC-X storage use as the number of parity blocks divided by the number of data blocks. For example, a 4:1 strip uses 25 percent more storage than replication factor 1, and a 4:2 strip uses 50 percent more.

The following table shows EC-X data and parity configuration options based on the number of nodes and replication factor used and the encoded strip size overheads.

Table: EC-X Strip Size and Overheads

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3357

Cluster Size (Nodes)	EC-X Strip Size (Replication Factor 2 Availability)	EC-X Overhead (Replication Factor 2 Availability)	EC-X Strip Size (Replication Factor 3 Availability)	EC-X Overhead (Replication Factor 3 Availability)
4	2:1	1.5×	N/A	N/A
5	3:1	1.33×	N/A	N/A
6	4:1	1.25×	2:2	2×
7	4:1	1.25×	3:2	1.6×
8+	4:1	1.25×	4:2	1.5×

AOS performs EC-X postprocess on write-cold data, using the Curator MapReduce framework for task distribution. AOS determines the block placement in a strip based on the read nature of data (read-hot versus read-cold). For read-cold data, AOS distributes data blocks from the same vDisk across nodes to form the strip. This process makes garbage collection easier because you can remove a full strip when you delete the vDisk. For read-hot data, AOS keeps the vDisk data blocks local to the node providing data locality for reads and forms the strip with data from different vDisks. If a read-cold strip becomes hot, AOS tries to bring the remote data blocks local.

Because MapReduce is a postprocess framework, it doesn't affect the traditional write I/O path. Automatic resource adjustments between front- and back-end operations ensure that EC-X tasks don't limit user application performance.

You can change the replication factor for containers with EC-X enabled to achieve your desired level of data protection during the application life cycle. Because containers can transition efficiently between replication factor 2 and replication factor 3, the system can create or remove a resulting parity block automatically without additional read-modify-write operations.

Nutanix automatically adjusts the size of existing, erasure-coded strips during node additions and removals. This feature limits the protection overhead after node removals and continues to optimize capacity usage as the cluster grows.

You can override the default strip size (which is 4:1 for replication factor 2 or 4:2 for replication factor 3) using the nCLI. In the following example command, <N> is the number of data blocks and <K> is the number of parity blocks:

```
ctr [create/edit] ... erasure-code=<N>/<K>
```

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3358

The following figure illustrates the data layout of a normal environment using a replication factor.

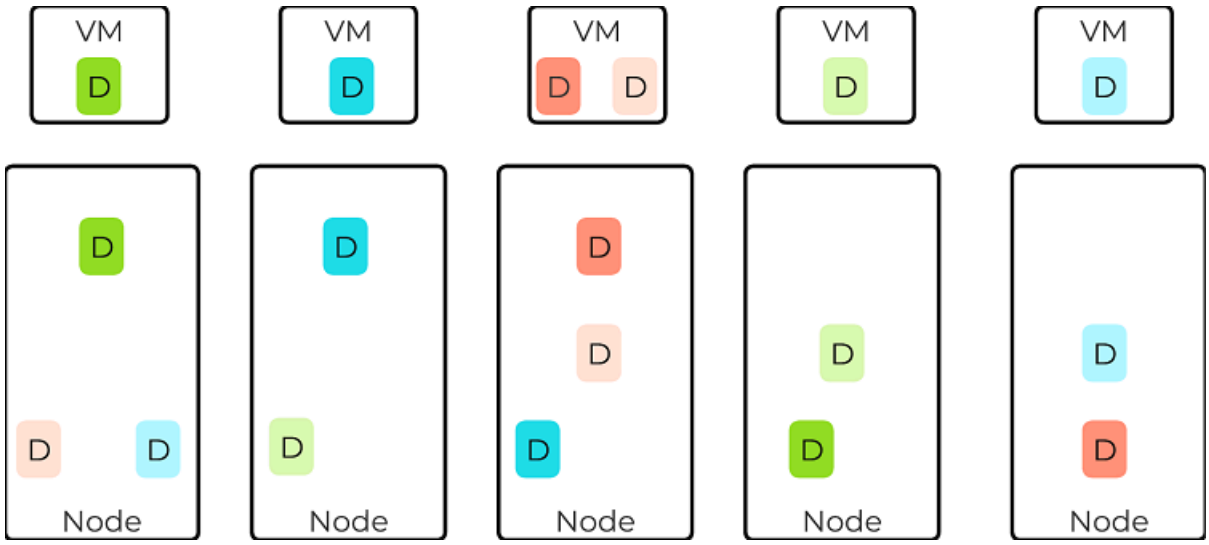


Figure 5: Typical Replication Factor Data Layout

This layout has replication factor 2 data whose primary copies are local and whose replicas are distributed to other nodes throughout the cluster.

When Curator runs a full scan, it finds eligible write-cold extent groups (data not written or overwritten for seven days) that are available for encoding. After the Curator process finds the eligible candidates, Chronos distributes and throttles the encoding tasks.

The following figure shows an example of a 3:1 strip. The strips are constructed of extent groups from different vDisks on different nodes and parity blocks.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3359

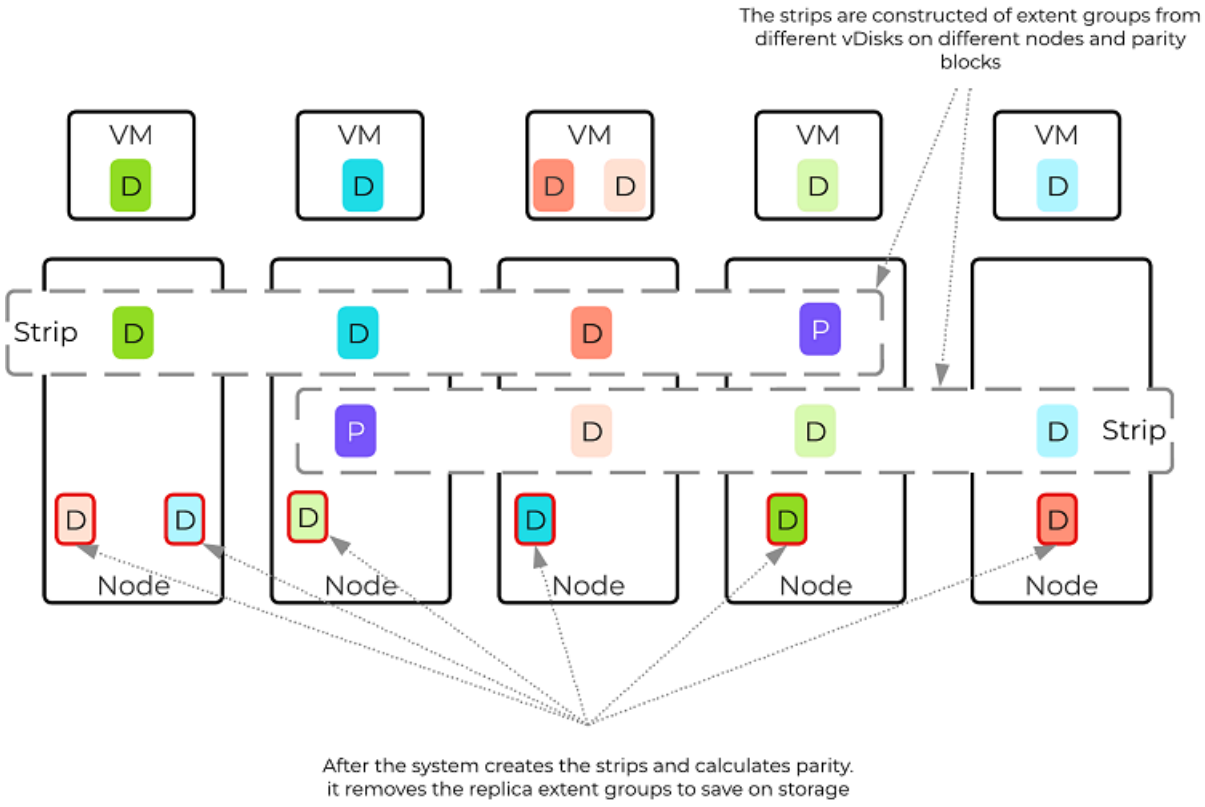


Figure 6: Strips Before Encoding

After the system creates the strips and calculates parity, it removes the replica extent groups to save on storage. The following figure shows the environment and storage savings after AOS finishes EC-X.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3360

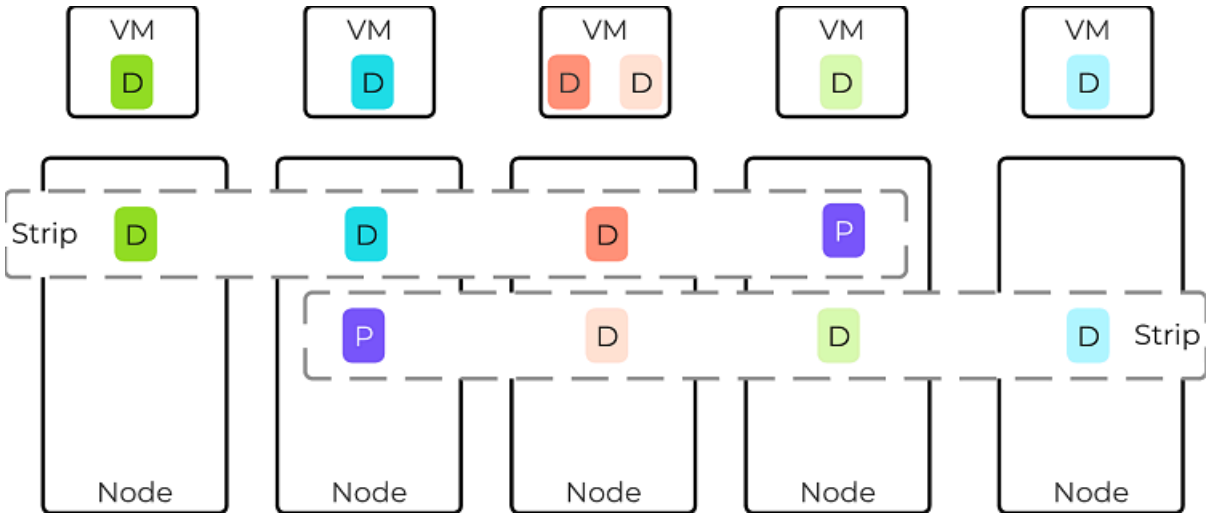


Figure 7: Strips After Encoding

You can enable inline EC-X on containers using nCLI. Inline EC-X creates coding strips inline by erasure-coding the data without waiting for it to become write-cold. Inline EC-X creates the erasure-coded strips on the same vDisk data by default. With AOS 6.6, you can create strips across different vDisks if you require data locality. We only recommend using inline EC-X for workloads that don't perform numerous overwrites.

> **Note:** Nutanix Objects containers enable inline EC-X by default.

To view EC-X storage savings in Prism, hover over the **Erasure Coding** setting on the Storage Container Details page.

We recommend using EC-X for write once, read many (WORM) workloads and other workloads with limited overwrites:

- Nutanix Objects
- Backups
- Archives
- File servers
- Log servers
- Email (depending on usage)

Don't use EC-X with the following workloads:

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3361

- Anything write or overwrite intensive
- VDI

> **Note:** Because of data-avoidance technology like intelligent cloning, VDI workloads are typically very write intensive but not capacity intensive.

Elastic Deduplication Engine

The Elastic Deduplication Engine deduplicates data in the extent store. Unlike traditional approaches that use background scans to read data again, the Elastic Deduplication Engine stores fingerprints persistently as part of the written block's metadata. The stored fingerprints allow the Elastic Deduplication Engine to detect and remove duplicate copies without scanning or reading the data again.

At ingest, the Elastic Deduplication Engine fingerprints data streams with 64 KB or more I/O operations (either initial I/O operations or when draining from the oplog) at a 16 KB granularity in every 1 MB extent. AOS uses logical checksums to select candidates for deduplication.

In previous versions, AOS marked an entire extent for deduplication if it found duplicates for more than 40 percent of the 16 KB chunks in a 1 MB extent. This process created many dedupe extents that didn't have duplicates. Starting with version 6.6, AOS only marks chunks with duplicates for deduplication, not the entire extent. This enhancement significantly reduces the metadata required for deduplication.

After AOS marks the duplicate chunks for deduplication, the Curator MapReduce framework removes those chunks. Automatic resource adjustments between front- and back-end operations ensure that deduplication tasks don't limit user application performance.

The following figure illustrates how the Elastic Deduplication Engine interacts with the I/O path.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3362

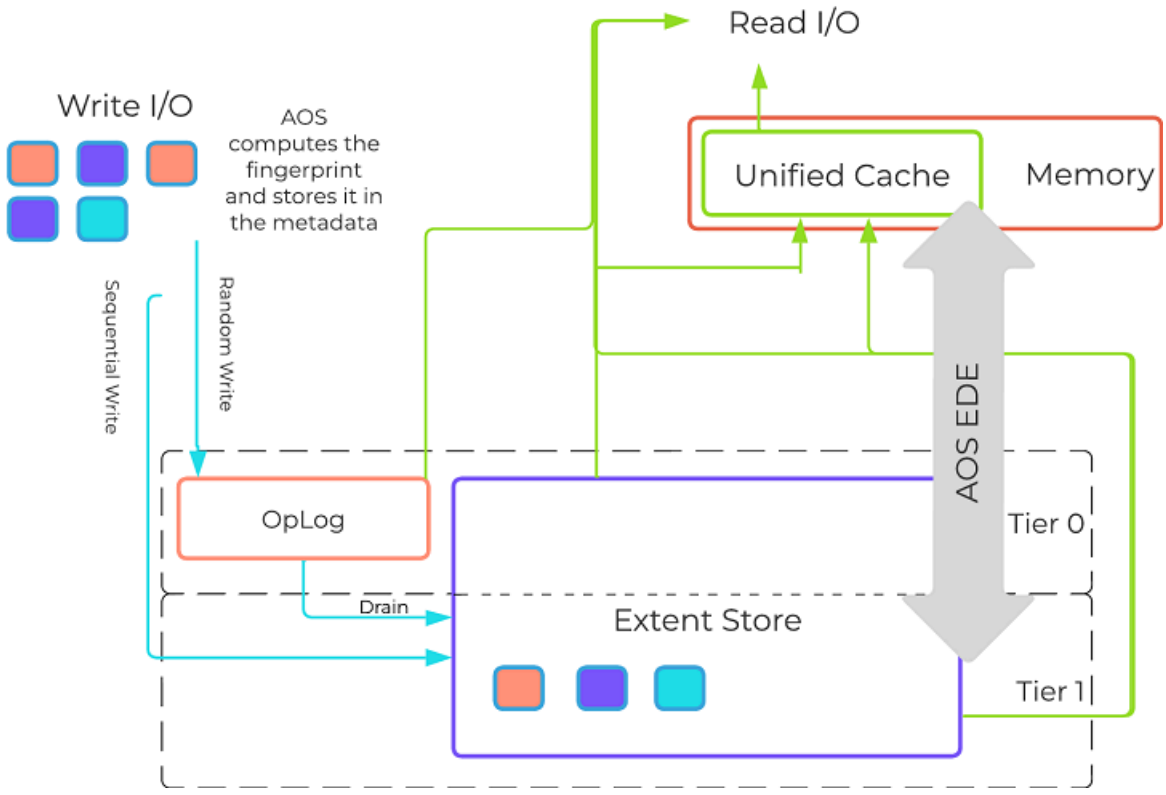


Figure 8: Elastic Deduplication Engine I/O Path

To view the current deduplication savings in Prism, hover over the **Capacity Deduplication** setting on the Storage Container Details page.

We recommend deduplication for the following workloads:

- Full clones in VDI
- Persistent desktops
- Physical to virtual and virtual to virtual conversion when using Hyper-V because Windows ODX uses a full data copy

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3363

3. Conclusion

The Nutanix Cloud Platform incorporates agile and scalable data-efficiency techniques. Thin provisioning and intelligent cloning, which are native data-avoidance technologies, provide significant space savings and fast snapshots and replicas. Deduplication and compression generate dramatic performance improvements while increasing the cluster's effective storage capacity—all with low computational overhead. The Nutanix EC-X algorithm delivers predictable storage efficiency across all data types and workloads without affecting performance.

For more information on data efficiency with Nutanix or to review other Nutanix technical documents, see the Nutanix website.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3364

About Nutanix

Nutanix offers a single platform to run all your apps and data across multiple clouds while simplifying operations and reducing complexity. Trusted by companies worldwide, Nutanix powers hybrid multicloud environments efficiently and cost effectively. This enables companies to focus on successful business outcomes and new innovations. Learn more at Nutanix.com.

© 2025 Nutanix, Inc. All rights reserved |

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3365

List of Figures

Figure 1: Example Clone Block Map.....8
Figure 2: Clone Block Maps: New Write.....8
Figure 3: Inline Compression I/O Path.....10
Figure 4: Postprocess Compression I/O Path.....11
Figure 5: Typical Replication Factor Data Layout.....14
Figure 6: Strips Before Encoding.....15
Figure 7: Strips After Encoding.....16
Figure 8: Elastic Deduplication Engine I/O Path.....18

v4.5 | October 2024 | TN-2038

SOLUTIONS DOCUMENT

Nutanix AHV Virtualization

NUTANIX

Legal

© 2024 Nutanix, Inc. All rights reserved. Nutanix, the Enterprise Cloud Platform, the Nutanix logo and the other Nutanix products, features, and/or programs mentioned herein are registered trademarks or trademarks of Nutanix, Inc. in the United States and other countries. All other brand and product names mentioned herein are for identification purposes only and are the property of their respective holder(s), and Nutanix may not be associated with, or sponsored or endorsed by such holder(s). This document is provided for informational purposes only and is presented "as is" with no warranties of any kind, whether implied, statutory or otherwise.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

Contents

1. Executive Summary 5

2. Nutanix AHV Components 7

3. AHV Integrated Management Capabilities 9
- Cluster Management 9
- Virtual Machine Management 12

4. Performance and Scale 21
- AHV Turbo 21
- vNUMA 21
- Remote Direct Memory Access 22
- iSCSI Extensions for RDMA 22
- Memory Overcommit 23
- Virtual Trusted Platform Module and Secure Boot 23

5. Graphics Processing Unit Support 24
- GPU Passthrough 24
- vGPU 24

6. Migration 27
- Nutanix Move 27
- Cluster Conversion 27

7. Security 29
- Security Development Life Cycle 29
- Security Baseline and Self-Healing 29
- Prism Audits 30
- Credential Guard 30
- Nutanix Data Lens 30
- Nutanix Flow Virtual Networking 30
- Nutanix Flow Network Security 31

8. Conclusion..... 33

9. References..... 34

About Nutanix.....35

List of Figures.....36

1. Executive Summary

Nutanix natively converges compute and storage into a single appliance that you can deploy in minutes to run any application out of the box. The Nutanix solution offers powerful virtualization capabilities—including core virtual machine (VM) operations, live migration, VM high availability, and virtual network management—as fully integrated features of the infrastructure stack rather than standalone products that require separate deployment and management.

The native Nutanix hypervisor, AHV, represents a fresh approach to virtualization that brings substantial benefits to enterprise IT administrators by simplifying every step of the infrastructure life cycle, from buying and deploying to managing, scaling, and supporting.

Table: Document Version History

Version Number	Published	Notes
1.0	January 2016	Original publication.
1.1	July 2016	Updated platform information.
1.2	December 2016	Updated for AOS 5.0.
1.3	May 2017	Updated for AOS 5.1.
2.0	December 2017	Updated for AOS 5.5.
2.1	March 2019	Updated for AOS 5.10 and updated Nutanix overview.
2.2	January 2020	Updated Nutanix overview and the AHV section.
3.0	June 2020	Updated terminology throughout.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3371

Version Number	Published	Notes
4.0	January 2022	Updated for AOS 6.1 in the Live Migration, Backup APIs, and vGPU sections, and added VM Templates, OVA Import and Export, Metro Availability, Memory Overcommit, vGPU Live Migration, Credential Guard, Flow Network Visualization, and Flow Microsegmentation sections.
4.1	September 2022	Updated for AOS 6.5.1 by adding the Virtual Trusted Platform Module section.
4.2	October 2023	Updated for AOS 6.7 in the Live Migration, Generation ID, Compute-Only Nodes, iSCSI Extensions for RDMA (iSER), and Migration sections.
4.3	July 2024	Updated the Graphics Processing Unit Support section.
4.4	September 2024	Updated live migration guidance in the Graphics Processing Unit Support section.
4.5	October 2024	Added the Advanced Processor Compatibility and Automatic Cluster Selection sections.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3372

2. Nutanix AHV Components

Nutanix built AHV on a proven open-source Kernel-based Virtual Machine (KVM) foundation and extended KVM's base functionality to include features such as high availability and live migration. AHV comes preinstalled on Nutanix appliances and you can configure it in minutes to deploy applications.

AHV has three main components:

KVM-kmod

KVM kernel module.

Libvirtd

An API, daemon, and management tool for managing KVM and the QEMU emulator. Communication between AHV, KVM, and QEMU occurs through libvirtd.

Qemu-KVM

A machine emulator and virtualization tool that runs in user space for every VM (domain). AHV uses it for hardware-assisted virtualization, and VMs run as hardware virtual machines.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3373

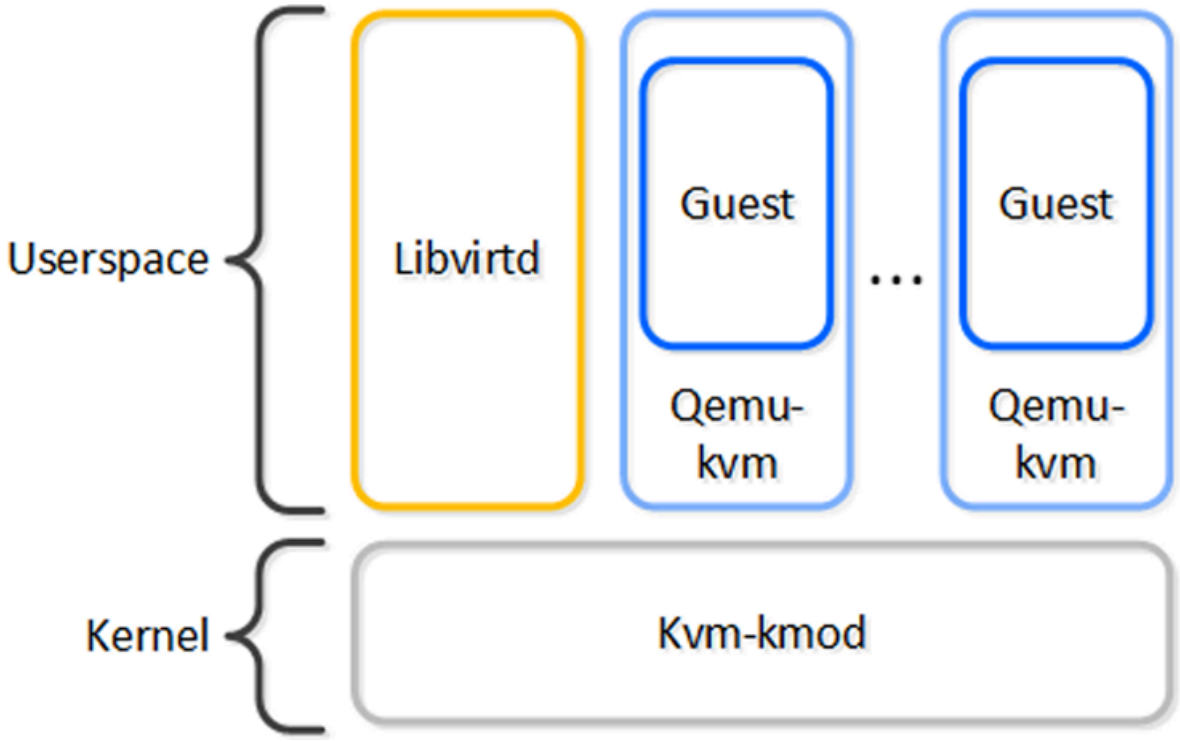


Figure 1: AHV Components

© 2024 Nutanix, Inc. All rights reserved

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3374

3. AHV Integrated Management Capabilities

You can manage the Nutanix platform from a single pane of glass with Nutanix Prism. Prism provides integrated capabilities for cluster management and VM management that are available from the Prism web console, command line interface (CLI), PowerShell, and REST API.

Cluster Management

Managing clusters on AHV focuses on creating, updating, deleting, and monitoring cluster resources. These resources include hosts, storage, and networks.

Host Profiles

Prism provides a central location for administrators to update host settings like virtual networking and high availability across all nodes in an AHV cluster. Controlling configuration at the cluster level eliminates the need for manual compliance checks and reduces the risk of having a cluster that isn't uniformly configured.

Storage Configuration

Nutanix uses hypervisor-agnostic distributed storage to deliver data services such as storage provisioning, snapshots, clones, and data protection to VMs directly, rather than using the hypervisor's storage stack. On each AHV host, an iSCSI redirector service establishes a highly resilient storage path from each VM to storage across the Nutanix cluster. QEMU is configured with the iSCSI redirector as the iSCSI target portal. When the redirector receives a sign-in request, it performs an iSCSI sign-in redirect to a healthy Controller VM (CVM) (preferably the local one).

For more information on AHV storage, see Storage Overview in the AHV Administration Guide.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3375

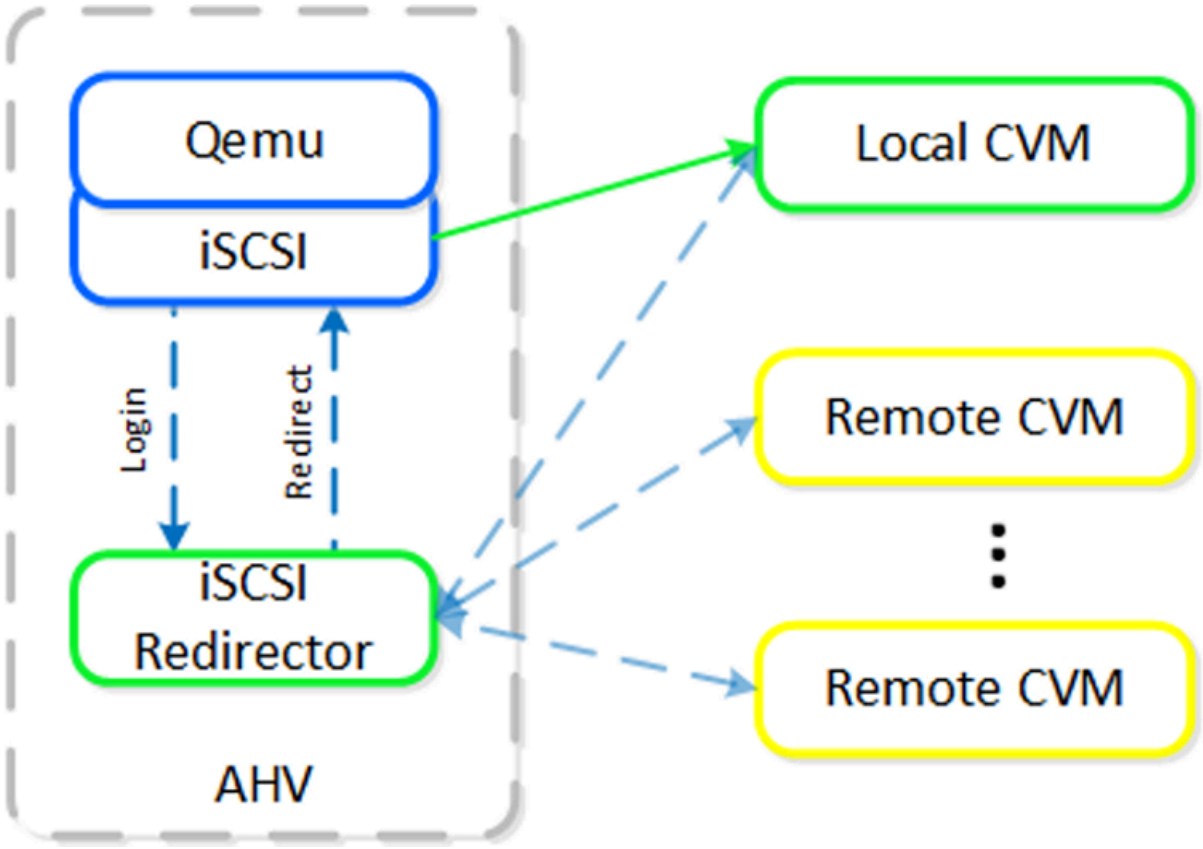


Figure 2: Storage Configuration

Virtual Networking

AHV uses Open vSwitch (OVS) for all VM networking. When you create a new AHV cluster, the system configures the CVM and management networking paths automatically. Administrators can easily create new VLAN-backed layer 2 networks through Prism. After the administrator creates a network, they can assign it to existing and new VMs.

For more information on the AHV implementation of OVS, see the AHV Administration Guide.

Along with streamlining VM network creation, AHV can manage DHCP addresses for each network that administrators create. This functionality allows administrators to configure address pools for each network that they can automatically assign to VMs.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3376

Nutanix Flow networking products offer advanced networking capabilities on AHV clusters. Nutanix Flow Virtual Networking brings virtual private cloud, virtual public cloud, and other advanced virtual networking constructs together to bridge traditional and cloud-native network models. With Nutanix Flow Network Security, you can create Zero Trust firewalls to segment and protect your users, apps, and data from cyber threats without disrupting your current infrastructure.

For more information on AHV networking, see the AHV Networking best practice guide.

Rolling Upgrades

Nutanix delivers a one-click upgrade process through Life Cycle Manager (LCM) for all software in the Nutanix platform, including AOS, AHV, firmware, and Nutanix Cluster Check (NCC). Upgrades are nondisruptive and allow the cluster to run continuously while nodes upgrade on a rolling basis in the background, ensuring always-on cluster operation during software maintenance. LCM manages the dependencies between products and versions and only shows upgrade options that are possible for the single or multiple upgrades selected. Nutanix qualifies firmware updates from the manufacturers of the hard or solid-state disk drives in the cluster and makes them available through the same upgrade process.

Host Maintenance Mode

Administrators can place AHV hosts in maintenance mode during upgrades and maintenance-related operations. Maintenance mode live-migrates all VMs running on the node to other nodes in the AHV cluster, and the CVM can safely shut down if required. After the maintenance process finishes all the steps for the node, it returns the CVM to service and synchronizes with other CVMs in the cluster. Maintenance mode enables graceful host suspension for routine cluster maintenance.

Scaling

The Nutanix solution's scale-out architecture enables incremental, predictable capacity and performance scaling in a Nutanix cluster running any hypervisor, including AHV. Administrators can start with as few as three nodes and scale out by easily adding nodes until they reach the desired cluster size or cluster maximum, adding more clusters as needed. The system automatically discovers new nodes and makes them available for use. To expand a cluster, select the discovered nodes you want to add and provide network configuration details. Use the same process to deploy new clusters in the same

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3377

location or at an edge site. With Prism, administrators can image or update new nodes to match the AHV version of their preexisting nodes for seamless node integration, no matter what version they installed originally.

Virtual Machine Management

VM management on AHV focuses on creating, updating, deleting, protecting, and monitoring VMs and their resources. These cluster services and features are all available through the highly available Prism interface.

VM Operations

Prism displays a list of all VMs in an AHV cluster along with configuration, resource usage, and performance details on a per-VM basis. Administrators can create VMs and perform many operations on selected VMs, including power state, reset, shut down, restart, snapshot and clone, migrate, category assignment, policy assignment, and launch a remote console. You can manage the entire life cycle of a VM and its policies that govern security and data protection from Prism.

Image Management

The image management service in AHV is a centralized repository that provides access to virtual media and disk images and the ability to import from external sources. With AHV's image management service, you can store VMs or virtual disks as images, which you can then use to create new VMs quickly from a known good base image. The image management service can store the virtual disk files you used to create the VMs or OS installation media as an .iso file that you can mount to provide a fresh OS install experience. Incorporated into Prism, the image management service can import and convert existing virtual disk formats, including .raw, .vhd, .vmdk, .vdi, and .qcow2. The previous virtual hardware settings don't constrain an imported virtual disk, so administrators have the flexibility to fully configure CPU, memory, virtual disks, and network settings when they provision VMs.

VM Templates

AHV has always had an image library, which captures data in a single vDisk so you can clone it easily but requires input from the admin to declare the CPU, memory, and network details. VM templates simplify this concept further. You create AHV VM

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3378

templates from existing VMs, so they inherit the attributes of the defining VM, such as the CPU, memory, and networking details. You can then configure the template to customize the guest OS on deployment and provide a Windows license key if needed. With VM templates, you can maintain multiple versions of a template, making it easy to apply updates like operating system and application patches without creating new templates. The template versioning function allows the administrator to declare which version of the template is active, allowing for a rollback to a previous version if needed or the ability to stage updates before making them available.

OVA Import and Export

You might need to use an Open Virtual Appliance (OVA) file in many situations, but the most common are when you deploy virtual appliances (typically from a non-Nutanix vendor) and when you move VMs to a different hypervisor. To help you accomplish these tasks, the OVA import-and-export process is available in Prism Central. Now you can export VMs on AHV to OVA format to keep on external storage, or import standard OVAs to get third-party VMs up and running fast based on this industry standard.

Acropolis Dynamic Scheduler

The Acropolis Dynamic Scheduler (ADS) is an automatic function enabled on every AHV cluster to avoid hot spots in cluster nodes. ADS continually monitors CPU, memory, and storage data points to make migration and initial placement decisions for VMs and Nutanix Volumes. Starting with existing statistical data for the cluster, ADS watches for anomalies, honors affinity controls, and only makes move decisions to avoid hot spots. Using machine learning, ADS can adjust move thresholds over time from their initial fixed values to achieve the greatest efficiency without sacrificing performance.

ADS tracks each node's CPU and memory usage. When a node's CPU allocation breaches its threshold (currently 85 percent), Nutanix migrates VMs or Nutanix Volumes off that host as needed to rebalance the workload.

ADS only uses migration when the system experiences contention. If the nodes experience skewed usage (for example, three nodes at 10 percent and one at 50 percent), ADS doesn't migrate the nodes, as migration offers minimal benefit if the system has enough resources.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3379

Intelligent VM Placement

When you create, restore, or recover VMs, the system assigns them to an AHV host in the cluster based on a recommendation from ADS. This VM placement process also takes into account the AHV cluster's high-availability configuration, so it doesn't violate any failover host or segment reservations. We explain these high-availability constructs in the Automated High Availability section.

Affinity and Antiaffinity

With affinity controls, you can govern where VMs run. AHV has two types of affinity controls:

- VM-host affinity strictly ties a VM to a host or group of hosts, so the VM only runs on that host or group. Affinity is particularly applicable for use cases that involve software licensing or VM appliances. In such cases, you often need to limit the number of hosts an application can run on or bind a VM appliance to a single host.
- Antiaffinity lets you declare that a given list of VMs can't run on the same hosts. Antiaffinity allows clustered VMs or VMs running a distributed application to run on different hosts, increasing the application's availability and resilience. To prefer VM availability over VM separation, the system overrides this type of rule when a cluster becomes constrained.

Live Migration

Live migration allows the system to move VMs from one host to another while the VM is turned on without workload interruption, regardless of whether the administrator or an automatic process initiates the movement. Live migrations occur regularly in the cluster nodes, triggered by maintenance operations, ADS workload balancing, node expansion, or administrator-driven requests.

You can also use live migration to migrate VMs to another physical cluster in the same location or in a different location to rebalance workloads, run maintenance operations, or avoid planned interruptions. For cross-cluster live migrations, we recommend a network with 5 ms of network latency and can support up to 40 ms of network latency.

Cross-Hypervisor Migration

Nutanix simplifies the process of migrating existing VMs between an ESXi cluster and an AHV cluster using built-in data protection capabilities. You can create one or more

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3380

protection domains on the source ESXi cluster and set the AHV cluster as the target remote cluster. Then, snapshot VMs on the source ESXi cluster and replicate them to the AHV cluster, where you can restore them and bring them online as AHV VMs.

Generation ID

Multiple applications use the Generation ID to access a VM identifier to validate if the VM was cloned or duplicated for licensing or functionality verification. Starting in AOS version 6.7, AHV creates a Generation ID for each VM you create, which applications running inside that VM can access. Applications can then make decisions on how they want to behave based on whether the correct Generation ID is present. This feature ensures that safeguards exist for cloning and rolling back to protect applications such as Windows domain controllers from the issues that accidental rollbacks or cloning can cause. Generation ID provides this information to a VM, allowing these restrictions to be tested and enforced by the app.

Advanced Processor Compatibility

Advanced Processor Compatibility (APC) can streamline upgrades and transition clusters to the latest generation of CPUs. With APC, clusters aren't limited by the lowest common denominator CPU. VMs can use APC to accurately identify and take advantage of the CPU features available to them, enabling improved migrations.

APC offers flexibility in multiple ways. Clusters can be leveled for consistent CPU presentation to guest VMs, which is the default behavior. You can also set a baseline CPU model on a per-VM basis for on-demand, cross-cluster live migrations to different hardware generations.

Automatic Cluster Selection

Many organizations have general-purpose environments, where a single Prism Central instance manages multiple clusters, and an administrator manages cluster resource use. The Automatic Cluster Selection feature intelligently determines the optimal cluster for VM deployment based on resource availability, host affinities, project specifications, and image distribution policies.

Automatic Cluster Selection helps you deliver a cloud-like experience to your users with minimal management overhead. It ensures that resources are automatically balanced across clusters as new VMs are deployed. It also saves valuable time and ensures that

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3381

workloads are evenly distributed for maximum performance and utilization across the infrastructure.

Automated High Availability

AOS offers virtual machine high availability (VMHA) to ensure VM availability in the event of a host or block outage. If a host fails, the VMs previously running on that host restart on healthy nodes throughout the cluster. Multiple high-availability configuration options are available to account for different cluster scenarios:

- By default, all AHV clusters provide best-effort high availability, even when you didn't configure the cluster for high availability. Best-effort high availability works without reserving any resources and doesn't enforce admission control, so the capacity might not be sufficient to start all the VMs from the failed host.
- You can also configure an AHV cluster for high availability with resource reservation to guarantee that the resources required to restart VMs are always available. To enable guaranteed high-availability reservations, select the **Enable HA Reservation** checkbox.

The Acropolis leader CVM restarts the VMs on the healthy hosts and tracks host health by monitoring connections to the libvirt on all cluster hosts. If the Acropolis leader becomes partitioned or isolated, or if it fails, the healthy portion of the cluster elects a new Acropolis leader from the Acropolis workers in the CVMs.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3382

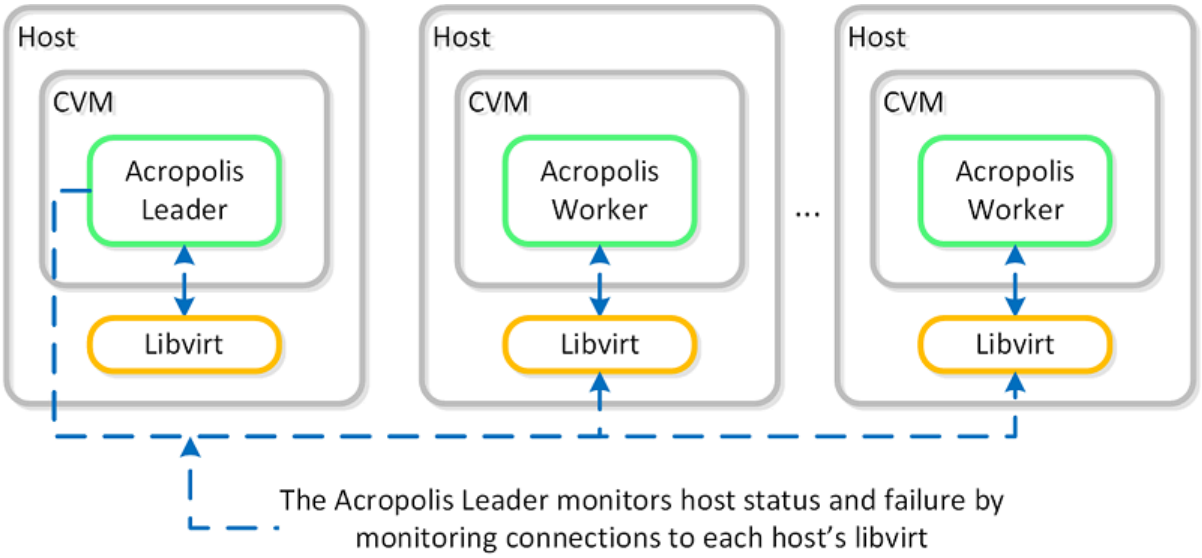


Figure 3: Acropolis Leader Monitoring

Storage-Only Nodes

With AHV, you can declare a node as never schedulable when joining it to a cluster. Commonly referred to as storage-only nodes, these never-schedulable nodes enable you to scale the storage performance and capacity of a cluster without expanding the compute resources. Because you configure this setting when you join a node to a cluster, you can't easily undo it without removing the node from the cluster and rejoining it as a regular node. This setting is most helpful when you need to scale storage resources for workloads licensed by compute resources, such as popular database services.

Compute-Only Nodes

Compute-only nodes enable you to achieve more control and value from restrictive licenses. Compute-only nodes don't have CVMs, so VMs use the CVMs on the hyperconverged infrastructure (HCI) or storage-only nodes to access disks. As a result, licensed cores on the compute-only nodes are only used for the application VMs. As with storage-only nodes, you must configure the compute-only status when you image the node with Foundation before adding it to the cluster.

Applications or databases that are licensed on a per–CPU core basis require you to license the entire node, which includes the cores that the CVM runs on. With compute-only nodes, you might see a much higher return on investment on your database

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3383

licenses because the CVM doesn't consume any compute resources from the node where the application or database runs.

AHV compute-only nodes support the following two types of deployments:

- AHV compute-only node + AHV HCI nodes
- AHV compute-only node + AHV storage-only nodes

  This deployment type is also called the Nutanix Optimized Database Solution (Nutanix Portal credentials required).

Converged Backup and Disaster Recovery

Nutanix clusters running any hypervisor have access to Nutanix data protection services, which safeguard VMs both locally and remotely for use cases ranging from basic file protection to recovery from a complete site outage. For more information on the built-in backup and disaster recovery capabilities in the Nutanix platform, see the Data Protection and Disaster Recovery tech note.

Metro Availability

Metro Availability creates a global file system namespace across Nutanix clusters and uses synchronous replication. Combining the Nutanix hyperconverged infrastructure with a continuous-availability solution limits downtime and preserves all data, even during a complete site failure. Metro Availability also enables workload mobility for disaster avoidance and planned maintenance scenarios. Administrators can use Metro Availability to extend hypervisor clustering technologies across datacenters. We call this type of configuration a stretched cluster, and it helps to minimize downtime during unplanned outages.

Metro Availability also supports VM migration across sites using technologies like live migration, which means that you have zero downtime while transitioning workloads between datacenters. Nutanix has built safeguards into the platform for everything from minor events, such as individual VM deletion, to major ones, including unplanned datacenter failure.

Nutanix AHV Backup APIs

AHV publishes a rich set of APIs to support external backup vendors. The AHV backup APIs use changed region tracking to allow backup vendors to back up only the data

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3384

that has changed since the last backup job for each VM. Changed region tracking also allows backup jobs to skip reading zeros, further reducing backup times and bandwidth consumed.

Nutanix backup APIs allow backup vendors that build integration to perform full, incremental, and differential backups. Changed region tracking is always on in AHV clusters; you don't need to enable it on each VM. Backups can be either crash-consistent or application-consistent.

Another feature available in the backup APIs is instant recovery, which enables supported backup vendors to instantly recover a VM or vDisk typically on their backup appliance and allow immediate access to its contents. You can use and delete the VM or vDisk or migrate it to a Nutanix volume for permanent storage.

Nutanix Prism Analytics

Nutanix Prism offers in-depth analytics for every element in the infrastructure stack, including hardware, storage, and VMs. Administrators can use Prism views to monitor these infrastructure stack components, and they can use the Analysis view to get an integrated assessment of cluster resources or to see specific metrics on a given element.

Prism makes detailed VM data available, grouping it into the following categories:

- VM Performance: Multiple charts with CPU- and storage-based reports around resource usage and performance
- Virtual Disks: In-depth data points that focus on I/O types, I/O metrics, read source, cache hits, working set size, and latency on a per–virtual disk level
- VM NICs: vNIC configuration summary for a VM
- VM Snapshots: A list of all snapshots for a VM with the ability to clone or restore from the snapshot or to delete the snapshot
- VM Tasks: A time-based list of all operational actions performed against the selected VM, including task summary, percent complete, start time, duration, and status
- Console: A pop-up console session or an inline console session for a VM

The Storage tab provides a direct view of the storage fabric running on an AHV cluster. Administrators can look at detailed storage configurations, capacity usage over time,

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3385

space efficiency, and performance, as well as a list of alerts and events related to storage.

The Hardware tab gives you a direct view of the Nutanix blocks and nodes that make up a cluster. These reports are available in diagram and table format for easy consumption.

The Prism Analysis tab allows administrators to explore and understand what is going on in their clusters quickly and to identify steps for remediation as required. You can create custom interactive charts using hundreds of metrics available for elements such as hosts, disks, storage pools, storage containers, VMs, protection domains, remote sites, replication links, clusters, and virtual disks, then correlate trends in the charts with alerts and events in the system. You can also choose specific metrics and elements and set a desired time frame when building reports so that you can focus precisely on the data you're looking for.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3386

4. Performance and Scale

The Nutanix platform optimizes performance at both the AOS and hypervisor levels. The CVMs that represent the control and data planes contain the AOS optimizations that benefit all supported hypervisors. Although we built AHV on an open-source KVM foundation, we added a significant amount of innovation to make AHV a unique Nutanix offering. The following sections outline a few of the innovations in AHV focused on performance.

AHV Turbo

AHV Turbo represents significant advances to the data path in AHV over the core KVM source code foundation. In the core KVM code, all I/O from a VM flows through the hosted VM monitor, QEMU. While this architecture can achieve impressive performance, some application workloads require more. AHV Turbo provides a new I/O path that bypasses QEMU and services storage I/O requests, which decreases CPU usage and increases the amount of storage I/O available to VMs.

When using QEMU, all I/O travels through a single queue, which can affect performance. The AHV Turbo design introduces a multiqueue approach to allow data to flow from a VM to storage, resulting in much higher I/O capacity. The storage queues scale out automatically to match the number of vCPUs configured for a given VM, making even better performance possible as the workload scales up.

While these improvements demonstrate immediate benefits, they also prepare AHV for future technologies such as NVMe and persistent memory advances that offer dramatically increased I/O capabilities with lower latencies.

vNUMA

Modern Intel server architectures assign memory banks to specific CPU sockets. In this design, one of the memory banks in a server is local to each CPU, so you see the highest level of performance when accessing memory locally, as opposed to accessing it remotely from a different memory bank. Each CPU and memory pair is a NUMA node.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3387

vNUMA allows a VM's architecture to mirror the NUMA architecture of the underlying physical host.

vNUMA doesn't affect most workloads, but it can be beneficial to large VMs configured with more vCPUs than available physical cores in a single CPU socket. In these scenarios, configure vNUMA nodes to use local memory access efficiently for each CPU to achieve the highest performance results.

Remote Direct Memory Access

Remote direct memory access (RDMA) enables a node to write to the memory of a remote node by granting a VM running in the user space access to a NIC directly. This approach avoids TCP and kernel overhead, resulting in CPU savings and performance gains. AOS RDMA support is reserved for inter-CVM communications and uses the standard RDMA over Converged Ethernet (RoCEv2) protocol on systems configured with RoCE-capable NICs.

iSCSI Extensions for RDMA

iSCSI Extensions for RDMA (iSER) is an extension of iSCSI that uses RDMA direct data placement technology to eliminate copies in the data path. The system uses the CPU resources efficiently by taking advantage of Mellanox NICs for offloading functions and reduces latency between the AHV host and CVM I/O transfer. iSER provides the following key benefits:

- Enhances the I/O flow performance between AHV host and CVM: iSER bypasses both the AHV host and CVM kernel spaces and enables you to achieve low latency in the I/O data transfer as the data is sent and received between AHV host and CVM without involving the TCP software stack. iSER enables you to achieve a high bandwidth in the I/O data transfer as it removes the unwanted context switches and system calls between the AHV host and CVM.
- Saves platform resources: iSER reduces CPU utilization because an application can read remote memory without any intervention from the remote processor.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3388

Memory Overcommit

One of the central benefits of virtualization is the ability to overcommit compute resources, making it possible to provision VMs with more CPUs than are physically present on the server host. Most workloads don't need 100 percent of their assigned CPU all the time, and the hypervisor can dynamically allocate CPU cycles to workloads that need them.

You can also overcommit memory. The VMs on the host might not use all their allocated memory, and the hypervisor can share that unused memory with other workloads. Memory overcommit enables administrators to provision more VMs per host by combining the unused memory and allocating it to VMs that need it.

AOS 6.1 offers memory overcommit to AHV for environments like test and development that need additional memory and VM density. You define overcommit on a per-VM basis, so you control whether to share memory between all VMs on a cluster or just a subset.

Virtual Trusted Platform Module and Secure Boot

Nutanix AHV supports host secure boot and provides a virtual Trusted Platform Module (vTPM) for VMs. A Trusted Platform Module (TPM) is a piece of hardware in a server or computer that provides secure storage for keys or credentials. A vTPM is an integrated feature in the hypervisor that provides the same functionality but is implemented as software for VMs to use. Windows 11 is the primary reason most organizations use a vTPM in their environments, as it's required for running that operating system virtually. Other Windows features such as BitLocker and Credential Guard also use vTPM.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3389

5. Graphics Processing Unit Support

A graphics processing unit (GPU) is the hardware or software that displays graphical content to end users. In laptops and desktops, a GPU is either a physical card or built directly into the CPU hardware, while GPU functions in the virtual world historically were software-driven and consumed additional CPU cycles. With modern operating systems, applications, and 3D tools, more organizations find themselves needing a hardware GPU. You can install physical GPU cards in qualified hosts and present them to guest VMs using passthrough or vGPU mode. Nutanix AHV allows you to assign up to 16 vGPU profiles to a single VM or a single GPU using passthrough.

GPU Passthrough

The GPU cards deployed in server nodes for virtualized use cases typically combine multiple GPUs in a single Peripheral Component Interconnect (PCI) card. AHV can pass a GPU through to a VM, allowing the VM to own that physical device in a 1:1 relationship. Configuring nodes with one or more GPU cards that attach multiple GPUs to a larger number of VMs allows you to consolidate applications and users on each node. With passthrough, you can also use GPUs for offloading computational workloads—a more specialized situation than the typical graphical use cases.

AHV currently supports NVIDIA GRID cards for GPU passthrough. For the current list of supported devices, see the AHV Administration Guide.

Nutanix LCM doesn't support live migration for VMs configured with GPU passthrough. For more information, see the limitations in the GPU Passthrough for Guest VMs section of the AHV Administration Guide.

vGPU

While passthrough is a method that works well for fewer VMs that require more GPU resources, workloads such as VDI often have different requirements. VDI workloads typically have more VMs that need varying GPU resources based on application types and usage.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3390

Today's NVIDIA GRID GPU cards contain 1–4 GPU on each physical PCI card, and each physical host can support installing one or two cards. This capability allows up to 8 GPU in each node to meet the density requirements of VDI workloads. For maximum flexibility, vGPU mode allows you to slice each GPU into smaller segments that you can virtually assign to VMs.

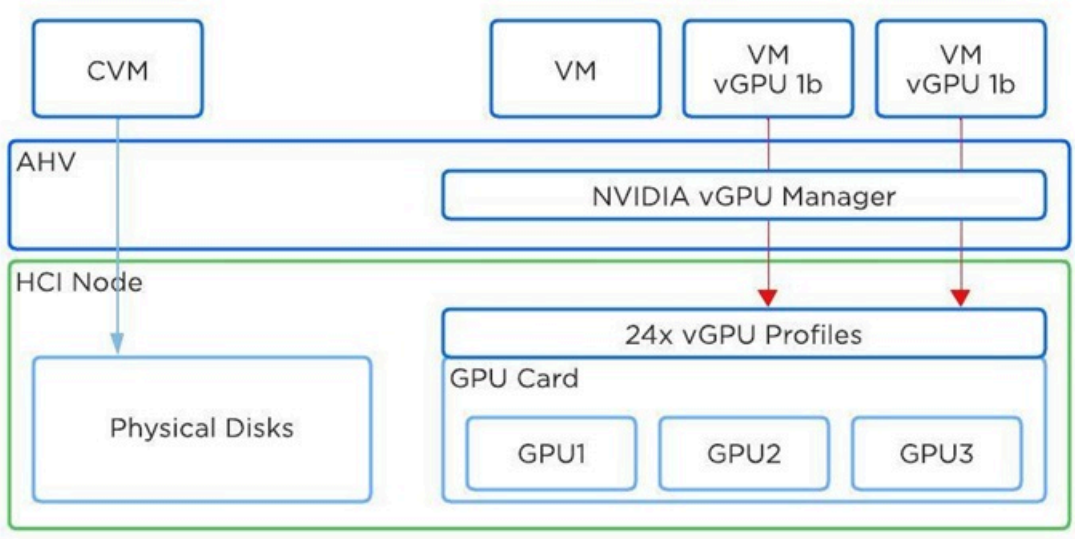


Figure 4: HCI Node with One PCI Card and 3 GPU with vGPU Enabled

vGPU profiles allow you to assign different levels of resources to VMs, so each VM can use a defined maximum number of displays and quality of resolution. Working within these parameters lets you choose the correct GPU profile to meet your application requirements, and when you also know the type and number of GPU cards in your deployment, you can accurately describe the maximum density possible per host.

In some rare use cases, you might need additional GPU resources for demanding workloads. With AHV, you can assign multiple vGPU profiles to a single VM to fulfill the requirements of these workloads.

AHV currently supports NVIDIA GRID cards for vGPU. For the current list of supported devices, see the NVIDIA Drivers section of the Compatibility and Interoperability Matrix.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3391

vGPU Live Migration

If you want maintenance operations like upgrades and failure handling to be as efficient as possible, you need the ability to migrate your VMs. With AHV, you can live-migrate VMs with vGPU assignments. For more information on live migration with your combination of GPU and NVIDIA host driver, see the NVIDIA GRID Host Driver for AHV Installation Guide or contact Nutanix support.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3392

6. Migration

The most common migration method in virtualized environments involves moving an existing operating system and its applications without modification. AHV supports a wide range of operating systems that you can migrate from either physical or virtual environments. The following sections present a few of the primary methods of migrating workloads to AHV.

For more information, see Migrating VMs to Nutanix AHV.

Nutanix Move

Nutanix Move quickly and easily transfers VMs from ESXi, Hyper-V, and public cloud environments (including AWS and Azure) to Nutanix AHV, keeping VM data unmodified and intact. Nutanix Move is a VM appliance, typically hosted on the target AHV cluster. After you deploy this free product as a VM in your AHV environment, you can use its HTML5-based interface to manage it.

With Nutanix Move, you can create migration groups that consist of a single VM or large groups. This migration group construct allows you to schedule and control data replication and to cut over the entire group, specific VMs, or a single VM to the target cluster. The source data remains intact, but the VMs are shut down and disconnected until it's safe to clean up.

Cluster Conversion

Sometimes, you might need to convert a cluster rather than migrate to a new cluster; for example, if you have a single Nutanix cluster that is deployed at a site that you need to convert to AHV. The cluster conversion process allows you to convert a Nutanix cluster running VMware ESXi to AHV in place with minimal downtime.

The process is a rolling cluster conversion similar to the upgrade process except that the node's hypervisor under maintenance is converted to AHV. The automated process places a node into maintenance and live-migrates all VMs on that node to other nodes. After the hypervisor is fully evacuated and in maintenance mode, the process converts it

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3393

to AHV. Once AHV is running on that node, the process shuts down the VMs that were running on it, converts them into AHV format, and then turns them on in the AHV node. Because you changed the VM format, each VM experiences a brief downtime. Once the process converts the first node, it moves on to the next node and rolls through the cluster until each node is converted. When the process finishes, the cluster is fully converted to AHV, and you can roll it back to ESXi if you need to.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3394

7. Security

The fully integrated Nutanix infrastructure stack reduces security risks associated with legacy solutions that involve many vendors with a narrow, fragmented view of security. Nutanix designed AHV to be an integral component of the converged infrastructure stack rather than a general-purpose hypervisor. Consequently, to reduce the security surface area, we turned off many of the services that we don't use or that AHV obviates. For example, with AHV, you don't need to use Virtual Network Computing to console VMs, because Prism offers a more robust and secure service.

Security Development Life Cycle

To maintain agile and comprehensive security, Nutanix developed its own Security Development Life Cycle (SecDL) that addresses security at every step of the development process instead of applying it at the end. SecDL integrates security features into the software development process, including automated security testing during development and threat modeling to assess and mitigate customer risk from code changes.

Security Baseline and Self-Healing

Nutanix developed custom Security Technical Implementation Guides (STIGs)—security tools based on well-established National Institute of Standards and Technology (NIST) standards—that administrators can apply to multiple baseline requirements for the United States Department of Defense (DoD) and PCI-DSS. Unlike general-purpose STIGs that make blanket security recommendations, Nutanix STIGs are specific to the Nutanix platform and therefore more effective. Encoded in a machine-readable format, Nutanix STIGs enable automated validation, ongoing monitoring, and self-remediation, reducing the time required to verify security compliance from weeks or months to days.

For more details, see the Information Security tech note.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3395

Prism Audits

The audits log in Prism provides a comprehensive list of all actions taken by administrators and users against AHV resources. You can easily locate details on who took an action (such as VM creation, deletion, and updates) and when.

Credential Guard

Credential Guard is an additional virtualization-based security layer for the Local Security Authority Subsystem Service (LSASS) process in Windows that stores credentials for New Technology LAN Manager (NTLM) and Kerberos. Credential Guard isolates the LSASS process in a virtual container that can't be accessed by users and creates a proxy process to communicate with it, protecting the system from further lateral incursion. Nutanix AHV supports Credential Guard through our vTPM.

Nutanix Data Lens

If you host unstructured data on AHV using Nutanix Unified Storage (NUS)—including Nutanix Files and Nutanix Objects—Nutanix Data Lens offers ransomware resilience and data analytics for unstructured data on the Nutanix Cloud Platform. This service offers global data visibility to proactively assess and mitigate data security risks by identifying anomalous activity, auditing user behavior, and adhering to compliance requirements while enabling efficient data life-cycle management. Nutanix Data Lens centralizes information from all your clusters connected to Nutanix Pulse across various datacenter locations. Using cloud resources eliminates scaling constraints, allowing you to analyze an unlimited number of files and objects and unlimited amounts of data.

Nutanix Flow Virtual Networking

Nutanix Flow Virtual Networking is a software-defined network virtualization solution that provides overlay capabilities for on-premises AHV clusters. It uses networking features like Virtual Private Cloud (VPC) and Virtual Private Network (VPN) to support flexible, app-driven networking that focuses on VMs and applications instead of virtual LANs and network addresses. Flow Virtual Networking provides the following benefits:

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3396

- A simplified, Prism Central–based workflow that deploys the application-driven network virtualization features
- A secure multi-tenancy solution that enables per-tenant isolation using VPC-based network segmentation and namespace isolation
- A secure, VPN-based connectivity solution for multiple sites, with automated VPN bundle upgrades
- NAT-based secure egress to external networks, with IP address retention and policy-based routing
- Self-service networking using REST APIs or Nutanix Cloud Manager Self-service blueprints and projects
- Stretched layer 2 networking for more effective disaster recovery

Nutanix Flow Network Security

Nutanix Flow Network Security protects against new threats like ransomware designed to spread laterally from one system to another in the same protected datacenter. Because perimeter-based firewalls traditionally only protect the environment from external threats, it can be difficult to repurpose them to protect internal traffic. The problem is compounded by virtualized workloads changing their network configurations and hosts as they start, stop, and migrate frequently. Flow Network Security applies security rules between all applications and VMs in the datacenter, adding internal protection behind your perimeter firewall.

Flow Network Security includes a policy-driven security framework that inspects traffic in the datacenter. Security policies are applied to categories (a logical grouping of VMs) and not to the VMs themselves. Therefore, it doesn't matter how many VMs you have in a category; traffic associated with that category is secured without administrative intervention even at scale.

The framework uses a workload-centric approach instead of a network-centric approach, so it can scrutinize traffic to and from VMs in a datacenter regardless of changes to their network configurations or their locations in the datacenter. This approach also enables the virtualization team to implement these security policies without having to rely on network security teams.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3397

Prism Central works with Flow Network Security to offer a visualization-based approach to configuring security policies and monitoring the traffic a policy applies to.

Flow Network Security is complemented by the SaaS-based Nutanix Security Central to provide threat detection, compliance, and security planning using machine learning analysis of on-prem configuration and network traffic metadata.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3398

8. Conclusion

The Nutanix Cloud Platform embodies a radically new approach to infrastructure—one that simplifies every step of the life cycle from buying and deploying to managing, scaling, and supporting. The Nutanix solution's web-scale technologies and architecture let you run any workload at any scale. With Nutanix AOS and Nutanix Prism, administrators enjoy powerful virtualization capabilities fully integrated into the converged infrastructure stack and managed from a single pane of glass.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3399

9. References

1. AHV Administration Guide
2. Nutanix AHV best practice guide
3. Nutanix AHV Networking best practice guide
4. Data Protection and Disaster Recovery tech note
5. Information Security tech note

© 2024 Nutanix, Inc. All rights reserved

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3400

About Nutanix

Nutanix offers a single platform to run all your apps and data across multiple clouds while simplifying operations and reducing complexity. Trusted by companies worldwide, Nutanix powers hybrid multicloud environments efficiently and cost effectively. This enables companies to focus on successful business outcomes and new innovations. Learn more at Nutanix.com.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3401

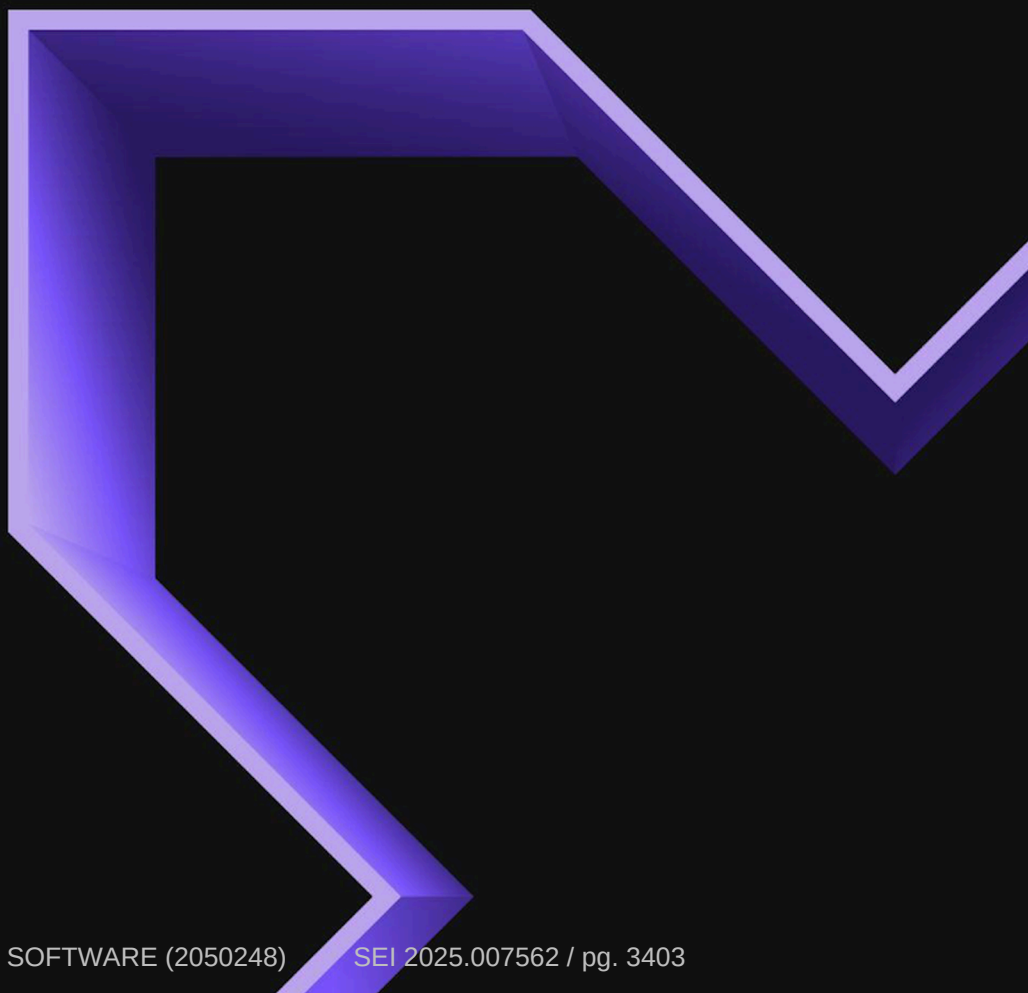
List of Figures

Figure 1: AHV Components..... 8
Figure 2: Storage Configuration..... 10
Figure 3: Acropolis Leader Monitoring..... 17
Figure 4: HCI Node with One PCI Card and 3 GPU with vGPU Enabled..... 25

v2.5 | January 2025 | TN-2042

SOLUTIONS DOCUMENT

Nutanix Prism



NUTANIX

Legal

© 2025 Nutanix, Inc. All rights reserved. Nutanix, the Enterprise Cloud Platform, the Nutanix logo and the other Nutanix products, features, and/or programs mentioned herein are registered trademarks or trademarks of Nutanix, Inc. in the United States and other countries. All other brand and product names mentioned herein are for identification purposes only and are the property of their respective holder(s), and Nutanix may not be associated with, or sponsored or endorsed by such holder(s). This document is provided for informational purposes only and is presented "as is" with no warranties of any kind, whether implied, statutory or otherwise.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

Contents

1. Executive Summary..... 5

2. Nutanix Prism Overview.....7

Prism Element Distributed Architecture.....7
Prism Central Architecture.....8
Nutanix Prism Interaction with Other Services.....9

3. Infrastructure Management.....10

Cluster Management.....10
Life Cycle Manager One-Click Upgrades.....11
Storage Management.....12
Virtual Machine Management.....13
Prism Central Entity Explorer.....14
Entity Tagging.....17
Nutanix Prism Search.....17
Networking.....18
Data Protection.....18
User Management and Authentication.....19
Tasks.....19
Localization.....20

4. Operational Insights..... 21

Alerts.....21
User-Created Alerts.....21
Alert-Driven Root Cause Analysis.....22
Analytics.....22
Analysis.....24
VM I/O Metrics.....25
Network Visualization.....25

5. Prism API..... 27

6. Conclusion.....28

About Nutanix.....29

List of Figures.....30

1. Executive Summary

The Nutanix Cloud Platform natively converges compute, storage, virtualization, systems management, and operations management into a turnkey platform that you can deploy in minutes to run any application out of the box. Nutanix offers powerful virtualization capabilities, including core virtual machine (VM) operations, live migration, VM high availability, and virtual network management as fully integrated features of the infrastructure stack rather than as standalone products that require separate deployment and management. The Nutanix solution has two primary product families: Nutanix AOS and Nutanix Prism. AOS is the distributed data plane that provides storage, virtualization, backup, and disaster recovery services, and Nutanix Prism is the centralized management solution for Nutanix environments.

This document describes how to use Nutanix Prism to manage, monitor, and scale Nutanix clusters. It explains and highlights simplified cluster administration methods and operational insights.

Table: Document Version History

Version Number	Published	Notes
1.0	March 2016	Original publication.
1.1	June 2016	Added a section on localization for AOS 4.7.
1.2	December 2016	Updated for AOS 5.0.
1.3	January 2018	Updated for AOS 5.5.
2.0	February 2019	Updated for AOS 5.10.
2.1	February 2020	Annual update.
2.2	January 2022	Updated the LCM One-Click Upgrades section.
2.3	October 2022	Updated product naming in the Prism Central Architecture section.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3407

Version Number	Published	Notes
2.4	December 2023	Updated branding and images throughout.
2.5	January 2025	Updated the LCM One-Click Upgrades, Cluster Management, and Storage Management sections.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3408

2. Nutanix Prism Overview

Nutanix Prism provides central access to configure, monitor, and manage virtual environments. Nutanix Prism uses machine learning to mine large volumes of system data easily and quickly, generating actionable insights for optimizing all aspects of virtual infrastructure management. Included as a part of every Nutanix deployment, Nutanix Prism has two core components:

Prism Element

Prism Element is a service built into the platform for every deployed Nutanix cluster. Prism Element fully configures, manages, and monitors Nutanix clusters running any hypervisor.

Prism Central

Because Prism Element manages only the cluster that it's part of, each deployed Nutanix cluster has a unique Prism Element instance for management. With Prism Central, you can manage different clusters across separate physical locations on one screen and gain an organizational view into a distributed Nutanix environment.

Prism Element Distributed Architecture

Prism Element is a distributed service in every Nutanix cluster and provides users access to the distributed system. Prism Element runs on every node in the cluster, and like other components, it elects a leader. The system forwards all requests from followers to the leader. This configuration allows you to access Prism Element using the cluster IP address or any Controller VM (CVM) IP address. If the leader fails, the system elects a new leader.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3409

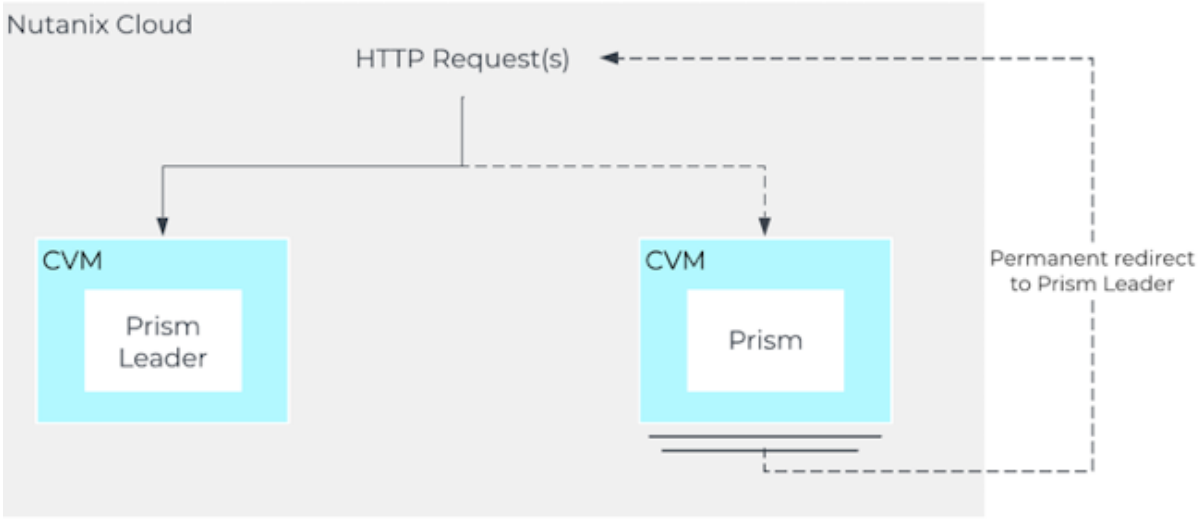


Figure 1: Conceptual View of Prism Element Services and HTTP Request Handling

Prism Central Architecture

You can deploy Prism Central in a VM (Prism Central VM) or in a scale-out cluster of VMs (Prism Central instance) manually, import a VM template, or install Prism Central directly from Prism Element. A Prism Central VM can run in a VM of any size; the only difference is the amount of CPU and memory available to the Prism Central VM for VM management. You can deploy a Prism Central instance initially as a scale-out cluster or, if you're running it as a single VM, scale it out from Prism Element. The design decisions involved in using this architecture are simpler than legacy solutions because you need to answer only two questions before deploying:

- How many VMs do you need to manage?
- Do you want high availability?

Prism Central allows you to scale an instance up and out to address changing conditions. A single Prism Central VM can support 2,500–12,500 VMs. The following diagram shows the two architectures. In this example, the scaled-out Prism Central instance can support 5,000–25,000 VMs.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3410

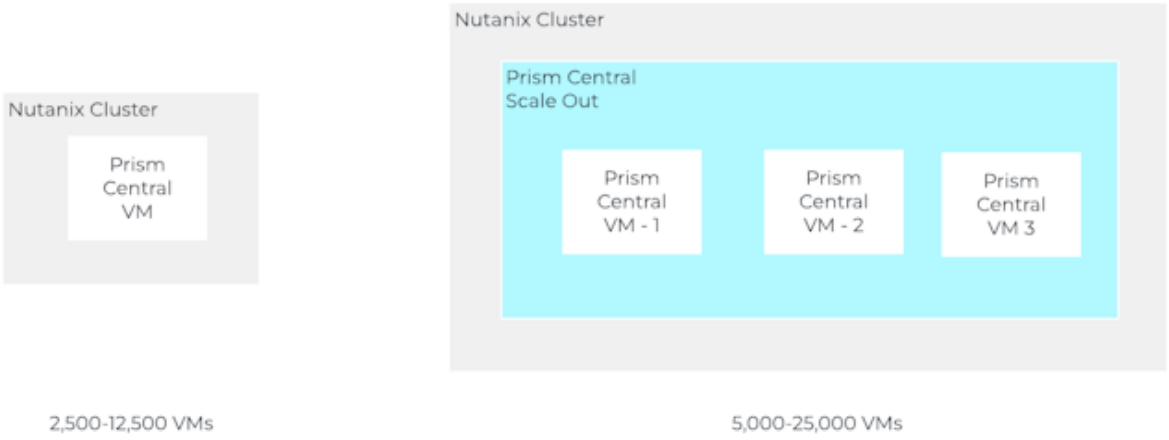


Figure 2: Prism Central Architectures

With the extensible architecture, you can add features and products from the Prism Central application, such as Nutanix Cloud Manager and Flow Virtual Networking. These additional features operate in a single Prism Central VM or clustered Prism Central instance and don’t require you to design or deploy separate products. This streamlined strategy creates a simplified experience throughout a project's phases and includes one-click upgrades so that users can benefit from regular innovations.

Nutanix Prism Interaction with Other Services

Nutanix Prism is the user interface for the Nutanix solution, and it must communicate with and collect data from each of the underlying services. Nutanix Prism interacts with a distributed configuration management database for cluster configuration data and with a distributed NoSQL key-value store for statistics to present to the user. It also liaises with the hypervisor hosts for VM status, configuration, performance data, and related information.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3411

3. Infrastructure Management

Historically, managing a datacenter’s infrastructure components consumed a significant amount of time. Through software, Nutanix removed most of these time-consuming tasks and simplified the rest to a few mouse clicks.

Nutanix Prism provides detailed data in an accessible and intuitive layout. In Nutanix Prism, you first see a home screen that summarizes your cluster hardware and software, performance reports, and whether you need to investigate any events or alerts. The home screen provides a simple overview of your environment’s health and performance.

When you need to investigate further or make changes, you can dive deeper with focused views for each major infrastructure component. Each focused view provides the same look into its specific area that the home screen offers for the entire environment.

Cluster Management

Prism Element provides a single control plane for a cluster's typical management and maintenance tasks, including configuration, expansion, performance, and cluster updates. The first view is a cluster summary that shows a count of blocks and hosts and their model numbers, how many hosts are part of the cluster, and the number of newly discovered hosts. The view shows the cluster's total available compute capacity in terms of the amount of CPU in GHz and the total usable memory. Nutanix Prism presents multiple lists of the top-performing hosts for I/O, bandwidth, and memory and CPU usage.

For deeper insights into the hosts in the cluster, the table-based view offers a detailed look into hardware, host configuration, and resource consumption. This perspective helps you understand the current state of a cluster and provides a starting place when looking for the root cause of an issue. The same table offers comparable data for all the cluster disks so that you can see usage and performance statistics for each drive.

The Nutanix platform is built on a scale-out architecture, and Nutanix Prism lets you scale clusters with minimal effort by discovering newly cabled and network-attached

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3412

nodes. When the system discovers new nodes, the nodes are available for you to add to an existing cluster or to create a new one.

In Nutanix Prism, the Expand Cluster feature offers a simple process for adding these new nodes to a cluster. When you expand the cluster, the interface presents any available new nodes and allows you to select which ones to prepare and add to the existing cluster. If necessary, the system images new nodes with the correct hypervisor to match the other nodes in the cluster. This process allows you to add one or multiple nodes without changing the workflow.

Beginning with Prism Central 2024.3, you can create cluster profiles and apply them to configure system settings across multiple clusters with a single click. These profiles include configurations for NTP servers, name servers, SNMP, SMTP servers, syslog servers, file system allowlists, and Nutanix Pulse.

Life Cycle Manager One-Click Upgrades

Historically, updating IT infrastructure was a tedious and time-consuming activity typically reserved for correcting a serious bug or maintaining compliance for support reasons. Nutanix Prism solves update reluctance by offering Life Cycle Manager (LCM) one-click upgrades for each product in a cluster. The LCM one-click upgrade process downloads the next version or allows you to upload manually.

Each upgrade process is a nondisruptive workflow that follows a rolling upgrade flow through the clusters on a node-by-node basis. Before beginning the upgrade, the system performs a series of preupgrade and health checks on the cluster that it must pass before proceeding. After every node in the cluster upgrades, a final health check runs before finalizing the process.

LCM upgrades are available for AOS, which includes Nutanix Prism and Nutanix storage. LCM also updates the hypervisor version, host firmware, Foundation, Nutanix Files, and Nutanix Cluster Check. You can find all these upgrades in Nutanix Prism and start each with a mouse click.

Access LCM from the Prism Central Admin Center. Beginning with AOS 7.0 and Prism Central 2024.3, go to the Connected Clusters page to view the inventory of clusters registered to Prism Central and perform updates. You can also update LCM settings from this same interface.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3413

Storage Management

Nutanix clusters provide storage services that avoid legacy headaches and relying on logical unit numbers. Storage management views in Prism Element look and feel similar to the cluster management views previously described. The storage-focused view shows the storage environment, providing important performance charts, data reduction metrics, capacity summaries, and important alerts and warnings.

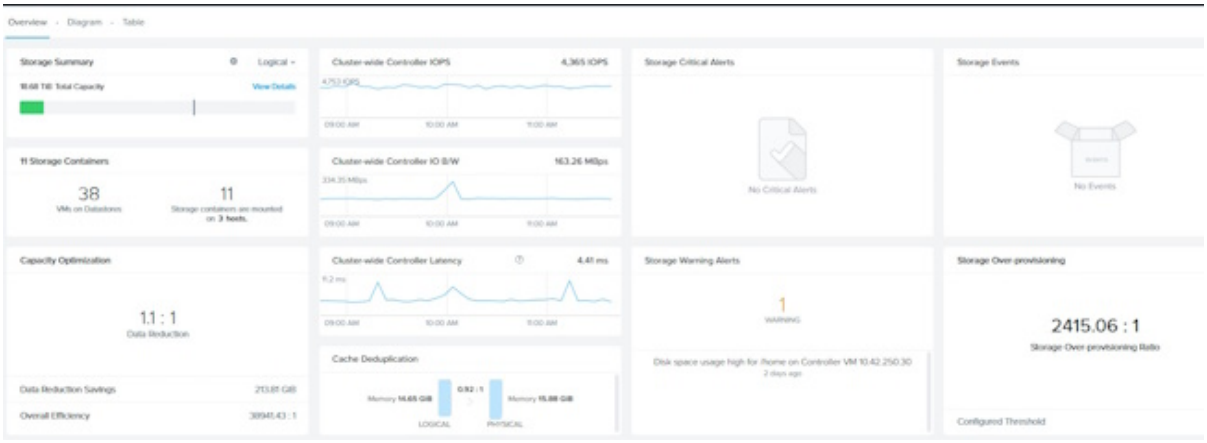


Figure 3: Prism Element Storage Management View

You can use the detailed table view for more details about storage services. This view shows three primary areas of the storage constructs in a cluster: volume groups, containers, and storage pools. The table view displays the configuration settings for each container, capacity metrics, and several performance charts.

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3414

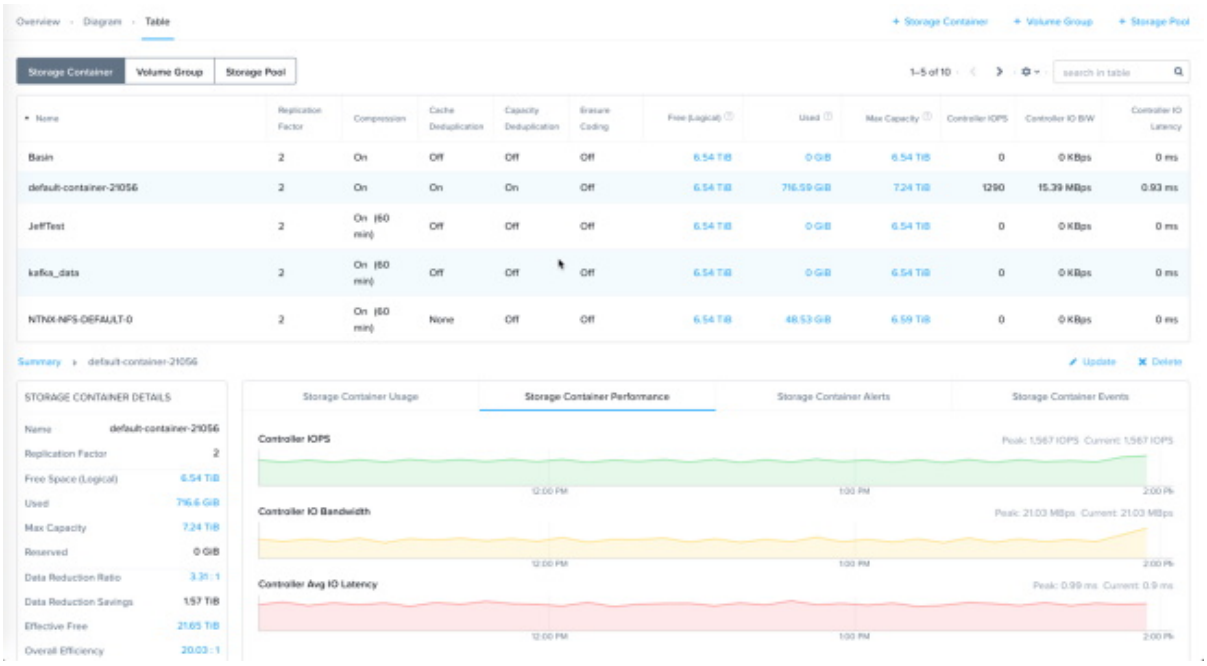


Figure 4: Prism Element Storage Management Table View

Creating a new datastore container for a hypervisor and VMs to consume is simple. Use the blue links in the upper-right corner of each storage management view in Prism Element to create or add items. You can also create objects in Prism Element from the **Settings** menu. Provide a name for the container and check the data reduction settings to create the container.

Storage policies in Prism Central centrally manage storage attributes such as replication factor, encryption, compression, and quality of storage for entities like VMs and volume groups. A single storage policy can control the attributes of multiple entities linked to different categories.

Virtual Machine Management

For more visibility into your VMs, Prism Element delivers a VM-focused management view. The VM view provides the same kind of overview summary that the cluster and storage management views offer. The VM summary delivers VM counts and power status. Highlighted CPU and memory usage statistics focus on provisioned amounts versus reserved amounts. You can also see the top consumers for IOPS, latency,

© 2025 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3415

memory usage, and CPU usage, helping you identify which VMs use the most resources and detect any outliers.

Similar to the other sections, the VM-focused view in Prism Element also offers a table-based layout for VM management that provides more VM-focused data points.

This VM-focused view compares the configured CPU and memory settings versus the actual amounts of CPU and memory used. You can also access storage metrics for read versus write IOPS, combined IOPS, storage bandwidth, and latency. Prism Element tracks each of these data points on a per-VM basis to give a quick overview and locate potential issues faster.

When your system combines Nutanix Prism with Nutanix AHV or VMware ESXi, you can manage all VMs using Nutanix Prism. This single interface covers create, read, update, and delete (CRUD) operations in a VM’s life cycle.

Along with VM life cycle management, Prism Element delivers simple processes for taking snapshots, adding resources to VMs, providing console access, and operating vNIC, vDisk, and power controls. These standard VM-based operations are available through the VM table view in Prism Element when you select a VM.

Prism Central Entity Explorer

Prism Central is a single management point for multicluster and multisite Nutanix environments. In multicluster environments, you need easy access to summary information. The entity explorer in the explore view in Prism Central provides this overview.

Prism Central's analysis features can report on several entities in a Nutanix cluster. The entity explorer focuses on a subset of entities that provides access to configuration and inventory data:

- Virtual machines
- Nutanix clusters
- Hosts
- Disks
- Containers

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3416

When you select an entity to view, Prism Central immediately returns a list of all the items in the selected entity. If you select VMs, for example, you see a list of every VM on each cluster a Prism Central instance manages. You can view the entity list in one of three formats: a list view, tile view, or circle view. Each view provides a unique look into the data provided.

When viewing a set of entities, such as VMs, Prism Central presents two data options. The first option delivers a general data set, which in this example includes common VM-related details such as the host and cluster the VM is running on, IP address, and hypervisor version. The second option is a performance-based view; in this example, this view reports VM memory usage and several other vital storage performance metrics. You can set the table that contains the selected data points to display 10–60 rows in increments of 10.

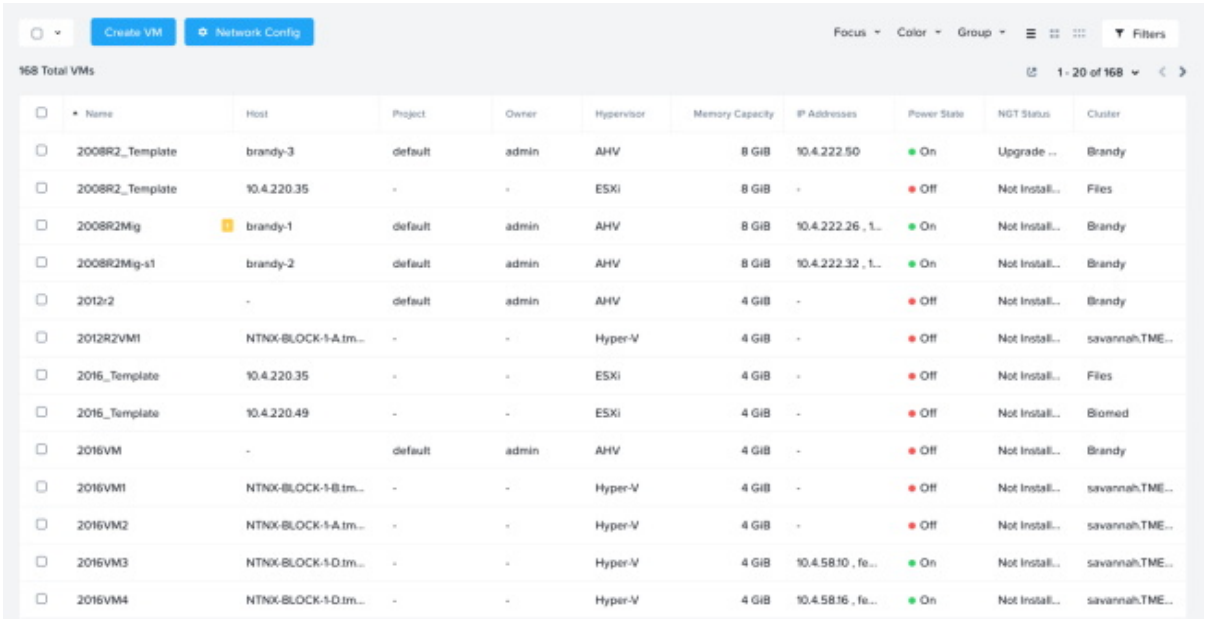


Figure 5: Entity Explorer in Prism Central

In the explore view, several ways to group and filter entity data points make the information easier to consume. When viewing VMs, you can apply a color to each entity to show the vCPU count, VM health, or power state. The group function displays VMs that you can group by cluster, hypervisor, power state, health, or vCPU count. After you filter the data, choose multiple items by selecting the checkbox for each item or by pressing the Shift key and clicking the first and last items to select a contiguous range.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3417

In addition to the general and performance-focused views available in the entity browser, you can create custom views. Select the **Custom** option from the Focus dropdown menu to create new custom views. This option prompts you to name the new custom view and select from a list of columns that provide a variety of data points. You can create multiple custom views, including custom views for any of the five entities available in the entity browser, with each providing a unique set of data points relevant to the selected entity.

When you select VMs running on AHV in the entity explorer, you can run VM actions on a single VM or a group of selected VMs. This capability implements traditional VM management for distributed environments from a centralized point. The available actions are as follows:

- Power actions
- Clone VM
- Launch console
- Pause VM
- Resume
- Snapshot
- Migrate VM
- Update VM configuration
- Delete VM

You can quickly find a specific entity, a subset of entities, or a range of entities by applying a filter to the results in the explore list. You can apply multiple filters to a single view to reduce the total results into a focused set. Each filter provides a count of the number of entities it applies to.

The filters for each type of entity are different but include the following:

- Host name
- Cluster name
- Hypervisor type
- Health

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3418

- Memory capacity
- CPU usage
- Memory usage
- Read IOPS
- Write IOPS
- I/O bandwidth
- I/O latency

Entity Tagging

You can use the entity explorer to tag VMs with one or more labels. When the entity explorer displays results, it represents the labels with a symbol and offers labels as an additional method to filter results.

Labels can have several uses, including tagging VMs that belong to a single application, business owner, or customer.

Nutanix Prism Search

Nutanix Prism quickly searches for data points and reduces the clicks required to find information through the search function. You can enter common tasks and entities in the search bar. The interface displays the returned results in a formatted entity explorer layout, typically with counts for each result type.

Beyond searching for entities, search quickly finds data such as versioning or a configuration setting from a group of entities. The updated search feature jumps directly to a page in Nutanix Prism, such as the software upgrade or name server configuration pages.

The search function offers autocomplete to help you identify or complete your target search string.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3419

Networking

Nutanix Prism network management features convey networking configuration and metrics for analysis. Nutanix Prism collects network data for VMs from the configured hypervisor and from configured physical network switches through SNMP.

When Nutanix Prism manages a cluster running AHV, it also lets you create new VM networks. Nutanix Prism provides a simple form for the network name and corresponding VLAN ID. After you create a network, you can assign it to existing and newly created VMs.

When creating each VM network, Nutanix Prism can also provide DHCP address management. This functionality allows you to configure address pools for each network that can be automatically assigned to VMs requesting DHCP addresses.

Data Protection

The data protection view in Nutanix Prism offers insight into Nutanix backup and replication capabilities following the same user experience as the other management views. The summary layout provides a single point of management for synchronous and asynchronous replication.

The data protection overview summarizes the number of remote sites and protection domains, giving you a quick look into the cluster’s data protection. Charts report replication data transfer bandwidth and a list of the top remote sites by bandwidth consumption. This report helps you understand the bandwidth that replication consumes, whether something is operating abnormally, and which sites use the most resources.

You can also monitor ongoing replication, pending replication, and successful replication tasks to see if any tasks stall or verify that replication completes successfully.

A protection domain is a set of policies governing local backup and remote replication functions for one or more VMs. A schedule attached to each protection domain controls the rate at which snapshots are taken and how long the system retains them. This architecture allows you to create protection domains that can protect a single VM or groups of VMs. The flexibility to use multiple protection domains in a cluster means that you can create different policies for protecting diverse applications and groups of VMs and for controlling replication to different sites and clusters.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3420

The data protection table view summarizes the configuration, performance, and status of the protection domains that provide backup and disaster protection in your cluster. From this view, you can see how many resources each protection domain consumes, what is contained in a protection domain, when the last snapshot was successfully taken, and whether any pending jobs exist.

When you select a specific protection domain or remote site, more data becomes available through additional charts and tables. These entity-specific data points provide extensive details on each item's contents, schedules, alerts, and metrics.

The protection domains that Nutanix uses to safeguard VMs can contain a single VM or groups of VMs. Selecting the VMs to include in a protection domain is simple and follows the previous upgrade and configuration examples. When you create or edit an existing protection domain, you can select from the list of all VMs running on the cluster.

User Management and Authentication

Prism Element offers two types of user accounts for authentication. You can create and manage the first type, local accounts, in the associated Prism Element instance. The second type of account bases authentication on a directory service. Configuring Prism Element to use a directory service supports Microsoft Active Directory and OpenLDAP as authentication sources, allowing you to use existing user accounts and groups to control access to Prism Element.

Prism Central supports local, Microsoft Active Directory, and OpenLDAP authentication in addition to SAML authentication. Both Prism Element and Prism Central support client authentication certificates.

Tasks

Monitoring and understanding the actions performed over time is helpful in any environment. Nutanix Prism records these actions and presents them as tasks in the tasks view. A table format displays all tasks and lists the performed action, the involved entity, and the cluster, status, running time, and duration of each action.

The task view shows recent actions for a comprehensive sense of the current status. It's also helpful when looking back to a specific period to research an issue’s root cause or to find the source of configuration changes.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3421

In environments running AHV, you can see a list of tasks performed against a single VM through the VM view in Prism Element.

Localization

Nutanix Prism offers Unicode (UFT-8 encoded) support for characters not contained in ASCII. Unicode support allows you to use supported characters in the names of entities such as containers, VMs, and clusters. Because Unicode support is native through every layer, service, and access point in the Nutanix platform, everything from command-line access to system services can use this expanded character set. When users change their preferred language in Nutanix Prism, the date, time, and number formats update to display correctly for the selected language.

Nutanix Prism also supports Simplified Chinese and Japanese.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3422

4. Operational Insights

Nutanix Prism helps you manage your Nutanix clusters by providing operational insights. Operational insights focus on providing alerts, metrics, and the ability to analyze data.

Alerts

The Nutanix Prism alerts view presents all notifications and events in an easy-to-consume table format. The table presents each alert with a color-coded severity level, a description of the alert, the timestamp, which entities the alert involves, and cause and resolution guidance.

To help you remediate alerts, Nutanix Prism summarizes the probable root cause for each alert. Nutanix Prism also provides the most likely resolution, helping correct issues faster.

Organizations can vary significantly, and if alert policies are too rigid to accommodate these differences, they become a hindrance. Nutanix Prism lets you update and customize alert policies with different values to suit your organization's conditions. The Prism Central instance applies such policy changes to all clusters under management.

When a different value applies to different clusters in the environment, you can configure each alert policy with exceptions.

With centralized control for alert policies and SMTP email alerts, you can set alerting policies from Prism Central, and the policies for all managed clusters automatically update to match. This feature saves time configuring and updating policies and ensures that each cluster is compliant.

User-Created Alerts

Along with customizable platform-level alerts, you can create alert policies to satisfy more specific monitoring requirements for an entity (VM, cluster, host, container) or group of entities. Each policy focuses on a selected metric, and you can configure it with a warning and alert value. To prevent false notifications, you can also configure the

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3423

policy such that the value doesn’t trigger an alert until that value is sustained for a certain amount of time.

Alert-Driven Root Cause Analysis

Prism Central offers a summary of probable causes and the most likely resolution for each generated alert. Each possible root cause that Prism Central suggests includes recommended steps for correcting the issue along with items to review, logs to examine, and any other applicable actions.

Some root cause corrective measures also provide a performance metric chart to review. To help identify whether a performance issue caused the problem, a bell on the chart marks the time when the alert was created. This marker allows you to see if the suggested metric was in violation at the time of the event.

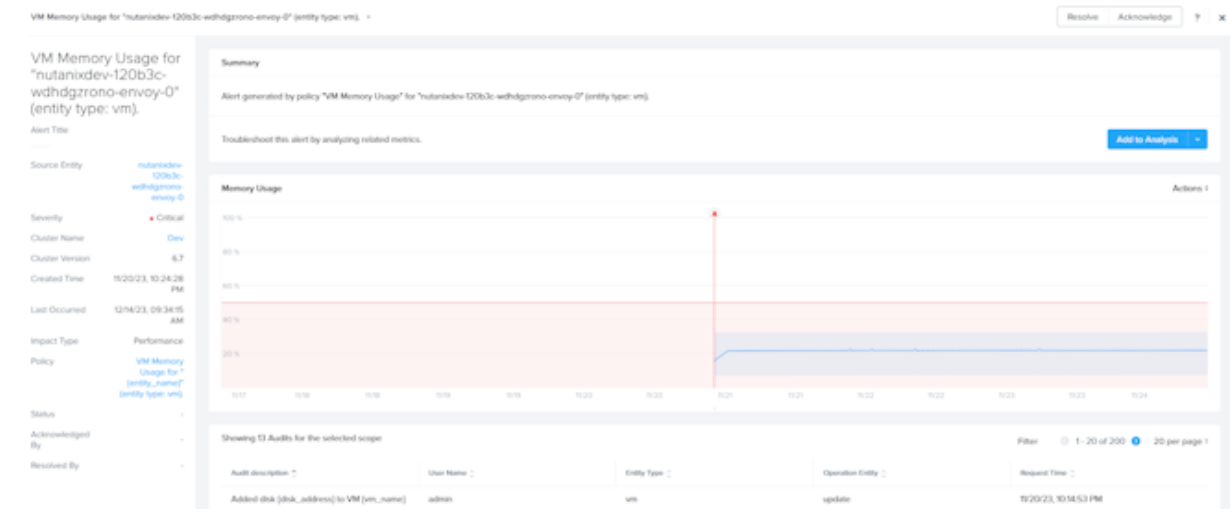


Figure 6: Root Cause Analysis

Analytics

Prism Central produces charts based on metrics that you select from the hundreds available. Each chart focuses on a single metric and can display data for one or multiple entities. The following entities are available in analytical charts:

- Hosts

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3424

- Clusters
- Disks
- Virtual disks
- Storage pools
- Containers
- Virtual machines
- Protection domains
- Remote sites
- Replication links

With granular entity selection and a large list of metrics, you can create charts as focused or as broad as you require.

Prism Element stores analytical data for 90 days; if you need to store data longer, you can configure a Prism Central instance for additional data retention. You can also look at an analytical chart in different time increments:

- Three hours
- Six hours
- One day
- One week
- Week to date
- One month

By changing a chart's time increments, you can select a specific day and focus on that date, a portion of the selected date, or the week surrounding the selected date. Variable date views provide insight into events leading up to or following a specific point in time.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3425

Analysis

Prism Element's analysis feature brings all relevant analytics into a single view. This unique analysis view stacks all the charts and lines them up in time sync. Above the stack of charts, Prism Element adds all alerts and events, represented with colors and counts.

Click a chart at any point to place a vertical line through all charts for easy correlation. Focusing on a specific point and syncing all metrics can reduce the effort to identify possible root causes. The column on the right provides a summary of any alerts and events so that you don’t need to leave the analysis page.

Prism Element brings all the relevant analytics into one view.

Figure 7: Prism Element Analysis View

The analysis view allows you to fully customize the number and size of the analytical charts you see, add charts or remove them as needed, and export each chart to a CSV or JSON file.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3426

VM I/O Metrics

When you select a VM in the VM-focused view in Prism Element, the I/O Metrics tab provides a deeper set of storage-related data points. These data points focus on I/O statistics and patterns for the selected VM. Determining I/O behavior and patterns is helpful when sizing or scaling workloads or troubleshooting issues.

The following data points are available:

- Read performance distribution by I/O block size
- Write performance distribution by I/O block size
- Average I/O latency (read versus write)
- Read latency distribution by percentage
- Write latency distribution by percentage
- Read source (DRAM, SSD, or HDD tiers)
- Read I/O (sequential versus random) by percentage
- Write I/O (sequential versus random) by percentage

Network Visualization

The network view in Prism Element visually represents networking connections and traffic flows. In this view, VMs are located on the left and you can group them using filters or show them as a list. The physical nodes appear in the middle of the screen, and the connected network switches are represented on the right. This visualization provides access to the entire environment, and you can filter each column to a group or single entity.

With network visualization, you can select a single VM and understand its connected networks. You can see the host a VM runs on, which physical network connection it uses, and what switch port that connection uses. This level of detail is vital when you need to report on environment configuration, make changes, or troubleshoot an issue.

In Prism Element, you can use network visualization for a single VM, a group of VMs, or hypervisor nodes. Networks are color-coded at the VM and network switch levels so

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3427

you can easily understand whether the networks configured for a VM are available on the switch port they're using. Network visualization is currently only available for clusters running AHV as the hypervisor.

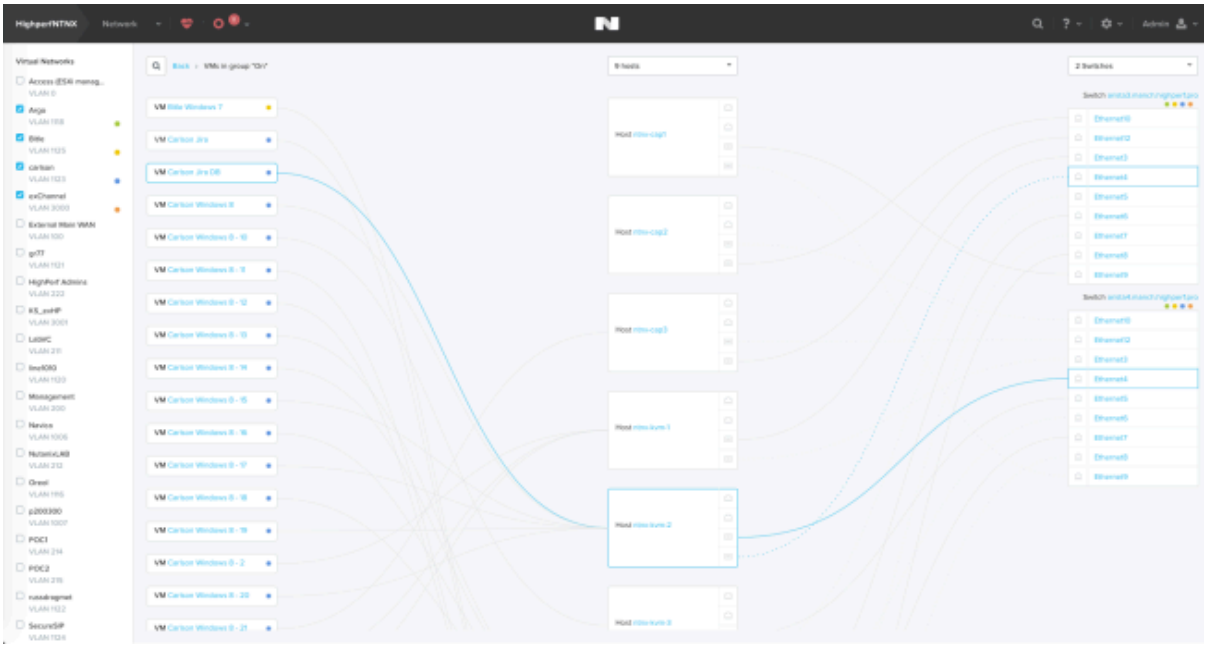


Figure 8: Network Visualization View

© 2025 Nutanix, Inc. All rights reserved |

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3428

5. Prism API

Nutanix Prism offers and consumes the Nutanix API. Each function you can use in the Nutanix Prism HTML5 interface is performed in the background using API calls. The REST API is also available to allow other systems to access Nutanix data and to let you build your own automation using API functions.

Nutanix Prism provides a REST API explorer to simplify the experience of discovering available functions and testing their outputs before trying them in your custom code. The explorer-focused view lists all commands and groups them into categories based on the entity or function to connect with.

You can expand each group in the explorer to show the list of API commands in the group. These include GET, PUT, PATCH, POST, and DELETE commands, allowing for a specific function to be created, updated, or deleted.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3429

6. Conclusion

Nutanix embodies a new approach to enterprise infrastructure that simplifies every step of the infrastructure life cycle, from buying and deploying to managing, scaling, and supporting. The Nutanix solution’s web-scale technologies and architecture let you run any workload at any scale. With Nutanix AOS and Nutanix Prism, you have powerful virtualization capabilities that are fully integrated into the converged infrastructure stack and can be managed from a single pane of glass.

© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3430

About Nutanix

Nutanix offers a single platform to run all your apps and data across multiple clouds while simplifying operations and reducing complexity. Trusted by companies worldwide, Nutanix powers hybrid multicloud environments efficiently and cost effectively. This enables companies to focus on successful business outcomes and new innovations. Learn more at Nutanix.com.

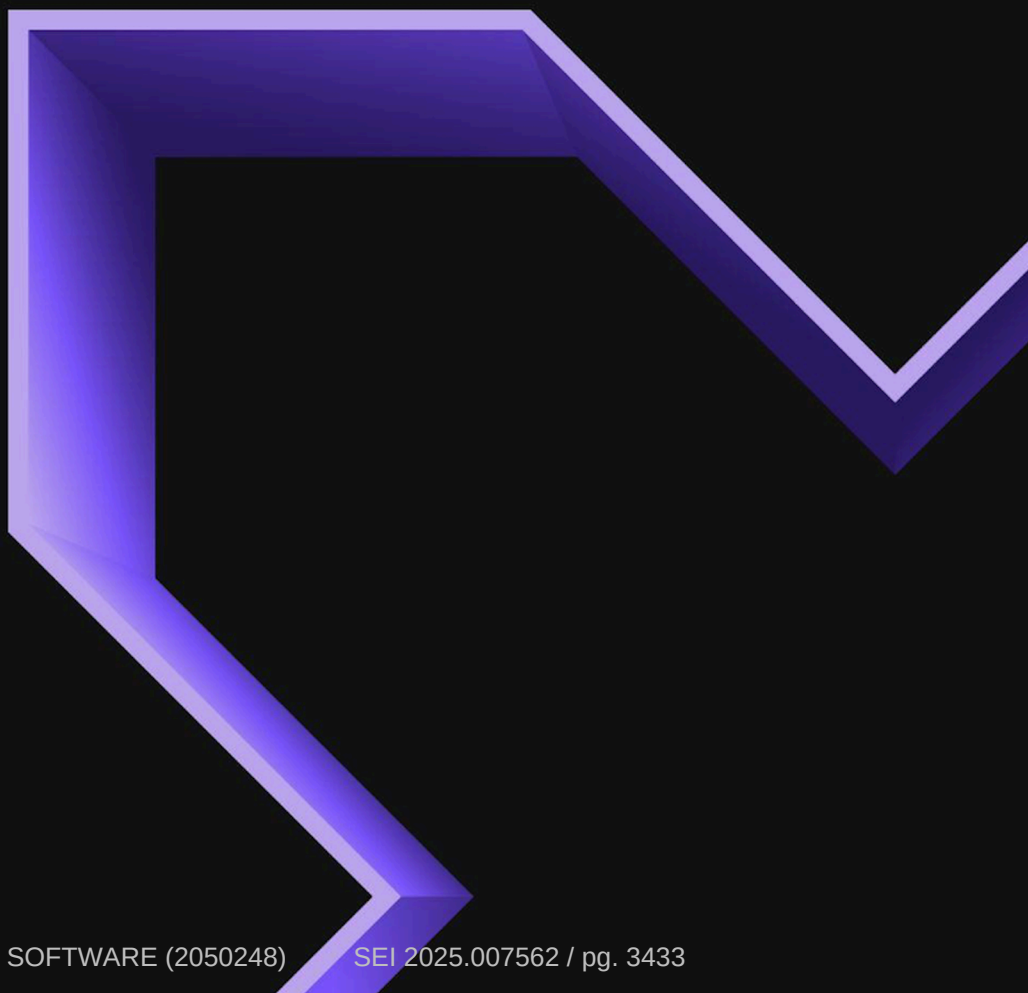
© 2025 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3431

List of Figures

Figure 1: Conceptual View of Prism Element Services and HTTP Request Handling....8
Figure 2: Prism Central Architectures....9
Figure 3: Prism Element Storage Management View....12
Figure 4: Prism Element Storage Management Table View....13
Figure 5: Entity Explorer in Prism Central....15
Figure 6: Root Cause Analysis....22
Figure 7: Prism Element Analysis View....24
Figure 8: Network Visualization View....26

SOLUTIONS DOCUMENT

Nutanix Pulse and Remote Diagnostics



NUTANIX

Legal

© 2024 Nutanix, Inc. All rights reserved. Nutanix, the Enterprise Cloud Platform, the Nutanix logo and the other Nutanix products, features, and/or programs mentioned herein are registered trademarks or trademarks of Nutanix, Inc. in the United States and other countries. All other brand and product names mentioned herein are for identification purposes only and are the property of their respective holder(s), and Nutanix may not be associated with, or sponsored or endorsed by such holder(s). This document is provided for informational purposes only and is presented "as is" with no warranties of any kind, whether implied, statutory or otherwise.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

Contents

1. Executive Summary....4
Document Version History....4

2. Nutanix Pulse Overview....6
Pulse Health Monitoring Configuration....7
Network Configuration for Pulse Health Monitoring....7
Pulse Related Software Components....8
Data Obfuscation....8
Pulse Information Transmission Frequency....9

3. Remote Diagnostics Overview....10
Enabling and Disabling Remote Diagnostics....10
Remote Diagnostics Required Software....10
Remote Diagnostics Workflow....11
Remote Diagnostics Data Collection....11
Auditing Remote Diagnostic Collections....11
Remote Diagnostics Security....13

About Nutanix....14

Legal....15

List of Figures....16

1. Executive Summary

Most enterprise IT solutions rely on a reactive approach to system maintenance and issue resolution. For example, when a technical issue arises, vendor support teams typically capture detailed system data from the customer and recreate the issue in a separate environment—only then can the actual debugging begin. This approach consumes unnecessary time and resources and ultimately delays resolution.

Nutanix simplifies and streamlines this process through two important support services: Pulse Health Monitoring and Remote Diagnostics. When enabled, Pulse captures purpose-driven diagnostic data on a regular schedule. The Remote Diagnostics service, which is enabled by default on Pulse-enabled clusters (and which the customer can disable), is event-driven and helps to provide proactive support.

Benefits of enabling Pulse Health Monitoring and Remote Diagnostics include:

- Reduce resolution time by up to 40 percent
- Personalize your Nutanix Support experience
- Proactive issue resolution
- Intelligent monitoring
- Secure data transmission

For more information, see the Nutanix Insights solution brief and the Pulse Health Monitoring section of the Prism Central Admin Center Guide.

Document Version History

Version Number	Published	Notes
1.0	October 2019	Original publication.
1.1	November 2020	Refreshed content.
1.2	April 2021	Updated the Remote Diagnostics section.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3436

Version Number	Published	Notes
1.3	March 2022	Updated the Nutanix Pulse section.
1.4	April 2022	Updated the Data Obfuscation section.
1.5	October 2023	Updated the references to relevant product documentation throughout.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3437

2. Nutanix Pulse Overview

Nutanix Pulse is the telemetry capability built into all Nutanix clusters that sends key health metrics to the Nutanix Insights service. Nutanix can use the diagnostic system information that Pulse sends to help build better products and provide a great customer experience. At Nutanix, our vision is to enable invisible infrastructure for IT teams—Nutanix Pulse is another step in that direction.

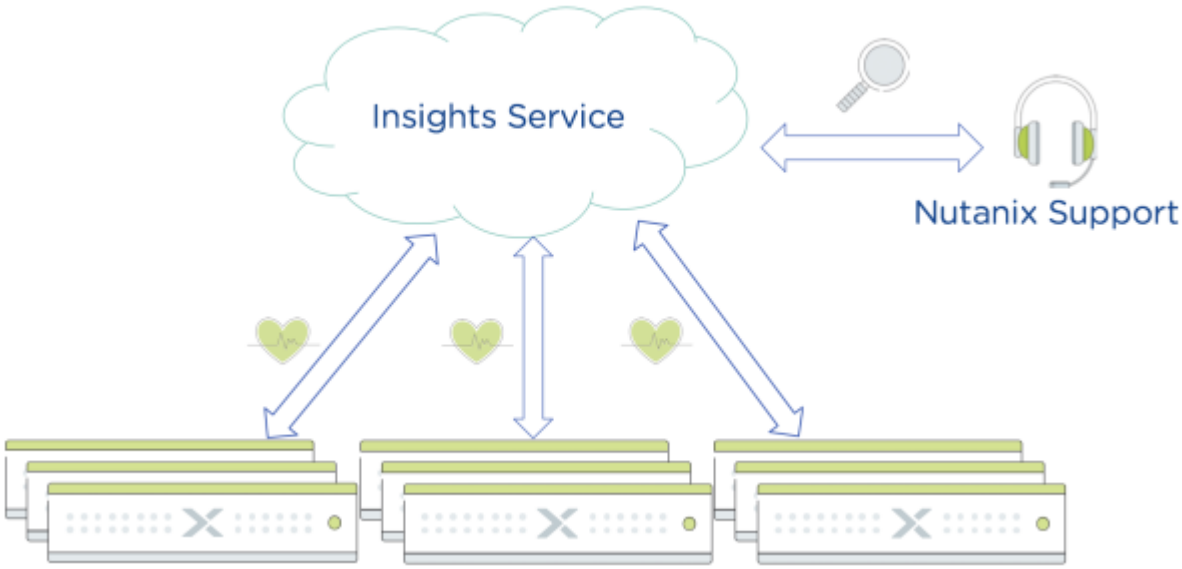


Figure 1: Pulse-Enabled Clusters Send Pulse Telemetry to Nutanix Insights

Nutanix uses this Pulse information in several important ways:

- Nutanix Support teams can use this data to deliver proactive, context-aware support for Nutanix solutions.
- IT admins can see insights and alerts from the data on the Nutanix Portal, with actionable guidance to help them address issues themselves.
- When a cluster encounters fatal or critical alerts, support teams can proactively create a case and kickstart the resolution process, often before IT teams have even discovered the issue.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3438

- Nutanix can also use this information to analyze product and feature usage and effectiveness.

When Pulse is enabled, a Nutanix cluster automatically and unobtrusively collects diagnostic information. Pulse shares this system-level information to monitor the health and status of a Nutanix cluster. The shared information includes the following data points:

- System alerts
- System tasks
- System logs
- System configuration
- Performance metrics
- Current Nutanix software version
- Nutanix processes and Controller VM (CVM) information
- Hypervisor details such as type and version

All the information in these categories is specific to Nutanix internal processes and doesn't contain information regarding customer workloads or applications. Nutanix encrypts all communication from clusters to the Nutanix Insights service for security.

Nutanix processes data that Pulse sends in a manner consistent with your agreement with Nutanix and, where applicable, the Nutanix Privacy Statement. Certain Nutanix products require Pulse enablement for functionality and features. See the applicable product documentation for more details.

Pulse Health Monitoring Configuration

For more information on configuring Pulse Health Monitoring, see the Prism Central Admin Center Guide.

Network Configuration for Pulse Health Monitoring

For more information on network configuration for Pulse Health Monitoring, see the Prism Central Admin Center Guide.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3439

All traffic for Pulse is outbound. No inbound connection is initiated to the clusters.

Nutanix recommends that you set up Alert emails for proactive support and case creation. For more information, see the Configuring Alert Emails section in the Prism Web Console Guide.

Pulse Related Software Components

Three key components contribute to Pulse Health Monitoring functionality:

Nutanix Cluster Check (NCC)

All diagnostic data collectors are built into NCC and are responsible for collecting and packaging the right metrics, counters, configuration details, and logs. We recommend that all Nutanix clusters always run the latest version of NCC.

Prism Central

Although Pulse doesn't require Prism Central to function, using Prism Central dramatically simplifies the setup and network configuration.

Nutanix Insights

The Insights service, operated by Nutanix, always runs the latest version and doesn't require any maintenance effort from IT teams.

Data Obfuscation

Based on your Pulse settings, the following attributes and rules might be obfuscated when they are collected. The Insights platform receives this information as random strings.

- cluster name
- ipv6_address
- ipv4_address
- domain
- vm_name
- container_name

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3440

- vstore_name
- remote_name
- ntp_server_list
- smtp_server
- http_proxy
- service_center
- directory_url
- snmp trap address
- access url
- management server name
- ipmi address
- ipmi username
- Any attribute value having regex pattern similar to IP address

Pulse Information Transmission Frequency

A cluster with Pulse enabled sends information at different intervals, balancing bandwidth conservation, latency sensitivity, and utility.

- Every configuration change streams immediately to the Insights service.
- Select critical or fatal log messages stream immediately to the Insights service.
- Pulse aggregates metrics (such as resource consumption, service counters, and so on) and sends them every 15 minutes or 60 minutes, depending on the NCC version installed.
- Pulse takes a snapshot of the current cluster configuration every 12 hours.

Pulse collectors have strict resource-use limitations in place, with a clear intent to never burden CPUs, memory, or disks on the cluster.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3441

3. Remote Diagnostics Overview

With the Remote Diagnostics service, Nutanix Support can request granular diagnostic information from Pulse-enabled clusters. While Pulse-enabled clusters stream configuration, metrics, alerts, events, and select logs back to Nutanix Insights, this data is aggregate in nature and represents the cluster at a high level. This high-level cluster state is extremely useful, but there are times when Nutanix Support may require detailed information (such as specific service logs) to diagnose a specific issue.

In such cases, authenticated and authorized Nutanix employees across the Nutanix Support, Nutanix Sales Engineering, and Nutanix Customer Success organizations can use the Nutanix Remote Diagnostics service to connect to Pulse-enabled Nutanix clusters when relevant to the case or customer and initiate a diagnostic collection.

Enabling and Disabling Remote Diagnostics

The Remote Diagnostics service is enabled by default for every cluster where Nutanix Pulse is enabled. You can disable Remote Diagnostics without turning off Pulse. Nutanix Support can still provide seamless proactive support based on Nutanix Pulse without Remote Diagnostics.

For the latest guidance on configuring Remote Diagnostics, see Pulse Health Monitoring in the Prism Central Guide.

Remote Diagnostics Required Software

To support the Remote Diagnostics capability, you must have NCC version 3.7.0.1 or later on Pulse-enabled clusters. Nutanix recommends that you always run the latest NCC version.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3442

Remote Diagnostics Workflow

When Nutanix Systems Reliability Engineers (SREs) are engaged in a Support case and assess the need to collect some diagnostic data from the relevant clusters, they go through the following workflow:

1. Access the Remote Diagnostics service internally operating at Nutanix, then connect to the relevant cluster.
2. Define a diagnostic collection on the cluster.

   Defining the diagnostic collection establishes the data to collect and the specific time window for data collection.
3. Run the defined diagnostic collection on the cluster.

   Relevant diagnostic data streams to the Remote Diagnostics service, using the existing Pulse HTTPS channel, which is outbound from the cluster.

At the end of this workflow, the Nutanix SRE has the relevant data to proceed with case analysis and resolution.

In addition to SRE-initiated collections, Remote Diagnostics is also integrated with an alert-triggered log collection (ATLC) feature for clusters running NCC version 4.2.0 and later. For a subset of ATLC-enabled alerts, Pulse collectors initiate a request and start streaming the bundle to the Remote Diagnostics service using the same Pulse HTTPS channel. For more details, see Alert Triggered Log Collection.

Remote Diagnostics Data Collection

Remote Diagnostics allows Nutanix Support to request a restricted set of data for use when troubleshooting a specific issue. For more information on the data that the service can request remotely, see Pulse Health Monitoring in the Prism Central Guide.

Only Nutanix Support can view the collected diagnostic bundles.

Auditing Remote Diagnostic Collections

Nutanix audits every use of the tool on the Nutanix clusters and internally in the Remote Diagnostics service. Every time Nutanix Support uses Remote Diagnostics to trigger a diagnostic collection on the cluster, the system creates an entry in the cluster's audit trail.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3443

There are always two entries for Remote Diagnostics events:

- Start of the diagnostic collection
- End of the diagnostic collection

You can access this audit trail on the Prism Central instance where the cluster is registered.

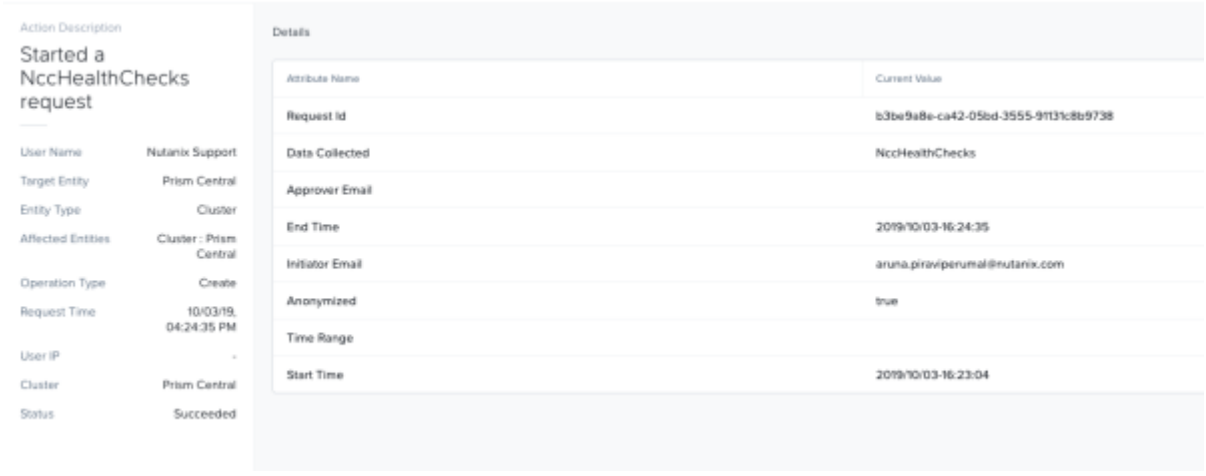


Figure 2: Sample Audit Entry Showing the Start of a Diagnostic Collection

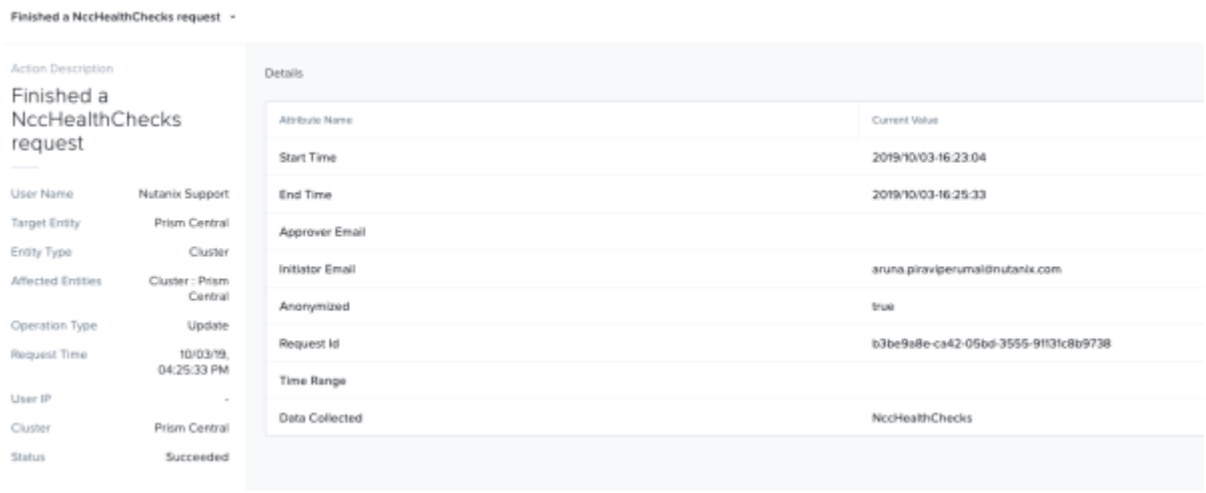


Figure 3: Sample Audit Entry Showing the End of a Diagnostic Collection

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3444

Remote Diagnostics Security

Security is a prime consideration at Nutanix and central to the design of the Remote Diagnostics service. The internal communication mechanism that powers Remote Diagnostics demonstrates how this functionality is secure by design.

- While Remote Diagnostics allows Nutanix Support to remotely initiate a diagnostic collection on a cluster, this connection is never inbound to a cluster. Inbound connections would require opening the firewall in your network. To ensure a better security posture, all communication from a cluster is outbound.
- Pulse collectors on the cluster poll the Remote Diagnostics service every 2 minutes to check for a diagnostic collection request initiated by Nutanix Support. When a collection request is pending, the cluster's poll action picks up the relevant request payload.
- The outbound poll request and all subsequent traffic travels over HTTPS (port 443) using TLS 1.2.
- Pulse collectors on the cluster interpret the curated set of commands in the request payload that the cluster’s poll action picked up. To protect this payload from malicious commands, the user can only select from a tightly limited set of read-only commands in the Nutanix Insights service.

© 2024 Nutanix, Inc. All rights reserved |
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3445

About Nutanix

Nutanix offers a single platform to run all your apps and data across multiple clouds while simplifying operations and reducing complexity. Trusted by companies worldwide, Nutanix powers hybrid multicloud environments efficiently and cost effectively. This enables companies to focus on successful business outcomes and new innovations. Learn more at Nutanix.com.

© 2024 Nutanix, Inc. All rights reserved
Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3446

Legal

© 2024 Nutanix, Inc. All rights reserved. Nutanix, the Enterprise Cloud Platform, the Nutanix logo and the other Nutanix products, features, and/or programs mentioned herein are registered trademarks or trademarks of Nutanix, Inc. in the United States and other countries. All other brand and product names mentioned herein are for identification purposes only and are the property of their respective holder(s), and Nutanix may not be associated with, or sponsored or endorsed by such holder(s). This document is provided for informational purposes only and is presented "as is" with no warranties of any kind, whether implied, statutory or otherwise.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3447

List of Figures

Figure 1: Pulse-Enabled Clusters Send Pulse Telemetry to Nutanix Insights..... 6

Figure 2: Sample Audit Entry Showing the Start of a Diagnostic Collection.....12

Figure 3: Sample Audit Entry Showing the End of a Diagnostic Collection.....12

Veeam Data Platform

Veeam Backup & Replication
Veeam ONE
Veeam Recovery Orchestrator

Feature Comparison

Contents

Licensing Details	3
Licenses for Veeam Cloud and Managed Service Providers (VCSP)	3
AI *Powered by Veeam Intelligence*	5
AI	5
Backup and Recovery *Powered by Veeam Backup & Replication*	6
Security	6
Backup	8
Cloud Backup & Recovery	11
Enterprise App Backup Plugins	11
Storing Backups	12
Replication	14
Restore	15
Instant Recovery	16
File & Item-level Recovery	16
DataLabs	18
Self-service	19
Deployment	20
Management	21
Monitoring and Analytics *Powered by Veeam ONE*	22
Monitoring and Reporting	22
Monitoring and Alerting for Hybrid Cloud	23
Monitoring and Alerting for Virtual Infrastructure	24
Report and Alarm Customization and Automation	25
Governance and Compliance	25
Intelligent Automation	25
Dashboards	26
Capacity Planning	26
Chargeback and Billing	26
Recovery Orchestration *Powered by Veeam Recovery Orchestrator*	27
Recovery Orchestration & Automation	27
Dashboards & Reporting	28

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3450

Veeam Data Platform offers several options packaged to deliver relentless security, fast, reliable recovery, and complete data portability. Whether you're just getting started or you're managing a large enterprise operation, Veeam has a flexible option for you. The Veeam Universal License (VUL) is a game-changing portable license that allows you the flexibility to protect cloud, virtual and physical workloads interchangeably no matter where you are on your hybrid journey. The extremely capable backup, monitoring and recovery features of Veeam Data Platform are ready to keep your business running.

Licensing Details

The fully featured, portable Veeam Universal License (VUL) is how the Veeam Data Platform is licensed, enabling support across any environment, whether it be on-premises, or in hybrid- or multi-cloud deployments, including full feature capability for all workload types, including VMware, Hyper-V, AWS, Azure, Google Cloud, Windows, Linux, macOS, Nutanix, Oracle Linux Virtualization Manager, Red Hat Virtualization, Scale Computing HyperCore, Proxmox VE and much more. This document outlines the features that are available by the proper Veeam Data Platform edition.

If you need detail for cross-referencing legacy socket-based licensing which ceased sale in 2023, please see this asset.

Workloads **Environments**	**Veeam Universal License** **On-premises, cloud and hybrid**
Expanded	**Yes**
Virtual machines: VMware vSphere, Microsoft Hyper-V, Nutanix AHV, Oracle Linux Virtualization Manager, Red Hat Virtualization, Scale Computing HyperCore & Proxmox VE	
Physical servers, workstations and endpoints: Windows, Linux, macOS, Oracle Solaris and IBM AIX	**Yes**
Enterprise apps for Microsoft, Oracle, SAP HANA, MongoDB and more	**Yes**
Cloud-native backup and recovery for AWS, Microsoft Azure and Google Cloud	**Yes**
Object Storage backup and NAS File Shares	**Yes**
Microsoft Entra ID, Intune Policies	**Yes**
Deployment	
New Veeam Software Appliance	**Yes**

Licenses for Veeam Cloud and Managed Service Providers (VCSP)

VCSP rental licenses function in a similar way to subscription licenses, but uses a point-based system. For more information, please refer to your VCSP licensing documentation. For VCSP partners leveraging Veeam Data Platform, please use this feature comparison guide. For standalone licenses, service providers can access the VCSP Feature Comparison guide on **Pro**Partner Portal.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3451

Veeam Data Platform

	Secure Foundation			Cyber Resilience					Enterprise Resilience		
	Zero Trust Data Resilience	AI Guidance	Detect + Identify Threats		Security and Observability			GenAI Insights	Recovery Orchestration and Compliance		Threat Assessment
	Data Protection & Verified Recovery	On-demand Assistance	AI-powered Malware Detection	IoC Tools Scanning	Security Integrations	Analytics, Discovery & Reporting	Veeam Threat Center	Trends & Decision Support	Orchestrated Recovery & Validation	GRC Audit Documentation	Proactive Threat Assessment
Foundation	✓	✓	✓	—	—	—	—	—	—	—	—
Advanced	✓	✓	✓	✓	✓	✓	✓	✓	—	—	✓
Premium	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

- Veeam Backup & Replication
- Veeam ONE
- Veeam Recovery Orchestrator
- Coveware Recon Scanner

\+ veeam Cyber Secure

- Coveware incident response subscription with 15-min SLA
- Up to $5M ransomware warranty with Veeam Technical Account Manager
- 24/7/365 SWAT team and dedicated Support Account Manager
- Onboarding, design, implementation services, and quarterly security assessment checks

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

✓ Fully supported ✓ Partially supported

AI *Powered by* *Veeam Intelligence*	**Veeam Data Platform** **Veeam Universal License (VUL)**			**Description**
	Community	**Foundation**	**Advanced**	**Premium**	
AI					
New Malware Deep Analysis Agent			✓	✓	Quickly identify threats and understand their impact with clear visualizations and guided recovery steps. Respond faster to incidents, reduce downtime, and restore data safely without switching between tools.
New Deep Data Analysis Agent			✓	✓	Get to the right answers in moments by querying complex data with natural language. Convert massive reports into clear summaries and prioritized recommendations so you can act faster and with confidence. *Available in Veeam ONE
New Speech to Text		✓	✓	✓	Speak instead of type to get fast, accurate results. Voice input streamlines your workflow, captures technical details, and enables you to work without limits.
New Data Resilience Daily Summary report			✓	✓	Delivers one daily email summarizing policy and job results, correlating issues with Veeam KB articles, and listing recommended actions after analysis completes.
New Intelligent Reporting & Interaction			✓	✓	Turn complex data into clear, actionable insight so you can decide faster and move with confidence. Interactive reporting makes information easy to explore, reduces noise, and keeps your team focused on results. *Available in Veeam ONE
Chat assistance		✓	✓	✓	Resolve issues faster, optimize performance, and make confident decisions with quick answers and actionable insights.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3453

✓ Fully supported ✓ Partially supported

Backup and Recovery *Powered by Veeam* *Backup & Replication*	**Veeam Data Platform** **Veeam Universal License (VUL)**			**Description**
	Community	**Foundation**	**Advanced**	**Premium**	
Security					
New Veeam Updater		✓	✓	✓	Simplify and automate the process of keeping Veeam Software Appliance and Veeam Infrastructure Appliance components up to date. It enables seamless installation of updates and patches for both the operating system and Veeam applications through an intuitive web-based interface or command-line utility. Requires an active support contract.
New SAML support		✓	✓	✓	Support for SAML 2.0 (Security Assertion Markup Language) authentication to enable organizations to integrate with third-party identity providers (IdPs) for secure, federated single sign-on (SSO) and user authentication.
Veeam Threat Hunter			✓	✓	Experience improved speed and expanded protection against millions of malware threats using built-in low impact signature-based scans with real-time threat database updates.
IoC Tools Scanner			✓	✓	Expand the hunt for Indicators of Compromise (IoC) in protected machines and stop attacks by identifying known tools from hackers' toolkit and data exfiltration tools.
Coveware Recon Scanner			✓	✓	Protect your backup servers by identifying adversary tactics, techniques, and procedures (TTPs) used during a cyberattack. (Powered by Coveware).
Malware detection		✓	✓	✓	Scan and analyze all protected machines with little impact on backup windows — during the backup process. Using File Index Analysis — search for encrypted file extensions by comparing new data against last successful backup if found. Backup will continue to run but will flag as "suspicious, infected, or clean". (*YARA Scan requires Advanced or Premium Edition)
YARA scan			✓	✓	New Content Scan option available in SureBackup, Secure Restore, and Scan backup functionality backup provides an additional level of security by scanning entire backups with YARA engine against the detection rules of choice. Can be easily used to quickly pinpoint the known threat or to perform a pattern-based search. (*YARA Scan requires Advanced or Premium Edition)
Veeam App for CrowdStrike Falcon LogScale			✓	✓	Veeam Data Platform event data is sent to the CrowdStrike Falcon Logscale engine and automatically analyzed by leveraging pre-built monitoring dashboards and scheduled searches.
Veeam Data Connector for CrowdStrike Next-Gen SIEM			✓	✓	Data parser that can ingest over 300 individual Veeam Data Platform events for custom dashboards or data analytics.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3454

✓ Fully supported ✓ Partially supported

Backup and Recovery *Powered by Veeam Backup & Replication*	**Veeam Data Platform** **Veeam Universal License (VUL)**				**Description**
	Community	**Foundation**	**Advanced**	**Premium**	
Veeam App for Splunk			✓	✓	Leverage Veeam Event Forwarding capabilities, Veeam App for Splunk includes monitoring and security dashboards, security alerts, and reports. The app integrates seamlessly with Splunk user roles and location management.
Veeam App for Palo Alto Networks XSIAM			✓	✓	Leverage Veeam Event Forwarding capabilities from both Veeam Backup & Replication as well as Veeam ONE, the Veeam App for PaloAlto XSIAM includes monitoring and security dashboards and reports. It also integrates with PaloAlto user management and location awareness.
Veeam App for Palo Alto Networks XSOAR			✓	✓	Offers a bi-directional API-level integration with Veeam Backup & Replication and Veeam ONE for SOC and Automation teams. It provides automatic incident creation, a security dashboard based on Veeam security indicators and allows incident remediation right out of the XSOAR UI.
Veeam App for ServiceNow			✓	✓	Automate Veeam Backup and Recovery in ServiceNow with dashboards, audit-ready logs, and self-service to speed response and strengthen compliance.
Veeam App for Microsoft Sentinel			✓	✓	Integrates Veeam resilience into SOC workflows by streaming backup/security events and adversary TTPs to Microsoft Sentinel, enabling bi-directional incident API actions for faster detection and response.
Syslog Event Forwarding		✓	✓	✓	Veeam events can be streamed to external syslog servers, including third-party syslog-compatible SIEM tools that monitor for known events, extending support to security teams.
Veeam Incident API		✓	✓	✓	Let your cyberthreat tool report infections directly into the Veeam Incident API, marking existing restore points as infected or trigger backup.
Four Eyes Authorization for backup deletion		✓	✓	✓	Four Eyes Authorization will require secondary user to authorize destructive operations related to backup deletion or repository deletion in Veeam Backup & Replication, addition of new admins, removal of existing users, or changes to MFA.
Key Management System (KMS) Integration			✓	✓	Centrally manage cryptographic keys, eliminating the need for app-specific key management. (Requires Advanced or Premium editions for this functionality).
Secure Restore		✓	✓	✓	Increase security and reduce interruptions caused by malware and recover back to a safe, uncompromised restore point through an optional YARA scan performed directly in backup files prior to recovery. (*YARA Scan requires Advanced or Premium Edition).

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

✓ Fully supported ✓ Partially supported

Backup and Recovery *Powered by Veeam Backup & Replication*	**Veeam Data Platform Veeam Universal License (VUL)**				**Description**
	Community	**Foundation**	**Advanced**	**Premium**	
SureBackup		✓	✓	✓	Automatically detect threats, test, and verify the recoverability of each backup by running the VM directly from a backup file in a fenced-off copy of your production environment, including support for custom application test scripts. Perform manual, ad-hoc backup content scans* for imported backups or whenever threat analysis is required. (*YARA Scan requires Advanced or Premium Edition).
Immutability	✓	✓	✓	✓	Immutibility is provided by hardened repository for all editions.
Multi-factor authentication (MFA)		✓	✓	✓	Enhance Veeam Backup & Replication access control by enabling multifactor authentication for backup console users.
Deployment in Kerberos-only environments	✓	✓	✓	✓	Move security to a new level with the possibility to run all Veeam components in the Kerberos-only environments.
Veeam Security & Compliance Analyzer	✓	✓	✓	✓	
Deployment in IPv6 environments	✓	✓	✓	✓	Veeam backup infrastructure is fully prepared to operate in the modern data centers configured with IPv6 networking.
FIPS compliance	✓	✓	✓	✓	Veeam backup infrastructure components use FIPS-compliant cryptographic APIs and modules.
Audit capabilities	✓	✓	✓	✓	Track user actions and backup activities with Windows events and gain complete transparency over file level restore operations via specifically designed audit files.
Backup					
Support for VMware vSphere, Microsoft Hyper-V hypervisors	✓	✓	✓	✓	Protect VMs, data, applications, and more with the ability to instantly recover complete VMs as well as perform granular recovery of key application items.
Support for Proxmox VE hypervisor	✓	✓	✓	✓	Data protection and granular recovery for Proxmox Virtual Environment VMs and data.
Support for Nutanix AHV hypervisor	✓	✓	✓	✓	Protect Prism Central or Prism Element-hosted VMs, data, applications, and more with the ability to instantly recover any image-level backup to AHV as well as perform granular recovery of key application items.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

✓ Fully supported ✓ Partially supported

Backup and Recovery *Powered by Veeam Backup & Replication*	**Veeam Data Platform Veeam Universal License (VUL)**				**Description**
	Community	**Foundation**	**Advanced**	**Premium**	
New Support for Scale Computing HyperCore	✓	✓	✓	✓	Provides native, agentless backup and recovery for Scale Computing HyperCore with secure, immutable protection, ransomware resilience, and seamless portability.
Support for Oracle Linux Virtualization Manager and Red Hat Virtualization hypervisor	✓	✓	✓	✓	Data protection and granular recovery for Oracle Linux Virtualization Manager and Red Hat Virtualization hypervisor VMs, data, and applications.
Enhanced Veeam Backup *for Microsoft Entra ID*	✓	✓	✓	✓	Expand data protection and resilience with backup and restore capabilities for Entra ID, including Intune Device Configuration profiles and Device Compliance Policies. (Log backups require Advanced or Premium Edition).
Support for Public Cloud IaaS and PaaS	✓	✓	✓	✓	Native snapshotting, image-based backup and agent-based backup options for cloud-hosted VMs, databases, file shares, and object storage from leading providers like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud.
Application- aware, image-based backups	✓	✓	✓	✓	Create application-consistent backups with advanced, application-aware processing for granular recovery. (Transaction log backup for Oracle, PostgreSQL and SQL Server is not included with Community Edition).
MongoDB Backup		✓	✓	✓	MongoDB backup policy enables the protection of MongoDB workloads with application-consistent backups, enabling granular recovery.
NAS Backup	✓	✓	✓	✓	Protect and recover NAS file shares (SMB and NFS) effectively and at scale. Back up directly to Veeam repositories for short and long-term storage objectives. The first 500GB in each share is free with additional capacity licensed with VUL at 500GB per license. Write NAS backups to disk, tape or object storage targets. Long-term file version archival support for NAS data is not available with Community edition. The first 500GB of any data source is free with all additional capacity licensed with VUL at 500GB per license.
Backup of Object Storage	✓	✓	✓	✓	Protect data hosted on object storage with granular backup and recovery options. Ability to restore to different object storage types (e.g, S3 to SMB). Versatile backup targets, including existing backup repositories as well as directly to tape. Including new native protection and resilience for data residing in Azure Data Lake Storage Gen2. The first 500GB of any data source is free with additional capacity licensed with VUL at 500GB per license.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

✔ Fully supported ✔ Partially supported

Backup and Recovery *Powered by Veeam Backup & Replication*	**Veeam Data Platform Veeam Universal License (VUL)**				**Description**
	Community	**Foundation**	**Advanced**	**Premium**	
Agents *for Microsoft Windows, Linux* and *macOS*	✔	✔	✔	✔	Agent-based backup for Windows, Linux and macOS servers, and workstations with automated deployment and management directly within the backup console.
Cloud-Integrated Agents	✔	✔	✔	✔	Create application-aware backups of workloads hosted on Infrastructure as a Service (IaaS) VMs using cloud-optimized Veeam Agents. Optimizations include writing backups directly to object storage, utilization of AWS, Microsoft Azure, and Google Cloud services for workload discovery and inclusion/exclusion, and independent operation without direct network connectivity.
Agents for AIX and Solaris		✔	✔	✔	Agent-based backup for AIX and Solaris servers and workstations to Veeam backup repositories.
Backup copy jobs	✔	✔	✔	✔	Copy any backups to your DR storage location of choice automatically, including validation and remediation, to ensure copies are available and reliable.
End-to-end encryption	✔	✔	✔	✔	Secure the backup data and network transfers with end-to-end AES 256-bit encryption without any negative impact on built-in compression and WAN acceleration data reduction ratios. All editions include encryption at-source, in-flight, and at-rest. Community edition does not include lost password protection.
Primary Snapshot Orchestration	✔	✔	✔	✔	Additional storage snapshots, including the option for Oracle and SQL Server transaction log backup, can be created on the primary storage arrays for a wide range of storage systems. Orchestration for secondary storage snapshots is included for several storage vendors.
ROBO Guest Interaction Proxy		✔	✔	✔	Reduce the load on the central backup server, improve scalability, and simplify networking for environments with a large number of remote office/branch offices (ROBOs) when performing application-aware processing and guest file system indexing.
Proxy affinity		✔	✔	✔	Avoid cross-node network traffic across multiple all-in-one Veeam appliances by associating backup proxies and backup repositories located on the same appliance together.
Storage latency control		✔	✔	✔	Set the maximum acceptable I/O latency level for production datastores to ensure that backup and replication activities do not impact storage availability to production workloads. Enterprise edition includes a global latency setting.
Built-in WAN Acceleration		✔	✔	✔	Get replicas and backup copy jobs off site up to 50x faster and save bandwidth.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3458

✓ Fully supported ✓ Partially supported

Backup and Recovery *Powered by Veeam* *Backup & Replication*	**Veeam Data Platform** **Veeam Universal License (VUL)**			**Description**
	Community	**Foundation**	**Advanced**	**Premium**	
Backup from Storage Snapshots		✓	✓	✓	Create image-based backups and replicas as often as necessary with little to no impact on production from the world's leading storage providers for backups from primary and secondary storage snapshots. This includes a growing list of storage alliance and ecosystem partners.
Cloud Backup & Recovery					
AWS Backup & Recovery	✓	✓	✓	✓	Native protection for Amazon EC2, Amazon RDS, Amazon Aurora, Amazon DynamoDB, Amazon S3, Amazon VPC data, Amazon FSx, and Amazon Redshift. Full instance and granular restore options available in-place or as-new to the same or different account or region. Backup, restore, and migration out of AWS options include to on-premises, Microsoft Azure, and Google Cloud.
Azure Backup & Recovery	✓	✓	✓	✓	Native protection for Azure VMs, Azure SQL, Azure Files, Azure Blob, and Azure Cosmos DB. Full instance and granular restore options available in-place or as-new to the same or different subscription or region. Backup, restore, and migration out of Azure options include to on-premises, AWS, and Google Cloud.
Google Cloud Backup & Recovery	✓	✓	✓	✓	Native protection for Compute Engine VMs, Cloud SQL for MySQL, and PostgreSQL and Cloud Spanner. Full instance and granular restore options available in-place or as-new to the same or different project or region. Backup, restore, and migrate out of Google Cloud options include to on-premises, AWS, and Microsoft Azure.
Cost Control	✓	✓	✓	✓	Optimize and control cloud spend while meeting service-level, retention, and compliance objectives. Cost control measures include backup compression, tiering to archival object storage classes, dynamic compute resourcing, proactive cost forecasting, and capacity planning.
Cloud Security	✓	✓	✓	✓	Secure backup data in line with best practices and well-architected frameworks. Security measures include logical air-gapping of backups, least privilege access through identity and access management, integration with cloud-provided encryption and key management services, and immutability.
Enterprise App Backup Plugins					
Veeam Plug-in *for SAP HANA* on IBM Power		✓	✓	✓	Eliminate the need for multiple backup solutions in your data center with the new, fully certified powerful plug-in for SAP HANA running on IBM Power.
Veeam Plug-in *for IBM Db2* (Intel Linux + IBM AIX + IBM Power)		✓	✓	✓	Protect IBM Db2 databases running on Intel Linux, IBM AIX, or IBM Power. Supports standalone instances as well as high availability disaster recovery (HADR).

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3459

✓ Fully supported ✓ Partially supported

Backup and Recovery *Powered by Veeam Backup & Replication*	**Veeam Data Platform Veeam Universal License (VUL)**			**Description**
	Community	**Foundation**	**Advanced**	**Premium**	
Veeam Plug-in *for Oracle RMAN, SAP HANA* and SAP on Oracle		✓	✓	✓	Stream Oracle RMAN, SAP HANA, and SAP on Oracle backups into Veeam repositories and recover with ease, leveraging native backup and restore capabilities. Enterprise plug-ins can be deployed to Linux, AIX, Solaris and Microsoft Windows operating systems. Include central management on Windows and Linux.
Veeam Plug-in *for Microsoft SQL*		✓	✓	✓	Enable native Microsoft SQL Server backups directly to Veeam storage repositories. Integration with Microsoft SQL Server Management Studio simplifies backup and recovery administration tasks.
Storing Backups					
Veeam Data Cloud Vault	✓	✓	✓	✓	Gain instant access to secure, predictably priced cloud object storage with Veeam Data Cloud Vault, completely integrated with Veeam Data Platform.
Object storage	✓	✓	✓	✓	Directly backup to any object storage on-premises or in the public cloud with ransomware protection immutibility provided by storage vendors. Community Edition supports recovery from object storage only.
Linux Hardened Repository	✓	✓	✓	✓	Keep your backups safe in hardened, malware- and hacker-proof Linux repositories, with immutable backups preventing encryption and deletion by ransomware and malicious actors.
Veeam Cloud Connect Backup		✓	✓	✓	Get your backups off-site with fully integrated, fast and secure backup, and restore to the cloud with one of our Veeam-powered service providers. This built-in capability makes it easy to establish a connection with a Cloud Repository, target the repository for Backup Jobs, and even backup directly to the cloud.
VMware Cloud Director Backup	✓	✓	✓	✓	Backup vApp and VM metadata and attributes and restore vApps and VMs directly to vCloud with full support for fast provisioned VMs. All editions include integrated visibility of vCloud Director infrastructure, backup via VeeamZIP (including backup of vApp and VM metadata and attributes) and direct restore to vCloud. Community Edition does not include the following: support for scheduled incremental backup jobs of vCloud VMs, customer portal integrations via RESTful API, self-service, tenant-managed backup and restore via enterprise manager, as well as native vCloud Director authentication
Scale-out Backup Repository (SOBR) with object storage support		✓	✓	✓	Provide an abstraction layer across individual storage devices to create a single virtual pool of backup storage for your backups, with Performance, Capacity, and Archive Tiers automating management for the entire backup lifecycle. VUL has no limitations on the number of repositories or extents.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3460

✓ Fully supported ✓ Partially supported

Backup and Recovery *Powered by Veeam Backup & Replication*	**Veeam Data Platform Veeam Universal License (VUL)**				**Description**
	Community	**Foundation**	**Advanced**	**Premium**	
SOBR Capacity Tier		✓	✓	✓	Leverage native object storage integration with AWS, Microsoft Azure, IBM Cloud, Google Cloud Storage, and most S3-compatible object storage offerings for on-premises or cloud-based repositories. Protect your backups against malicious actors with S3 Object Lock based immutability. Other capabilities include the ability to move inactive backup chains to the capacity extent, copy new backup files, move data from capacity extent back to performance extents and restore data from capacity tier without creating a new SOBR.
SOBR Archive Tier		✓	✓	✓	Reduce the costs of long-term data archival and retention by up to 20 times and replace manual tape management with native support for Amazon S3 Glacier (including Glacier Deep Archive) and Microsoft Azure Archive Storage through end-to-end backup life cycle management.
S3-compatible object storage with data archiving enabled		✓	✓	✓	Move GFS restore points. Increase cost savings with tape via Smart Object Storage API for Amazon S3 Glacier compatible systems.
Health check for Capacity Tier		✓	✓	✓	Health Check proactively verifies the existence of objects via API calls. Object storage vendors usually provides 11 nines durability. Health check enabled per default (new installations).
Per-VM backup files	✓	✓	✓	✓	Store each VM in a separate backup file to enhance backup performance when backing up to enterprise-grade storage and deduplicating storage appliances. This is accomplished by leveraging parallel VM processing to enable multiple, concurrent write streams.
Move and Copy backup files		✓	✓	✓	Move or copy backup files across multiple jobs or repositories to easily achieve the desired RPO, rebalance backup storage or manage migration scenarios.
Native tape support	✓	✓	✓	✓	Backup files to any LTO-compatible tape devices. Backup to Tape jobs provide tighter integration with primary backup jobs, dedicated media pool type to simplify GFS retention and global media pools to simplify the usage of multiple tape devices. NDMP support for NAS device protection. VUL or Capacity Packs are required for File to Tape jobs. Community Edition only supports File to Tape jobs.
IBM Jaguar tape support		✓	✓	✓	Reduce costs without compromising on security by combining Veeam's air gapped data protection with low-cost storage at enterprise scale using IBM Jaguar drives.
Veeam External Repository		✓	✓	✓	Connect to object storage repositories managed by cloud-native Veeam backups, offering to perform restores from those backups, or copy them out of the cloud to achieve the 3-2-1 rule compliance.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3461

✓ Fully supported ✓ Partially supported

Backup and Recovery *Powered by Veeam Backup & Replication*	**Veeam Data Platform Veeam Universal License (VUL)**				**Description**
	Community	**Foundation**	**Advanced**	**Premium**	
File versions archiving		✓	✓	✓	Archive all or only specific file versions for a longer period of time with file share backup jobs.
NetApp ONTAP FlexGroups support	✓	✓	✓	✓	Backup and recover large volumes on NetApp ONTAP FlexGroups ensuring that your data stays protected at scale.
Support for primary snapshot immutability for HPE 3PAR/ Primera/Alletra		✓	✓	✓	Support for creating immutable snapshots on HPE 3PAR/Primera/Alletra arrays by leveraging the native Virtual Lock functionality. A valid Virtual Lock license is required.
HPE StoreOnce Catalyst Copy target immutability support		✓	✓	✓	Persist backup immutability and retention (GFS) using native APIs for HPE StoreOnce Catalyst Copy.
Snapshots for FlashCopies in IBM FlashSystem & SAN volume controller	✓	✓	✓	✓	Support for Volume Groups Snapshots (requires IBM Spectrum Virtualize 8.5.1 or newer).
Immutability for Dell Data Domain with support of DD-native Retention Lock		✓	✓	✓	Persist backup immutability when using Data Domain Retention Lock.
Smart Load balancing support for Isilon and NetApp		✓	✓	✓	Ability to automatically discover the cluster node that should be used during processing whenever source storage is a cluster with multiple nodes.
De-duplicating storage appliance integration		✓	✓	✓	Get faster backup performance by backing up to deduplicating storage integrations (Dell Data Domain Boost, HPE StoreOnce Catalyst, Quantum DXi, and ExaGrid Accelerated Data Mover).
Replication					
New Universal CDP		✓	✓	✓	Universal CDP delivers continuous data protection for any Windows machine, physical, virtual, or cloud, replicating directly to VMware vSphere or to VMware Cloud Director via Veeam Cloud Connect.
Veeam CDP (Continuous Data Protection)		✓	✓	✓	Eliminate downtime and minimize data loss for Tier-1 VMware vSphere and Cloud Director workloads with built-in CDP and achieve immediate recoveries to a latest state or desired point in time providing the best recovery point objectives (RPOs).

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3462

✓ Fully supported ✓ Partially supported

Backup and Recovery *Powered by Veeam Backup & Replication*	**Veeam Data Platform Veeam Universal License (VUL)**				**Description**
	Community	**Foundation**	**Advanced**	**Premium**	
SureReplica for CDP		✓	✓	✓	Ensure disaster recovery really works. Replication continues during failover tests. Failover, antivirus, YARA scan, and CRC check. Comprehensive reporting in Veeam Recovery Orchestrator.
File and application-level restore from CDP replica		✓	✓	✓	Recover files from CDP replica from any restore point. File-level recovery is possible from all restore points available. Replication continues in the background while restore happens.
Planned failover with CDP replicas		✓	✓	✓	Verified and orchestrated recovery for when you need to failover without disrupting workloads.
Image-based VM replication	✓	✓	✓	✓	Replicate VMs periodically on site for high availability or off site for DR.
Assisted failover and failback	✓	✓	✓	✓	Replica rollback and assisted failover and failback.
Replication from a backup	✓	✓	✓	✓	Create replicas directly from backup files without impacting production.
Veeam Cloud Connect Replication		✓	✓	✓	Ensure availability of your mission-critical applications with fully integrated, fast, and secure cloud-based DR through a Veeam-powered Disaster Recovery as a Service (DRaaS) provider. In the event of disaster or other use case, replicas stored in the repository can be used for partial- or full-site failover.
One-click failover orchestration		✓	✓	✓	Built-in failover plan orchestration enabling easy, one-click site failover to minimize unplanned downtime.
VMware Cloud Director Replication		✓	✓	✓	Dedicated replication job type enables service providers to perform vApp replication within and across vCloud Director instances. The replication job processes vApp VMs and metadata (such as networking or VM start order) to create a ready-to-use replica vApp in the target vCloud Director that can be leveraged instantly in case of a disaster.
Restore					
Entire VM restore	✓	✓	✓	✓	Restore selected VMs to the original or a new location.
VM disks and files restore	✓	✓	✓	✓	Restore individual virtual disks and other VM files (such as VMX) from both backups and storage snapshots.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3463

✔ Fully supported ✔ Partially supported

Backup and Recovery *Powered by Veeam Backup & Replication*	**Veeam Data Platform Veeam Universal License (VUL)**				**Description**
	Community	**Foundation**	**Advanced**	**Premium**	
Direct Restore *to AWS*, Azure, and Google Cloud	✔	✔	✔	✔	Restore or migrate on-premises, Windows-based or Linux-based VMs, physical servers and endpoints directly to AWS, Microsoft Azure, and Google Cloud.
Instant Recovery					
New Instant Recovery to Microsoft Azure	✔	✔	✔	✔	Instant Recovery to Azure restores VMware and Hyper-V VMs, Windows/Linux machines, Nutanix AHV VMs, and Amazon EC2 instances from Veeam Data Cloud Vault as Azure VMs in moments for rapid disaster recovery.
Instant VM Recovery	✔	✔	✔	✔	Accelerate DR and lower RTOs with Veeam's patented Instant Recovery engine. Restore ANY backup instantly to a VMware, Microsoft Hyper-V, or Nutanix AHV VM by running it directly from backup.
Instant disk recovery	✔	✔	✔	✔	Reduce your Instant Recovery footprint by instantly restoring only the required disks of large vSphere VMs, as opposed to restoring the entire VM (e.g., only OS disk, or only data disks).
Instant database recovery		✔	✔	✔	Instantly recover any Microsoft SQL Server and Oracle database from backup to the latest state or to an earlier point-in-time to any production database server or cluster (physical or virtual) in minutes regardless of its size.
Instant file share recovery	✔	✔	✔	✔	Instantly restore SMB file shares directly from backups to allow users to continue day-to-day operations quickly, and easily migrate all changes made to the SMB share to production. For NFS file shares, leverage the publishing functionality to provide read-only access to the data stored in the backup.
Instant disk publish	✔	✔	✔	✔	Empower application owners to quickly locate the data they need for operations and recovery, combining high-performance search with a disk published directly from backup.
File & Item-level Recovery					
File-level Recovery	✔	✔	✔	✔	Directly recover files from Windows, Linux, BSD, macOS, Novell, Solaris and AIX.
Compare with production	✔	✔	✔	✔	Easily compare files from backups with the production file system to view and recover only changed files. Available for image-level backups only. Community Edition and Standard can compare and view only. VUL, Enterprise and Enterprise PLUS can compare, view, and restore to production.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3464

✓ Fully supported ✓ Partially supported

Backup and Recovery *Powered by Veeam Backup & Replication*	**Veeam Data Platform Veeam Universal License (VUL)**				**Description**
	Community	**Foundation**	**Advanced**	**Premium**	
Permissions recovery		✓	✓	✓	Restore lost or modified permissions to an exisiting file. Available for image-level Windows backups.
Veeam Explorer *for MongoDB*		✓	✓	✓	Streamlined granular recovery of MongoDB collections, databases and instances without requiring a substantial MonogoDB skillset.
Veeam Explorer *for SAP HANA*		✓	✓	✓	Restore a single database or several databases from SAP HANA plug-in backups with ease to the original or to a different location to any point in time and customize restore options.
Veeam Explorer *for PostgreSQL:* Export DB	✓	✓	✓	✓	Export specific PostgreSQL databases in the native dump format directly from backup or from the published PostgreSQL instance.
Veeam Explorer *for Storage Snapshots*	✓	✓	✓	✓	Restore individual VMs, guest files and application items from storage snapshots.
Veeam Explorer *for PostgreSQL*	✓	✓	✓	✓	Restore and publish PostgreSQL instances to the original or to a new server with ease, without extensive PostgreSQL administration background.
Veeam Explorer *for Microsoft Active Directory*	✓	✓	✓	✓	Search and restore for all Active Directory (AD) object types, such as users, groups, computer accounts and contacts, including user and computer password recovery. All editions support single user and computer account restore (including the ability to restore passwords) as well as export into LDIFDE format. Community Edition does not allow multi-select restore and container restore, Group Policy Objects (GPO) restore, AD-integrated DNS records restore, and Configuration Partition objects restore.
Veeam Explorer *for Microsoft Exchange*	✓	✓	✓	✓	Get instant visibility into Microsoft Exchange backups for item recovery of individual Exchange items (emails, appointments, notes, contacts, etc .), online archive mailboxes and hard-deleted items. Leverage comprehensive e-Discovery functionality, including query result size estimation and detailed export reports. Community Edition does not support restoring back to the original mailbox.
Veeam Explorer *for Microsoft SQL Server*	✓	✓	✓	✓	Restore individual SQL databases with ease, without needing an extensive SQL background or having to search for database and transaction-log files. All editions support local, point-in-time SQL database file restores. However Community Edition does not include agentless, transaction log backup and replay, transaction-level recovery of databases and SQL objects (tables, stored procedures, views, etc.) back to the original or new SQL Server.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3465

✓ Fully supported ✓ Partially supported

Backup and Recovery *Powered by Veeam Backup & Replication*	**Veeam Data Platform Veeam Universal License (VUL)**				**Description**
	Community	**Foundation**	**Advanced**	**Premium**	
Veeam Explorer *for Microsoft SharePoint*	✓	✓	✓	✓	Get instant visibility into SharePoint backups with advanced search-and-browse capabilities for quick recovery of individual SharePoint items and entire sites. All editions support SharePoint item restore via save, send, and export. However, Community Edition does not support entire-site restore, as well as restore to the original location.
Veeam Explorer *for PostgreSQL*: Instant Recovery		✓	✓	✓	Provide instant availability to PostgreSQL directly from your backup, without compromise with background data recovery and journaling.
Guest file system indexing	✓	✓	✓	✓	A catalog of guest files enabling effortless search of individual files to find and restore a file without knowing its precise location, or the time when it was deleted. All editions provide a catalog of guest files in backups currently on disk. Community Edition does not provide a catalog of archived backup files or integrate with one-click to enable restores directly from search results.
Veeam Explorer *for Oracle*		✓	✓	✓	Restore individual Oracle databases with ease without needing an extensive Oracle background or having to search for database and transaction-log files. Includes agentless, transaction-log backup, archived log management, and transaction-level recovery of databases back to the original or new Oracle Server, as well as the ability to publish and export Oracle databases.
DataLabs					
Secure Restore		✓	✓	✓	Increase security and reduce interruptions caused by viruses and recover back to a safe, uncompromised restore point through an optional antivirus scan directly in backup files prior to recovery; agnostic support for Windows Defender, ESET, Kaspersky, and Symantec Protection Engine, as well as the ability to extend to other third-party antivirus tools. YARA scan not available in Community and Foundation.
SureBackup[2]		✓	✓	✓	Automatically test and verify recoverability of every backup by running the VM directly from a backup file in a fenced-off copy of your production environment, including support for custom application test scripts. YARA scans are not available in Community Edition and Foundation.
SureReplica[1]		✓	✓	✓	Automatically test and verify recoverability of every replica by performing a failover to a fenced- off copy of your production environment, including support for custom application test scripts.
Staged Restore		✓	✓	✓	Clean up sensitive data from the selected restore point in a fenced-off copy of your production environment before restoring the modified VM state to production.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3466

✔ Fully supported ✔ Partially supported

Backup and Recovery *Powered by Veeam Backup & Replication*	**Veeam Data Platform Veeam Universal License (VUL)**			**Description**
	Community	**Foundation**	**Advanced**	**Premium**	
On-Demand Sandbox		✔	✔	✔	Run one or more VMs directly from a backup a fenced-off copy of your production environment to troubleshoot issues, test upgrades, train staff on a working copy of the production environment, without impacting business operations.
On-Demand Sandbox from Storage Snapshots[1]		✔	✔	✔	Use storage snapshots to quickly create fenced-off copies of your production environment operating at full I/O performance.
Data Integration API		✔	✔	✔	Mount your backups instantly everywhere. Put your backups to work and reuse your data by enabling third-party applications and scripts to instantly access the content of any Veeam backup for data mining, security analysis, compliance checks, and other data reuse scenarios.
Self-service					
New Enhanced Role-Based Access Control (RBAC)		✔	✔	✔	Enhanced Role-Based Access Control (RBAC) provides granular, security-focused delegation of administrative tasks and access rights. RBAC allows organizations to define and manage who can access specific features, data, or resources within the Veeam environment, significantly enhancing security, compliance, and operational efficiency.
One-click file and VM recovery portal for help desk operators		✔	✔	✔	Restore files, VMs, or the entire vApp with a single click through a web UI.
Microsoft Exchange item recovery portal for help desk operators		✔	✔	✔	Restore missing mailbox items back to the original mailbox with a single click through a web UI.
Microsoft SQL Server database recovery portal for Microsoft SQL Server databases		✔	✔	✔	Restore individual databases back to the original server or a new SQL server with a single click through a web UI.
Oracle database recovery portal for Oracle databases		✔	✔	✔	Restore Oracle databases to the original server, a new Oracle server or PostgreSQL with a single click through a web UI.
Self-service file restore portal		✔	✔	✔	File-restore portal with automatic VM detection and automatic delegation based on the Local Administrator group membership.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3467

✓ Fully supported ✓ Partially supported

Backup and Recovery *Powered by Veeam Backup & Replication*	**Veeam Data Platform** **Veeam Universal License (VUL)**			**Description**
	Community	**Foundation**	**Advanced**	**Premium**	
Recovery delegation		✓	✓	✓	Enable full self-service for all web UI recovery features by delegating recoveries for individual VMs and groups of VMs to specific users or groups such as local IT staff, application owners, department members, etc.
Native VMware Cloud Director plug-in		✓	✓	✓	This capability allows service providers to extend the vCloud Director tenant UI to include Veeam Backup & Replication functionality, enabling tenants to manage their own backups and restores without leaving the convenience of the vCloud Director web console. This integration is based on Veeam's existing vCloud Director Self-Service Backup & Restore Portal.
Deployment					
Windows Installer	✓	✓	✓	✓	Installable software packages that are fully compatible with supported versions of Microsoft Windows enables straightforward deployment through familiar Windows installation processes. Can be installed either using a graphical user interface or by command-line for unattended (silent) installations. The software is available for all editions of Veeam Data Platform, allowing users to operate with essential backup and recovery features for even the smallest environments.
New Veeam Software Appliance (ISO)		✓	✓	✓	Pre-packaged, bootable installation image (ISO file) that includes a lightweight, secure-by-default Linux-based operating system (JeOS) and the Veeam Backup & Replication software to streamline the deployment process by bundling the required Operating System and Veeam components into a single installation. This reduces setup complexity and provides a consistent deployment experience. Essentials license holders cannot license an ISO based deployment.
New Veeam Software Appliance VMware Template (OVA)		✓	✓	✓	Pre-configured, ready-to-deploy virtual machine image distributed in the Open Virtual Appliance (OVA) format that includes a lightweight, secure-by-default Linux-based operating system (JeOS) and the Veeam Backup & Replication software to streamline the deployment process by bundling the required Operating System and Veeam components into a single installation. This reduces setup complexity and provides a consistent deployment experience.
New JeOS image for infrastructure components	✓	✓	✓	✓	The Veeam JeOS (Just Enough Operating System) image is a minimal, purpose-built Linux-based operating system bundled with Veeam software, designed to streamline the deployment and management of backup infrastructure components. This image is intended for roles such as backup proxies, repositories (including the Veeam Hardened Repository), mount servers, and gateways within the Veeam Backup & Replication architecture.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

✓ Fully supported ✓ Partially supported

Backup and Recovery *Powered by Veeam Backup & Replication*	**Veeam Data Platform** **Veeam Universal License (VUL)**			**Description**
	Community	**Foundation**	**Advanced**	**Premium**	
Management					
New Web UI		✓	✓	✓	Experience the power of the Web UI with an intuitive yet familiar interface, advanced filtering, and search tools to streamline your data protection management.
New High Availability				✓	Achieve continuous availability with built-in redundancy and failover, ensuring critical workloads stay resilient and operational at all times. Available only on the Veeam Software Appliance.
Veeam Backup Enterprise Manager: Centralized Management Web UI		✓	✓	✓	Access a web-based, consolidated view of your distributed deployment in a single pane of glass including centralized monitoring, reporting, consolidated alerting across multiple backup servers, and the ability to start and stop jobs. Additionally, full job management functionality and the ability to perform restores, including Instant Restore for VMware, Hyper-V, NAS backups as well as Migrate to Production.
PowerShell module	✓	✓	✓	✓	Use PowerShell Cmdlets to create custom workflows and automate Veeam tasks.
RESTful API		✓	✓	✓	Integrate into existing systems and execute and automate Veeam tasks using the RESTful API framework. Service Providers using rental licenses have API access across all editions.
Built-in management for Veeam Agents	✓	✓	✓	✓	The ability to organize, automate, and deploy Windows, Linux, Mac, AIX and Solaris agents with protection groups based on Active Directory containers, CSV files, or public cloud tags to configure custom automatic update and deployment schedules. Community Edition is limited to 10 instances.
Built-in management for Veeam Plug-ins		✓	✓	✓	Simplify operations with centralized management capabilities to organize, automate, and deploy Oracle RMAN, SAP HANA and SAP on Oracle database plug-ins including creation of application backup policies.
Infrastructure assessment: Veeam Backup & Replication		✓	✓	✓	Assessment reporting is designed to verify that your Veeam Backup & Replication installation meets all known best practices.

[1] VMware only [2] VMware and Hyper-V only

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3469

✓ Fully supported ✓ Partially supported

Monitoring and Analytics *Powered by Veeam ONE*	Veeam Data Platform			Description
	Community	Advanced	Premium	
Monitoring and Reporting				
Enhanced Veeam Threat Center dashboard	✓	✓	✓	Highlight threats, identify risks, and measure the security score of your environment from one dashboard. Centralized analytics for the entire platform.
New High Availability Health Monitoring			✓	Veeam ONE provides real-time High Availability health monitoring with remediation options and alerts to ensure continuous protection for critical workloads.
New Integration with Coveware Recon Scanner			✓	Veeam ONE surfaces Recon Scanner intel in Threat Center to deliver proactive threat visibility and integrated adversary intelligence, strengthening the security posture across Veeam Data Platform.
Enhanced Flexible and Customizable Report Generation		✓	✓	Generate lightning-fast, customizable reports at scale with PostgreSQL-powered performance, HTML5 interactivity, and executive-ready exports.
Protected Databases Reporting		✓	✓	Track database backup health, alerts, and compliance with real-time visibility across dashboards, inventory, and reports. Integrated for scalable monitoring.
ServiceNow integration	✓	✓	✓	Bi-directional Incident lifecycle with ServiceNow. Backup anomalies are instantly reported into ServiceNow so you can immediately perform triage and reduce further risk to your data.
Platform Reporting	✓	✓	✓	Complete monitoring, reporting, and alarming for new functionality, including: Backup of Object Storage, Malware Detection Engine and Security & Compliance Analyzer.
Performance monitoring and alerting for backup activity	✓	✓	✓	Performance monitoring and alerting for backup activity displays Veeam Backup & Replication jobs, including their latest state and performance statistics. Veeam ONE has no limitations on the number of Veeam Backup & Replication servers that can be monitored. Note that Veeam ONE *Community Edition* is limited to one server.
Email notification and reports		✓	✓	You can receive alarm notifications through a customizable email. Email customizations are not available in Veeam ONE *Community Edition*, and emails will not include all alarm details, such as time and affected object.
Veeam Backup *for Nutanix AHV*	✓	✓	✓	Support for Veeam Backup *for Nutanix AHV* includes several alarms and reports that help you analyze trends and determine how policies and backup jobs have evolved, as well as determine the backup status of Nutanix VMs. This helps users in verifying the data protection status for each discovered VM based on the agreed service level agreement (SLA).

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3470

✔ Fully supported ✔ Partially supported

Monitoring and Analytics *Powered by Veeam ONE*	**Veeam Data Platform**			**Description**
	Community	**Advanced**	**Premium**	
Veeam Backup for Proxmox VE and oVirt KVM	✔	✔	✔	Support for Veeam Backup for Proxmox VE and oVirt KVM includes several alarms and reports that help you analyze trends and determine how policies and backup jobs have evolved, as well as determine the backup status of workloads running on these environments. This helps users in verifying the data protection status for each discovered VM based on the agreed service level agreement (SLA).
Veeam Agent monitoring and reporting	✔	✔	✔	Support for Veeam backup agents includes several alarms and reports that help you analyze trends and determine how policies and backup jobs have evolved, as well as determine the backup status of agents, including which agents have no backup copies and how many are protected or unprotected. This is given with the backup state along with the total number of successes, warnings, and failures.
Veeam Cloud Connect reporting	✔	✔	✔	Reports include information about the Veeam Cloud Connect infrastructure, like user quota usage, capacity planning for cloud repositories and configuration data for cloud gateways and repositories.
Performance monitoring and alerting for Veeam Cloud Connect	✔	✔	✔	Performance monitoring and alerting for Veeam Cloud Connect displays jobs for Veeam Cloud Connect backup servers only, including their latest state and performance statistics. Note: To monitor and report on managed clients, Veeam ONE needs to be deployed at the tenant's site. Veeam ONE *Community Edition* is limited to one week of performance.
Heatmaps	✔	✔	✔	Heatmaps help plan resource usage and easily optimize backup activities with real-time visibility into backup repositories and proxies. Veeam ONE *Community Edition* is limited to three proxy servers and three repositories.
Monitoring and Alerting for Hybrid Cloud				
Veeam Backup *for AWS*, Veeam Backup *for Microsoft Azure*, and Veeam Backup *for Google Cloud* — native data protection support	✔	✔	✔	Monitoring and alerting: Veeam ONE users can now monitor the backup and snapshot job statuses of cloud-based workloads through predefined alarms and notifications. Backup status reporting: A predefined protected VMs report now includes VMs that are hosted in AWS, Microsoft Azure, and Google Cloud Platform public clouds. This helps users in verifying the data protection status of each discovered VM, based on the agreed service level agreement (SLA).
Reporting	✔	✔	✔	Get detailed visibility of protected and unprotected services from your Public Cloud. Supports AWS (EC2, RDS, EFS, VPC, FSx, Redshift Clusters, Redshift Serverless, DynamoDB), Microsoft Azure (Virtual Machines, SQL Database, Azure Files, Azure Virtual Network, CosmoDB), and Google Cloud Platform (Compute Engine, Cloud SQL, Cloud Spanner).

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3471

✓ Fully supported ✓ Partially supported

Monitoring and Analytics *Powered by Veeam ONE*	**Veeam Data Platform**			**Description**
	Community	**Advanced**	**Premium**	
Alarms for Real-time Data Protection Visibility	✓	✓	✓	For Veeam ONE Client protected cloud workloads Virtual Machines, Databases, VPC, and File Shares. Additionally, to the last backup status and date, the last Backup Copy and Last Archive have been introduced for full data retention visibility.
Monitoring and Alerting for Virtual Infrastructure				
Performance monitoring and alerting for virtual infrastructures	✓	✓	✓	Display virtual infrastructure hosts, datastores, and statistics. In Veeam ONE *Community Edition*, performance graphs only show one week of performance and emails include limited alarm details.
Application-level monitoring and management	✓	✓	✓	Ensure the availability of mission-critical applications, monitor select groups of applications, and create additional alarms to monitor VM service states. Make sure processes aren't exceeding available resources, identify if critical applications, like antivirus software, have been disabled, or indicate if unwanted changes have taken place. With Veeam ONE *Community Edition*, you can monitor an unlimited number of applications on up to three VMs.
VMware vSphere and Microsoft Hyper-V reporting	✓	✓	✓	Individual report packs for vSphere and Hyper-V provide general configuration overviews for vCenter servers, datastores, clusters hosts and VMs, as well as SCVMMs, volumes, clusters, hosts, and VMs, including information on the most common alarms raised for virtual infrastructure objects. Optimization report packs also allow users to evaluate the efficiency of resource usage and to optimize VM resource provisioning to help achieve improved output and increased ROI for virtualized environments. With Veeam ONE *Community Edition*, optimization reports are limited to show only three VMs and historical performance reports are limited to the last 24 hours of data.
Multi-tenant reporting and monitoring	✓	✓	✓	Delegate reporting to system administrators over a limited scope of assigned VMs (VMware vSphere only).
Infrastructure assessment: Veeam Backup & Replication	✓	✓	✓	Assessment reporting is designed to verify that your Veeam Backup & Replication installation meets all known best practices.
Virtual infrastructure assessment	✓	✓	✓	Assessment reporting is designed to verify that your VMware vSphere and/or Microsoft Hyper-V infrastructure meets all known best practices.
VMware Cloud Director monitoring and alerting	✓	✓	✓	Companies want to stay ahead of the issues impacting their virtual datacenters and ultimately their customers. To help, Veeam provides capabilities for monitoring teams of service providers to track the availability and configuration of their virtual data centers, including organizations and vApps.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3472

✓ Fully supported ✓ Partially supported

Monitoring and Analytics *Powered by Veeam ONE*	Veeam Data Platform			Description
	Community	Advanced	Premium	
VMware Cloud Director reporting	✓	✓	✓	Businesses want to ensure that they are using the ideal configuration and optimizing their resources to get the most out of their virtual infrastructure when building and maintaining virtual data centers to provide a reliable service to their customers.
Report and Alarm Customization and Automation				
Raw data analysis		✓	✓	Create custom Microsoft Excel reports using templates you define.
Customizable, predefined report templates	✓	✓	✓	Customize and save predefined report templates to create reports that fit your specific information and formatting needs. Veeam ONE *Community Edition* is limited to saving one customized report template.
Alarm customization and modelling	✓	✓	✓	Ensure complete monitoring coverage by creating custom alarms for events unique to your virtual environment. Model alarms against past performance data to understand potential alarm frequency and avoid inadvertent alert storms and missed events.
Governance and Compliance				
Business view	✓	✓	✓	Categorize and group clusters, hosts, VMs, and datastores by criteria such as business unit, department, purpose and SLA. Leverage VMware Tags to assist with role-based access control and eliminate human error, including tagging sensitive data by location to meet compliance. Easily monitor apps, regardless of geographic location and categorize business view objects based on multiple parameters to gather insight on how infrastructure investments are being leveraged. You also can assign administrators to manage specific parameters.
Intelligent Automation				
Veeam Intelligent Diagnostics	✓	✓	✓	Proactive identification and alerting of known issues within your Veeam environment, providing self-support resolutions via hotfixes or reconfigurations. For Veeam ONE *Community Edition*, all of the alarms will continue to work but the details for each alarm will not be shown.
Remediation actions	✓	✓	✓	Predefined and automated resolution of common backup and virtual infrastructure-related issues with self-healing remediation actions help to reduce IT management costs. With Veeam ONE *Community Edition*, remediation actions are available, but require manual approval.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3473

✓ Fully supported ✓ Partially supported

Monitoring and Analytics *Powered by Veeam ONE*	Veeam Data Platform			Description
	Community	Advanced	Premium	
Dashboards				
Predefined performance dashboards for backup and virtual infrastructures and Veeam Backup *for Microsoft 365*	✓	✓	✓	Get at-a-glance views of backup jobs and the backup infrastructure, as well as view the VMs, hosts, and clusters that are the highest consumers of CPU, memory, network, and datastore resources. Also, view datastore utilization metrics, including metrics relating to VM snapshots and guest disk space usage.
Customized reporting dashboards	✓	✓	✓	Create your own at-a-glance views of your virtual environment. Veeam ONE *Community Edition* allows for one customized reporting dashboard to be created.
Capacity Planning				
Capacity planning: VMware vSphere and Microsoft Hyper-V		✓	✓	Individual report packs for VMware vSphere and Microsoft Hyper-V are designed to forecast when the available virtual infrastructure resources will reach their minimum levels. The packs provide recommendations on resource allocation and load balancing to optimize performance and resource utilization in your respective virtual environment and to avoid possible performance bottlenecks.
Deployment project reports		✓	✓	Leverage fully automated "what-if" modeling scenarios to safely add or remove VMs or hosts from your infrastructure and to accurately calculate the required resources needed for each project.
Chargeback and Billing				
Chargeback analysis reports		✓	✓	Chargeback reports help you understand the costs associated with individual virtual infrastructure users, as well as help you perform chargeback by analyzing VM configuration and resource usage, including CPU, memory, and storage. Four reports are included: Host Configuration Chargeback, Host Resource Usage Chargeback, VM Configuration Chargeback, and VM Performance Chargeback.
Veeam backup: Billing	✓	✓	✓	This report provides chargeback capabilities for Veeam Backup & Replication and helps assess storage management costs for backup and replication operations, providing data that can be used in financial and billing reports.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3474

✔ Fully supported ✔ Partially supported

Recovery Orchestration *Powered by Veeam Recovery Orchestrator*	**Veeam Data Platform** Premium	**Description**
Recovery Orchestration & Automation		
Orchestration for Microsoft Hyper-V and Azure Local (Azure Stack HCI)	✔	Recover from Hyper-V backups to Hyper-V environments. Migrate from VMware to Hyper-V and build out a recovery plan for Hyper-V backups. Take your existing VMware plan, point it to your new Hyper-V environment and run the plan. Orchestration for Hyper-v and Azure Local (Azure Stack HCI) delivers end-to-end cross-platform orchestrated recovery and planned migration with zero data loss configuration.
Orchestration for VMware vSphere	✔	Recover backups from VMware to secondary VMware locations, or migrate VMware VMs to another platform including Hyper-V, Azure Local, Or Microsoft Azure VMs. Orchestration for VMware delivers end-to-end cross-platform orchestrated recovery and planned migration with zero data loss configuration.
Orchestration for Veeam Agents (Windows/Linux)	✔	Recover Veeam Agent Backups of Windows and Linux to VMware or Microsoft Azure environments.
Orchestration of Storage Snapshots	✔	Orchestrate workflows for machines running in vSphere but hosted on Storage Arrays including HPE Alletra MP B10000, NetApp, Lenovo. Failover vSphere VMs and their datastores backed by HPE Alletra MP.
Multi Factor Authentication (MFA)	✔	Multi-factor authentication secures recovery plan execution and approval by requiring multiple identity factors, ensuring compliance and preventing unauthorized actions.
Offline malware scanning for Recovery Plans	✔	On-demand and scheduled malware detection, including malware flag check, antivirus scan, and YARA scan.
Veeam Software Appliance support	✔	Orchestration for the new Veeam Software Appliance deployment models, including support for Veeam Software Appliance High-Availability Cluster.
YARA Rule Management	✔	YARA rule files can be imported to VRO allowing for increased security, manageability, and visibility. Control rule assignments to different groups using VRO scopes and preview YARA rule contents in VRO UI, allowing for version control and other checks. With automated distribution, YARA files are securely delivered to Veeam Backup servers, used for scanning, and then removed.
Support for additional repositories	✔	Recovery from Veeam Data Cloud Vault and S3 repositories — AWS, Wasabi, on-premises S3.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

✔ Fully supported ✔ Partially supported

Recovery Orchestration *Powered by Veeam Recovery Orchestrator*	**Veeam Data Platform**	**Description**
	Premium	
Automated Clean Recovery	✔	Restore points that have been marked as Clean during backup accelerate orchestrated recovery of an entire environment using malware-free restore points.
Testing for CDP replica plans	✔	CDP replica testing with zero-impact on production or replication. Fully-featured tests, heartbeat checks, network tests, and custom scrips with all VRO reporting features enabled.
In-guest scripts for Azure	✔	Reduce downtime and eliminate manual tasks when recovering an on-prem workload into Microsoft Azure by orchestrating post-recovery OS configuration and validation. Inject custom scripts into Azure VMs recovered from agent or vSphere backups with all script output captured in VRO reports.
One-Click Mass Recovery	✔	Enable application owners to securely recover single apps or an entire site with a single click. Execute DR plans to achieve automated recovery at scale.
Recovery to Cloud	✔	Orchestrated Direct Restore to Azure gives your business additional resiliency with disaster recovery to the cloud. Orchestrate recovery of VMware and Veeam Agent backups as a VM in Azure, featuring automated mapping of VM resources and cloud networking.
Clean Recovery	✔	During recovery, iterate automated virus scans through multiple restore points until the most recent clean one is found. Regularly scan restore points during DataLab testing, with the results shown in dashboards and reports for improved visibility.
DataLab Management	✔	DataLab tests simulate disaster recovery outcomes, with fully automated DR testing in an isolated network without impacting production systems, including detailed reporting. Create and schedule DataLabs to allow application teams to safely and securely test upgrades, patches, and more.
RBAC and Scopes	✔	Granular role-based access control combined with customizable scopes allows administrators full control over access to recovery resources, allowing secure delegation of DR planning and testing to specialist teams and offloading backup administrators.
Dashboards & Reporting		
Dynamic documentation	✔	Autogenerated reports for DR plan definitions, checks, tests and executions remove the burden of documentation production from front-line staff. Documentation is produced in two formats, with full details for deep-dive analysis and an executive summary.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3476

✔ Fully supported ✔ Partially supported

Recovery Orchestration *Powered by Veeam Recovery Orchestrator*	**Veeam Data Platform**	**Description**
	Premium	
Compliance monitoring for RTOs and RPOs	✔	Meet business needs with RTO and RPO monitoring and reporting. Display achieved RTO & RPO against desired targets for each DR Plan providing an at-a-glance view of SLA compliance.
Scheduled readiness checks	✔	Pre-recovery, detailed readiness check documents ensure you are prepared for any disaster, by checking available restore points, critical infrastructure and required credentials.
DR plan auditing	✔	Audit reporting for Recovery Plans including monthly audit of all recovery plan activity, with change tracking.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3477

NVIDIA Virtual GPU Software Packaging, Pricing, and Licensing Guide

Application Note

DA-09924-001_v12 | August 2024

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3478

Document History

Version	Date	Authors	Description of Change
01	April 22, 2020	CH, SM	Initial Release
02	May 12, 2020	CH, SM	Updates to “Perpetual Concurrent User License” and “NVIDIA Education Pricing Program” sections
03	June 25, 2020	CH, RR, MR	Update NVIDIA Virtual Compute Server subscription price
04	July 20, 2020	NN	Update NVIDIA Virtual Compute Server abbreviated name
05	September 30, 2020	MR, RR	Add Ampere GPU support
06	February 17, 2021	MR, VK, NS, SM	Updated new Ampere GPU support, vGPU rebranding changes
07	April 14, 2021	NS, SM	Added A10 and A16
08	June 25, 2021	NN, SM	Updated CCU description in Table 1 Updated maximum concurrent VMs
09	August 3, 2021	NN, SM	Added subscription pricing to Table 9 Updated annual license subscription in Table 10 Updated education pricing in Table 12
10	Feb 1, 2022	MR	Added A2, A100X and A30X support
11	Mar 30, 2023	MR	Added L4, L40 support
12	August 1, 2024	MR, PL	Updated software editions and supported GPUs

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3479

Table of Contents

Terminology 4
Overview 5
    General Purchasing Information 6
Virtual GPU Software Product Details 8
    Virtual GPU Software Products 8
        NVIDIA vApps 8
        NVIDIA vPC 8
        NVIDIA RTX vWS 9
    vGPU Software Products and Entitlement 9
vGPU Software Licensing and Pricing 11
    Enterprise vGPU Software Pricing 11
    Subscription Concurrent User License 11
    Perpetual Concurrent User License 12
    NVIDIA Education Pricing Program 12
Choosing the Right License 14
NVIDIA License System 15

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3480

Terminology

The following table lists the terms that will be used throughout this guide.

Table 1. Terminology

Term	Meaning
SUMS	Support, Upgrade and Maintenance program
Perpetual License	A non-expiring, permanent software license that can be used on a perpetual basis without the need to renew. SUMS is required and is available in five-year increments. One-year SUMS available only for renewals.
Annual Subscription	A software license that is active for a fixed period as defined by the terms of the subscription. An annual subscription includes SUMS for the duration of the license term.
License Server	An application that manages license allocation, installed on a physical or virtual server.
Concurrent User (CCU) Licensing	A method of allocating licenses based on the number of VMs that are concurrently being used. A CCU license allows only one concurrent VM to be hosted per license. For application streaming or session-based solutions, each concurrent user requires a CCU license.
GPU	Graphics processing unit
Per GPU Licensing	A method of allocating licenses based on the number of GPUs that are being used. A per GPU license allows a certain number of concurrent VMs to be hosted per license.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3481

Overview

NVIDIA virtual GPU (vGPU) solutions bring the power of NVIDIA GPUs to virtual desktops, applications, and workstations, accelerating graphics and compute to make virtualized workspaces accessible to creative and technical professionals working from home offices or anywhere.

This guide covers the entitlement, packaging, and licensing of the NVIDIA virtual GPU (vGPU) software family of products. It is intended to be a quick reference to understand the product portfolio at a high level, with the corresponding SKU information. It does not contain detailed product information, which can be obtained from the NVIDIA vGPU website at http://www.nvidia.com/virtualgpu. This guide is not intended to replace or contradict the End User License Agreement (EULA). Refer to the EULA for more detailed information.

Table 2. NVIDIA Virtual GPU Software Licensed Products

Product	Description
NVIDIA Virtual Applications (vApps)	For organizations deploying Citrix Virtual Apps and Desktops, RDSH or other app streaming or session-based solutions. Designed for PC level applications and server-based desktops.
NVIDIA Virtual PC (vPC)	For users who want a virtual desktop but need great user experience leveraging PC Windows applications, browsers, and high-definition video.
NVIDIA RTX™ Virtual Workstation (vWS)	For users who want to be able to use remote professional graphics applications with full performance on any device, anywhere.

Note: For compute-intensive server workloads, such as AI, deep learning, or HPC running VMware vSphere, refer to the *NVIDIA AI Enterprise Packaging, Pricing and Licensing Guide*.

NVIDIA vGPU software brings graphics and virtualization capabilities to NVIDIA data center deployments and is currently supported on the NVIDIA graphics cards listed in Table 3 through Table 6. Find certified servers that are supported by NVIDIA GPUs and vGPU software at https://www.nvidia.com/en-us/data-center/resources/vgpu-certified-servers/.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3482

Table 3. Supported NVIDIA GPUs

	Framebuffer (GB)	Recommended vGPU Software
NVIDIA M10	4 x 8	NVIDIA vPC
NVIDIA M60	2 x 16	NVIDIA vWS, NVIDIA vPC
NVIDIA M6*	1 x 8	NVIDIA vWS, NVIDIA vPC
NVIDIA P4	1 x 8	NVIDIA vWS (Entry to Mid)
NVIDIA P6*	1 x 16	NVIDIA vWS, NVIDIA vPC
NVIDIA P40	1 x 24	NVIDIA vWS (Mid to High-end)
NVIDIA P100	1 x 12 / 1 x 16	NVIDIA vWS (Mid to High-end)
NVIDIA T4	1 x 16	NVIDIA vWS (Entry) NVIDIA vPC
NVIDIA RTX 6000	1 x 24	NVIDIA vWS (High-end)
NVIDIA RTX 8000	1 x 48	NVIDIA vWS (High end)
NVIDIA V100S/V100 SXM2	1 x 32	NVIDIA vWS
NVIDIA A40	1 x 48	NVIDIA vWS (High-end)
NVIDIA A10	1 x 24	NVIDIA vWS (Mid)
NVIDIA A16	4 x 16	NVIDIA vWS (Entry) NVIDIA vPC
NVIDIA A2	1 x 16	NVIDIA vWS, NVIDIA vPC
NVIDIA A6000	1 x 48	NVIDIA vWS (High-end)
NVIDIA A5000	1 x 24	NVIDIA vWS (Mid)
NVIDIA L40/L40S	1 x 48	NVIDIA vWS (High-end)
NVIDIA L4	1 x 24	NVIDIA vWS (Entry-Mid) NVIDIA vPC
NVIDIA RTX 6000 Ada	1 x 48	NVIDIA vWS (High-end)
NVIDIA RTX 5880 Ada	1 x 48	NVIDIA vWS (High-end)
NVIDIA RTX 5000 Ada	1 x 32	NVIDIA vWS (Mid)

* Designed for blade servers

Note: NVIDIA L2 and L20 are also supported with NVIDIA virtual GPU software.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3483

General Purchasing Information

NVIDIA vGPU software products can be purchased through NVIDIA Preferred Partners and select server OEMs. A list of these Preferred Partners and OEMs can be obtained from: http://www.nvidia.com/buygrid.

NVIDIA vGPU software products can be purchased as either a perpetual license with a Support Updates and Maintenance Subscription (SUMS), or as an annual subscription. The perpetual license gives the user the right to use the software indefinitely, with no expiration. All NVIDIA vGPU software products with perpetual licenses must be purchased in conjunction with a five-year SUMS. A one-year SUMS is available only for renewals.

The annual subscription offering is a more affordable option to allow IT departments to better manage the flexibility of license volumes. NVIDIA vGPU software products with an annual subscription include SUMS for the duration of the software's subscription license.

Table 4. General Purchasing Information

Entitlement	NVIDIA vGPU Production SUMS
Maintenance	Access to all maintenance releases, defect resolutions, and security patches for flexibility in upgrading as per the NVIDIA Virtual GPU Software Lifecycle Policy
Upgrades	Access to all new major version releases including feature enhancements and new hardware support
Long-term branch maintenance	Available for up to 3 years from general availability as per the NVIDIA Virtual GPU Software Lifecycle Policy
Direct support	Direct access to NVIDIA support engineering for timely resolution of customer-specific issues
Support availability	Customer support available during standard business hours Cases accepted 24 × 7
Knowledgebase access	✓
Web support	✓
E-mail support	✓
Phone support	✓

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3484

Virtual GPU Software Product Details

NVIDIA vGPU software is the industry's most advanced technology for sharing true virtual GPU hardware acceleration between multiple users—without compromising the graphics experience. This virtualization technology ensures complete application compatibility, which means features and experience are the same as they would be on a physical device.

Virtual GPU Software Products

NVIDIA vGPU desktop and application virtualization solutions are designed to bring the power of virtualization to the users who need to be their most productive. vGPU technology ensures application compatibility, meaning any application that can run in a physical desktop environment can run in a virtual environment. Organizations can now expand their virtualization footprint without compromise.

The following NVIDIA vGPU software products are available:

- NVIDIA Virtual Applications (vApps)
- NVIDIA Virtual PC (vPC)
- NVIDIA RTX Virtual Workstation (vWS)

NVIDIA vApps

This product is for organizations deploying Citrix Virtual Apps and Desktops, RDSH or other app streaming or session-based solutions. Designed to deliver PC Windows applications at full performance, NVIDIA vApps allows users to access any Windows application at full performance on any device, anywhere.

Windows Server hosted RDSH desktops are also supported by NVIDIA vApps.

NVIDIA vPC

This product is ideal for users who want a virtual desktop but need great user experience leveraging PC Windows applications, browsers, and high-definition video. NVIDIA vPC delivers a native experience to users in a virtual environment, allowing them to run all their PC applications at full performance.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3485

NVIDIA RTX vWS

This product is ideal for compute intensive workloads, such as accelerated graphics, NVIDIA Omniverse, and AI development. It is suitable for high-end designers who use powerful 3D content creation applications such as Dassault CATIA, SOLIDWORKS, 3DExcite, Siemens NX, PTC Creo, Schlumberger Petrel, or Autodesk Maya. NVIDIA vWS allows users to access their applications with full features and performance, anywhere, on any device.

vGPU Software Products and Entitlement

Each NVIDIA vGPU software product includes the feature entitlements listed in Table 5.

Table 5. Feature Entitlements

Feature	NVIDIA vApps	NVIDIA vPC	NVIDIA vWS
License Entitlement			
Concurrent User (CCU)	✓	✓	✓
Per GPU			
Capability Entitlement			
Desktop Virtualization		✓	✓
RDSH App Hosting	✓	✓	✓[2]
RDSH Desktop Hosting	✓	✓	✓[2]
Compute Virtualization			✓
Windows Guest OS Support	✓	✓	✓
Linux Guest OS Support	✓	✓	✓
Maximum Displays	1[3]	4	4
Maximum Resolution[4]	1280 × 1024	5120 × 2880 (5K)	7680 × 4320 (8K)
NVIDIA RTX Enterprise Software Features			✓
OpenGL, DirectX and Vulkan	✓	✓	✓
CUDA and OpenCL Support			✓[5]
ECC and Page Retirement			✓

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3486

Multi-vGPU			✓
NVLink			✓
GPU Pass Through Support[7]	✓		✓
Bare Metal Support[8]	✓		✓
vGPU Profile Sizes Supported[9]			
512 MB		✓	✓
1 GB	✓	✓	✓
2 GB	✓	✓	✓
3 GB	✓		✓
4 GB	✓		✓
5 GB			
6 GB	✓		✓
8 GB	✓		✓
10 GB			
12 GB	✓		✓
16 GB	✓		✓
20 GB			
24 GB	✓		✓
32 GB	✓		✓
40 GB			
48 GB	✓		✓

Notes:

[1]Maximum 10 concurrent VMs per GPU

[2]With packaged NVIDIA vApps license

[3]Applies only to the console display in remote application environments. For details, see Supported GPUs

[4]Review the Virtual GPU Software User Guide for the supported display configurations for each profile

[5]Supported on 8GB 1:1 profile on NVIDIA Maxwell and all profiles on Pascal

[6]ECC support begins with Pascal

[7]Only supported on 1:1 profiles

[8]Only NVIDIA M6 hardware supported as primary display device

[9]Review the Virtual GPU Software User Guide for the vGPU profiles supported on your GPU

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3487

vGPU Software Licensing and Pricing

Enterprise vGPU Software Pricing

NVIDIA vApps, NVIDIA vPC, and NVIDIA RTX vWS are available on a per Concurrent User (CCU) model. A CCU license is required for every user who is accessing or using the software at any given time, whether an active connection to the virtualized desktop or session is maintained.

NVIDIA vGPU software products can be purchased by enterprises as either perpetual licenses with annual Support Updates and Maintenance Subscription (SUMS), or as an annual subscription. All NVIDIA vGPU software products with perpetual licenses must be purchased in conjunction with a five-year SUMS. A one-year SUMS is available only for renewals. For annual licenses, SUMS is bundled into the annual license cost.

Enterprise vGPU software licensing and pricing are described in the following subsections. Pricing is suggested pricing only. Contact your authorized NVIDIA partner for final pricing. If you are looking to run or host a service by using NVIDIA vGPU software, you need to join the NPN CSP partner program.

Subscription Concurrent User License

An annual Enterprise subscription is active for a fixed period as defined by the terms of the subscription license. To be kept active, the license will need to be renewed at the end of the subscription period. The subscription license includes the software license and production level SUMS for the duration of the license subscription period.

Table 6. Concurrent User License Annual Subscription Pricing

License	Annual Subscription Pricing
NVIDIA Virtual Applications	$10 per CCU subscription
NVIDIA Virtual PC	$50 per CCU subscription

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3488

	4-year subscription - $43.75 per CCU 5-year subscription - $40 per CCU
NVIDIA RTX Virtual Workstation	$250 per CCU subscription
	4-year subscription - $206.25 per CCU 5-year subscription - $180 per CCU

Perpetual Concurrent User License

A perpetual enterprise license allows for use of the licensed software indefinitely. Users that opt to license using this model are required to subscribe to SUMS for five years. The SUMS subscription can be renewed on a yearly basis after the expiration of the initial subscription.

Table 7. Enterprise Perpetual Licensing plus SUMS Pricing

License	Annual Licensing plus SUMS Pricing
NVIDIA Virtual Applications	$20 per CCU perpetual license
	$5 SUMS per year
NVIDIA Virtual PC	$100 per CCU perpetual license
	$25 SUMS per year
NVIDIA RTX Virtual Workstation	$450 per CCU perpetual license
	$100 SUMS per year

NVIDIA Education Pricing Program

The NVIDIA Education Pricing Program supports the use of visual computing in teaching and research institutions. The program makes it easy to procure and administer NVIDIA solutions, software licensing, and services for qualified educational institutions and helps

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3489

reduce their total cost. For more information on eligibility, review the NVIDIA Education Pricing Program documentation.

The Annual Subscription Model is available for NVIDIA vWS . The Perpetual Licensing Model is available only for NVIDIA vWS. Users that opt for the Perpetual Licensing Model are required to subscribe to SUMS for five years. The SUMS subscription can be renewed on a yearly basis after the expiration of the initial subscription.

Table 8. NVIDIA Education Pricing

License	Pricing Model	Price
NVIDIA vWS	Perpetual Licensing plus SUMS	$99 per CCU perpetual license
		$25 SUMS per year
	Annual Subscription	$50 per CCU subscription

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3490

Choosing the Right License

The following table provides a guideline to help decide which license is required based on the desired entitlement and capability. This is not an all-inclusive list of possible solutions. If you have further questions or are unable to decide based on the decision tree, contact NVIDIA vGPU Support at https://www.nvidia.com/en-us/support/enterprise/.

Table 9. Common Use Cases and Solutions

I am using...	I need this license...
Citrix Virtual Desktops	NVIDIA vPC – for PC level applications NVIDIA vWS – for workstation/professional 3D use cases
Omnissa Horizon 8	NVIDIA vPC – for PC level applications NVIDIA vWS – for each session utilizing a workstation/professional 3D use case
Citrix Virtual Apps and Desktops	NVIDIA vApps NVIDIA vWS – for each session utilizing a workstation/professional 3D use case
Omnissa Horizon 8 RDSH	NVIDIA vApps NVIDIA vWS – for each session utilizing a workstation/professional 3D use case
Other RDSH / Session-based	NVIDIA vApps NVIDIA vWS – for each session utilizing a workstation/professional 3D use case
Microsoft RemoteFX	NVIDIA vPC – for PC level applications
VMware vSGA	NVIDIA vPC – for PC level applications
Microsoft Hyper-V (DDA)	NVIDIA vWS
Microsoft AzureStack GPU-P	NVIDIA vPC – for PC level applications NVIDIA vWS – for each session utilizing a workstation/professional 3D use case
Red Hat Enterprise Linux with KVM	NVIDIA vWS – for workstation/professional 3D use cases

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3491

NVIDIA License System

The NVIDIA License System provides monitoring and reporting on license usage for capacity planning. It is available for download with the vGPU software packages from the NVIDIA Licensing Portal. This license server can be installed on either a physical server or, more likely, a dedicated virtual machine.

To ensure that the end user experience is not impaired by license overages or connection issues, the vGPU software runs with or without a valid license server connection. The license server allows the IT administrator to track license usage and determine correct sizing for their environments. In compliance with the EULA, IT administrators may also use any other method that reliably tracks the software usage to ensure they have enough licenses for their CCU or per GPU usage.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3492

Notice

This document is provided for information purposes only and shall not be regarded as a warranty of a certain functionality, condition, or quality of a product. NVIDIA Corporation (“NVIDIA”) makes no representations or warranties, expressed or implied, as to the accuracy or completeness of the information contained in this document and assumes no responsibility for any errors contained herein. NVIDIA shall have no liability for the consequences or use of such information or for any infringement of patents or other rights of third parties that may result from its use. This document is not a commitment to develop, release, or deliver any Material (defined below), code, or functionality.

NVIDIA reserves the right to make corrections, modifications, enhancements, improvements, and any other changes to this document, at any time without notice.

Customer should obtain the latest relevant information before placing orders and should verify that such information is current and complete.

NVIDIA products are sold subject to the NVIDIA standard terms and conditions of sale supplied at the time of order acknowledgement, unless otherwise agreed in an individual sales agreement signed by authorized representatives of NVIDIA and customer (“Terms of Sale”). NVIDIA hereby expressly objects to applying any customer general terms and conditions with regards to the purchase of the NVIDIA product referenced in this document. No contractual obligations are formed either directly or indirectly by this document.

NVIDIA products are not designed, authorized, or warranted to be suitable for use in medical, military, aircraft, space, or life support equipment, nor in applications where failure or malfunction of the NVIDIA product can reasonably be expected to result in personal injury, death, or property or environmental damage. NVIDIA accepts no liability for inclusion and/or use of NVIDIA products in such equipment or applications and therefore such inclusion and/or use is at customer’s own risk.

NVIDIA makes no representation or warranty that products based on this document will be suitable for any specified use. Testing of all parameters of each product is not necessarily performed by NVIDIA. It is customer’s sole responsibility to evaluate and determine the applicability of any information contained in this document, ensure the product is suitable and fit for the application planned by customer, and perform the necessary testing for the application in order to avoid a default of the application or the product. Weaknesses in customer’s product designs may affect the quality and reliability of the NVIDIA product and may result in additional or different conditions and/or requirements beyond those contained in this document. NVIDIA accepts no liability related to any default, damage, costs, or problem which may be based on or attributable to: (i) the use of the NVIDIA product in any manner that is contrary to this document or (ii) customer product designs.

No license, either expressed or implied, is granted under any NVIDIA patent right, copyright, or other NVIDIA intellectual property right under this document. Information published by NVIDIA regarding third-party products or services does not constitute a license from NVIDIA to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property rights of the third party, or a license from NVIDIA under the patents or other intellectual property rights of NVIDIA.

Reproduction of information in this document is permissible only if approved in advance by NVIDIA in writing, reproduced without alteration and in full compliance with all applicable export laws and regulations, and accompanied by all associated conditions, limitations, and notices.

THIS DOCUMENT AND ALL NVIDIA DESIGN SPECIFICATIONS, REFERENCE BOARDS, FILES, DRAWINGS, DIAGNOSTICS, LISTS, AND OTHER DOCUMENTS (TOGETHER AND SEPARATELY, “MATERIALS”) ARE BEING PROVIDED “AS IS.” NVIDIA MAKES NO WARRANTIES, EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE MATERIALS, AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL NVIDIA BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF ANY USE OF THIS DOCUMENT, EVEN IF NVIDIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Notwithstanding any damages that customer might incur for any reason whatsoever, NVIDIA’s aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms of Sale for the product.

Trademarks

NVIDIA, the NVIDIA logo, CUDA, NVIDIA HGX, NVIDIA Maxwell, NVIDIA Turing, NVIDIA RTX, NVIDIA Volta, NVIDIA Ampere, NVIDIA Ada NVLink, and TensorRT are trademarks and/or registered trademarks of NVIDIA Corporation in the U.S. and other countries. Other company and product names may be trademarks of the respective companies with which they are associated.

OpenCL

OpenCL is a trademark of Apple Inc. used under license to the Khronos Group Inc.

Copyright

© 2020, 2021, 2022, 2023, 2024 NVIDIA Corporation. All rights reserved.

Anexo Catálogo_CLM SOFTWARE (2050248) SEI 2025.007562 / pg. 3493

PROPOSTA TÉCNICA

SOLUÇÃO DE INFRAESTRUTURA HIPERCONVERGENTE NUTANIX

Pregão Eletronico 94001/2026
UASG: 925849
Ministério Público do Estado do Amazonas

Proponente:
CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA

A **CLM Software Comércio Importação e Exportação Ltda.,** empresa especializada no fornecimento de soluções de tecnologia da informação para ambientes corporativos críticos, apresenta sua Proposta Técnica para atendimento integral ao objeto do **Pregão Eletrônico 94001/2026**, cujo escopo contempla fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais do Ministério Público do Estado do Amazonas (MPAM), conforme especificações técnicas estabelecidas no Termo de Referência.

A solução proposta foi cuidadosamente dimensionada para assegurar total compatibilidade técnica, alta disponibilidade, continuidade operacional, preservação dos investimentos já realizados e aderência absoluta às exigências técnicas e operacionais do MPAM, não contemplando qualquer desvio, customização paralela ou mitigação alternativa ao solicitado.

1. DESCRITIVO TÉCNICO

ITEM 01 - EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9

Marca: Nutanix

Modelo: NX8155G9

Lista de Part Numbers:

PART-NUMBER	DESCRIÇÃO	QUANTIDADE ENTREGUE
NX-8155-G9-CM	Sistema	4
C-CPU-4510-CM	CPU	8

C-MEM-96GB-5600-CM	Memória	64
C-HDD-12TB-EA-CM	Disco HDD	32
C-NVM-3.84TB-B-CM	SSD NVMe	16
C-HBA-3816-1N-A-CM	Rede	4
C-LOM-10G2D1BT-CM	Rede	4
C-NIC-25G2A2-CM	Rede	4
C-PWR-4FC13C14A-CM	Cabo de força	8
C-TPM-2.0-U-CM	Modulo-TPM	4

ITEM 02 – EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU

Marca: Nutanix

Modelo: NX-3155-G9

Lista de Part Numbers:

PART-NUMBER	DESCRIÇÃO	QUANTIDADE ENTREGUE
NX-3155-G9-CM	Sistema	1
C-CPU-4510-CM	CPU	2
C-MEM-64GB-5600-CM	Memória	16
C-HDD-12TB-EA-CM	Disco HDD	4
C-NVM-3.84TB-B-CM	SSD NVMe	2
C-HBA-3816-1N-A-CM	Rede	1
C-LOM-10G2D1BT-CM	Rede	1
C-NIC-25G2A2-CM	Rede	1

C-PWR-4FC13C14A-CM	Cabo de força	2
C-TPM-2.0-U-CM	Modulo-TPM	1
C-GPU-L40S-48GB-A-CM	GPU	1

ITEM 03 – SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX

Marca: NUTANIX

Modelo: NAI GPT IN A BOX PRO

Lista de Part Numbers:

PART-NUMBER	DESCRIÇÃO	QUANTIDADE ENTREGUE
SW-NAI-GPT-PRO-C-PR	Subscription, Nutanix Enterprise AI (NAI) GPT-in-a-box Pro Software License & Production Software Support Service for 1 CPU Core	120
SWA-NCI-SEC-PR	Subscription, Nutanix Cloud Infrastructure (NCI) Security add-on Software License & Production Software Support Service for 1 CPU Core	120
S-HW-PRD	24/7Production Level HW Support for Nutanix HCI appliance	05

ITEM 04 – SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU

Marca: Nutanix

Modelo: SW-NAI-PRO-GB-PR

Lista de Part Numbers:

PART-NUMBER	DESCRIÇÃO	QUANTIDADE ENTREGUE
SW-NAI-PRO-GB-PR	Subscription, Nutanix Enterprise AI (NAI) Pro Software License and Production Software Support Service for 1 GB of GPU RAM	48

ITEM 05 – LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE

Marca: Nutanix

Modelo: SW-NAI-GPT-PRO-C-PR

Lista de Part Numbers:

PART-NUMBER	DESCRIÇÃO	QUANTIDADE ENTREGUE
SW-NAI-GPT-PRO-C-PR	Subscription, Nutanix Enterprise AI (NAI) GPT-in-a-box Pro Software License & Production Software Support Service for 1 CPU Core	50 TB

ITEM 06 – SOFTWARE DE BACKUP DE DADOS

Marca: VEEAM

Modelo: Veeam Data Platform Advanced

Lista de Part Numbers:

PART-NUMBER	DESCRIÇÃO	QUANTIDADE ENTREGUE
P-ADVVUL-0I-SU5YP-00	Veeam Data Platform Advanced Universal Subscription License. Includes Enterprise Plus Edition features. 10 instance pack. 5 Years Subscription Upfront Billing & Production (24/7) Support. Public Sector.	20
Win Server DC Core SLng LSA OLV 16L NL 3Y Aq Y1 AP	Windows Server 2025 Datacenter - 16 Core	3
Win Server DC Core SLng LSA OLV 16L NL 1Y Aq Y1 AP	Windows Server 2025 Datacenter - 16 Core	6

ITEM 07 – EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES

Marca: Exagrid

Modelo: EX54-SEC

Lista de Part Numbers:

PART-NUMBER	DESCRIÇÃO	QUANTIDADE ENTREGUE
EX54-SEC	Disk Capacity: Raw: 162 TB, Useable: 108 TB. 54 TB Full Backup. Includes 1 10 Gigabit Add on Card Disks are encrypted	1
EX-25GBE-OPTICAL	25 Gigabit Ethernet Dual Port SFP28 Optical Option for all ExaGrid models. Includes two qualified SFP28 short-range Modules.	1

ITEM 08 – SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ONPREMISES

Marca: EXAGRID

Modelo: Backup Storage Software

Lista de Part Numbers:

PART-NUMBER	DESCRIÇÃO	QUANTIDADE ENTREGUE
EX54-SEC-SW	108 TB Tiered Backup Storage Software - Software Only	1
EX-5YR-MS-P	Five year 7 x 24 Customer Support and product Maintenance	1

ITEM 09 – SWITCH CORE

Marca: JUNIPER

Modelo: QFX5120

Lista de Part Numbers:

PART-NUMBER	DESCRIÇÃO	QUANTIDADE ENTREGUE
JP-QFX5120-48Y-AFI2	QFX5120-48Y, airflow in, redundant AC PSUs and FANs Ships with base S/W features.	2
JP-CBL-EX-PWR-C13-BR	AC POWER CABLE - BRAZIL (10A/250V, 2.5M)	4
JP-JNP-100G-DAC-1M	QSFP28 to QSFP28 Ethernet Direct Attach Copper (twinax copper cable) 1m	2
JP-JNP-SFP-25G-DAC-3M	SFP28, 25GE DIRECT ATTACH COPPER CABLE, 3 METERS, STANDARD	10

	TEMPERATURE (0 THROUGH 70 DEGREE C), 0.5W, 26 AWG	
JP-SFPP-10G-SR-C	SFP+, 10GBASE-SR, MMF OM3 300 METERS AND OM4 400 METERS, STANDARD TEMPERATURE (0 THROUGH 70 DEGREE C), DUPLEX LC CONNECTOR	4
JP-SVC-ND-QFX5-48YB	JP-SVC-ND-QFX5-48YB Juniper) Care Next Day Support for) QFX5120-48Y-DAFO2,	2
JP-S-QFX5K-C1-A1-5	5 yr term Advanced1 license for Class 1 QFX5K products	2

Serra (ES), 19 de janeiro de 2026.

gov.br
Documento assinado digitalmente
TATIANA MONTEIRO MONTROZE
Data: 19/01/2026 11:38:25-0300
Verifique em https://validar.iti.gov.br

_____

Tatiana Monteiro Montroze
CPF: 354.042.638-81
Representante Legal

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

OFÍCIO Nº 29.2026.CPL.2050284.2025.007562

Manaus, 20 de janeiro de 2026.

Ao Senhor

EUDO DE LIMA ASSIS JUNIOR

Diretor de Tecnologia da Informação e Comunicação – DTIC

Assunto: Análise de proposta - Pregão Eletrônico Nº 94.001/2026-CPL/MP/PGJ.

Ao cumprimentá-lo cordialmente, e no âmbito do **PREGÃO ELETRÔNICO Nº 94.001/2026-CPL/MP/PGJ**, cujo objeto é a *contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma* ***solução de datacenter,*** *contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com* ***garantia de 60 (sessenta) meses****,* **encaminho,** com base no item 10.2 do instrumento convocatório, **a proposta de preços** (docs. 2050244, 2050248 e 2050251) apresentada pela empresa **CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA** , inscrita no CNPJ n.º 02.092.332/0003-30, **para análise e manifestação dessa Diretoria de Tecnologia da Informação e Comunicação – DTIC.**

Sarah Madalena B. Côrtes de Melo

Pregoeira - Portaria Nº 66/2026/SUBADM

Documento assinado eletronicamente por **Sarah Madalena Barbosa Santos Cortes**, **Presidente da Comissão Permanente de Licitação - CPL**, em 20/01/2026, às 12:05, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2050284** e o código CRC **995ECE37**.

Ao
MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

ANEXO VIII
DISPENSA DE VISTORIA TÉCNICA

A empresa **CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA**, pessoa jurídica de direito privado, inscrita no CNPJ sob nº 02.092.332/0003-30, com sede na Rua Samuel Meira, nº 394, sala 29, Bairro Taquara II, Serra/ES, CEP 29167-650, optou por não vistoriar o local dos serviços conforme previsto no Subitem 3.1. do Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562.

Declaro, ainda, que quaisquer alegações de desconhecimento ou erro orçamentário por parte da futura contratada, para a execução dos serviços propostos não serão considerados nem usados como possível juízo de valor afim de compensações futuras.

Serra (ES), 19 de janeiro de 2026.

gov.br
Documento assinado digitalmente
TATIANA MONTEIRO MONTROZE
Data: 16/01/2026 08:41:16-0300
Verifique em https://validar.iti.gov.br

CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA
Tatiana Monteiro Montroze
RG: 40.183.211-9
CPF: 354.042.638-81

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

PARECER Nº 5.2026.DTIC.2050482.2025.007562

PROCESSO DE COMPRA: 2025.007562

OBJETO: Contratação de empresa especializada para o **fornecimento, implantação, configuração e transferência de conhecimento infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado backup**, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais do Ministério Público do Estado do Amazonas (M

ORIGEM: Pregão Eletrônico n.º 94.001/2026-CPL/MP/PGJ, Termo de Referência n.º 28.2025.DTIC.2002143.2025.007562.

1. RELATÓRIO

Trata-se de análise técnica de compatibilização da proposta apresentada pela licitante **CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA.** , inscrita no CNPJ (MF) n.º 02.092.332/0003-30, constante dos documentos2050244, 2050248 e 2050251, encaminhado no âmbito do certame em epígrafe.

A presente manifestação tem por finalidade verificar a aderência técnica da proposta às exigências estabelecidas no Termo de Referência, observando-se os princípios da vinculação ao instrumento convocatório, do julgamento objetivo e da isonomia.

2. DA ANÁLISE

Item	Descrição	Marca/Modelo Ofertado	Exigênicas do TR	Proposta
ITEM 01	EQUIPAMENTO HIPERCONVERGENTE NUTANIX G9 (SEM GPU)	NUTANIX NX8155G9	• Appliances Nutanix série NX homologados; • uso de nós; • min. 2 CPUs x86 por nó (mín. 12nucleos/24T cada); • 1.536 GB RAM por nó (DDR5); • 4 SSD NVMe ≥ 3,84 TB + 8 HDD ≥ 12 TB por nó; • Interfaces 25/10 GbE + porta dedicada de gerenciamento; • Alta disponibilidade, Prism, expansão não disruptiva.	• Modelo: **NX8155 G9** (oficial Nutanix); • Quantidade: **4 nós**; • CPU: Intel Xeon Silver núcleos, threads e clo • Memória: **96 GB x 16** **1.536 GB por nó (DI** • Armazenamento: ◦ 4 x NVMe 3,84 TI ◦ 8 x HDD 12 TB • Rede: 25 GbE + 10 Gb gerência; • Prism e AOS/AHV nati
ITEM 02	EQUIPAMENTO HIPERCONVERGENTE NUTANIX G9 COM GPU	NUTANIX NX-3155-G9	• Appliance Nutanix NX; • 1 nó; • 2 CPUs x86; • ≥ 1.024 GB RAM; • GPU com 48 GB GDDR6 (classe NVIDIA L40S ou equivalente); • SSD + HDD conforme volumetria mínima; • Integração total com Nutanix e Prism.	• Modelo: **NX-3155 G9** • Quantidade: 1; • CPU: 2 x Xeon Silver 4 • Memória: **1.024 GB D** • GPU: **NVIDIA L40S –** • Storage e rede compa • Integração total Nutar
ITEM 03	SOFTWARE GESTÃO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX	NUTANIX NAI GPT IN A BOX PRO	• SDS nativo, sem RAID tradicional. • Snapshots, replicação local/remota e DR. • QoS, compressão e deduplicação. • Gerenciamento multi-cluster.	• Nutanix AOS (SDS nat • Funcionalidades nativ AOS/Leap. • Recursos nativos Nuta • Prism Central.
ITEM 04	SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU	NUTANIX Modelo: SW-NAIPRO-GB-PR	• Licença compatível com memória de GPU. • Capacidade conforme dimensionamento do projeto.	• Licença Nutanix NAI P GPU RAM (48 GB).

Item	Descrição	Marca/Modelo Ofertado	Exigênicas do TR	Proposta
ITEM 05	LICENÇA para Armazenamento de dados não estruturados (Nutanix Unified Storage)	NUTANIX Modelo: SW-NAIGPT-PRO-C-PR	• Capacidade mínima conforme dimensionamento; • Integração com Nutanix; • Licenciamento adequado.	• Nutanix Unified Storaç • **50 TB licenciados**; • Software e suporte inc
ITEM 06	SOFTWARE DE BACKUP DE DADOS	VEEAM Modelo: Veeam Data Platform Advanced	• Backup corporativo compatível com Nutanix. • Suporte 24x7.	• **Veeam Data Platfor** (20 packs de 10 VM / • Suporte 24x7 por 5 ar
ITEM 07	EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	Exagrid Modelo: EX54-SEC	• Repositório dedicado e criptografado.	• ExaGrid EX54-SEC (10
ITEM 08	SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES	EXAGRID Modelo: Backup Storage Software	• Software de gerenciamento e suporte.	• ExaGrid Backup Stor + suporte 5 anos.
ITEM 09	SWITCH CORE	JUNIPER Modelo: QFX5120	• Switch core compatível com 25/100 GbE; • Redundância; • Licenciamento e suporte.	• **Juniper QFX5120** (2 • Cabos DAC, SFPs; • Fontes redundantes, l suporte 5 anos.

2.1 CONCLUSÃO TÉCNICA FINAL

Após análise individualizada de todos os itens constantes do Termo de Referência, verificou-se que a proposta apresentada pela empresa **CLM Software Comércio Importação e Exportação Ltda.** atende integralmente às exigências técnicas estabelecidas, não sendo identificadas não conformidades, sejam elas sanáveis ou insanáveis.

Dessa forma, a proposta mostra-se tecnicamente compatível e aderente ao objeto licitado, encontrando-se apta ao prosseguimento do certame.

Diante do exposto, a equite técnica **OPINA** pela aceitação da proposta.

É o parecer.

Manaus, 22 de janeiro de 2026.

ANTOVLA FROTA BEZERRA JÚNIOR
Técnico em Computação

EUDO DE LIMA ASSIS JUNIOR
Diretor de Tecnologia da Informação e Comunicação

Documento assinado eletronicamente por **Antovila Frota Bezerra Junior**, **Requisitado**, em 22/01/2026, às 14:20, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Eudo de Lima Assis Júnior**, **Diretor de Tecnologia da Informação e Comunicação (DTIC)**, em 22/01/2026, às 15:00, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2050482** e o código CRC **CB06F975**.

Ao
MPAM
P.E 94.001/2026

Item 3.2.2 do Termo de Referência

DECLARAÇÃO DE INDICAÇÃO DE PESSOAL TÉCNICO, INSTALAÇÕES E APARELHAMENTO

A empresa **CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA,** pessoa jurídica de direito privado, inscrita no CNPJ sob nº 02.092.332/0003-30, com sede na Rua Samuel Meira, nº 394, sala 29, Bairro Taquara II, Serra/ES, CEP 29167-650, por intermédio de sua representante legal, o Sra. Tatiana Monteiro Montroze , brasileira, casada, portador da cédula de identidade nº 40.183.211-9 SSP/SP, inscrito no CPF/MF sob o nº 354.042.638-81, **DECLARA,** para os devidos fins e em atendimento ao item 3.2.2 do Edital, bem como ao disposto no art. 67, inciso III, da Lei nº 14.133/2021, que dispõe de pessoal técnico-operacional qualificado, bem como de instalações e aparelhamento adequados e disponíveis para a plena execução do objeto da licitação.

Equipe Técnica Responsável
A licitante indica como responsáveis técnicos pela execução dos serviços os seguintes profissionais, devidamente qualificados:

Lucas Makiyama
CPF nº 001.303.352-23
Especialista em Hiperconvergência e Backup

Ronnyelson Silva
CPF nº 008.938.752-01
Especialista em Hiperconvergência, Backup e Network

Daniel Galvão
CPF nº 428.347.788-50
Especialista em Hiperconvergência, Backup e Virtualização

Os profissionais acima indicados possuem experiência compatível com o objeto licitado e se responsabilizarão tecnicamente pela execução dos trabalhos, conforme as exigências editalícias.

Instalações e Aparelhamento
No que se refere às instalações, infraestrutura técnica e aparelhamento, a licitante declara que estes encontram-se adequados, disponíveis e compatíveis com a execução do objeto, conforme detalhamento constante na Proposta Técnica apresentada, a qual integra este processo para todos os fins.

Serra (ES), 19 de janeiro de 2026.

gov.br Documento assinado digitalmente
TATIANA MONTEIRO MONTROZE
Data: 16/01/2026 13:59:33-0300
Verifique em https://validar.iti.gov.br

CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA
Tatiana Monteiro Montroze
RG: 40.183.211-9
CPF: 354.042.638-81

ATESTADO DE CAPACIDADE TÉCNICA

A **CONVERGE DATA TECNOLOGIA DA INFORMACAO - CDTI**, **CNPJ: 20.621.724/0001-60,** vem por meio deste **ATESTAR** que a empresa **CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO** LTDA, inscrita no CNPJ nº. 02.092.332/0001-79, estabelecida na Calçada das Hortências, 131 - Andar 2, Alphaville – SP - CEP: 06453-017, forneceu a os itens abaixo relacionados, cumprindo fielmente as obrigações assumidas.

FABRICANTE VEEAM

ITEM	DESCRIÇÃO	QUANTIDADE	N.F / DANFE
1	PartNumber: V-ADVVUL-0I-SU1MP-00 - Veeam Data Platform Advanced Universal Subscription License. Includes Enterprise Plus Edition features. Subscription Upfront Billing 10 instance pack. & Production (24/7) Support - Monthly Coterm.	20	N.F - 12503
2	PartNumber: P-ADVVUL-0I-SU3YP-00 - Veeam Data Platform Advanced Universal Subscription License. Includes Enterprise Plus Edition features. 10 instance pack. 3 Years Subscription Upfront Billing & Production (24/7) Support.	10	
3	PartNumber: P-ADVVUL-0I-SU3YP-00- Veeam Data Platform Advanced Universal Subscription License. Includes Enterprise Plus Edition features. 10 instance pack. 3 Years Subscription Upfront Billing & Production (24/7) Support.	2	N.F - 12227

Declaramos ainda, que os serviços de instalação, suporte e garantia, foram executados satisfatoriamente, não existindo em nossos registros até a presente data, nada que desabone sua conduta e responsabilidade comercialmente ou tecnicamente.

Brasília (DF), 25 de março de 2025

MARCOS ALEX DE AGUIAR ALBANO:63489082168

Assinado de forma digital por MARCOS ALEX DE AGUIAR ALBANO:63489082168
Dados: 2025.03.25 16:29:33 -03'00'

Alex Aguiar
Diretor comercial
Converge Data Tecnologia da Informação

ATESTADO DE CAPACIDADE TÉCNICA

A **ALTAS NETWORKS & TELECOM LTDA.**, inscrita no CNPJ sob nº: 05.407.609/0001-01, situada à Av. Olegário Maciel, 1.217 – 4º andar. Bairro de Lourdes. Belo Horizonte/MG. CEP: 30.180-111, vem por meio deste **ATESTAR** que a empresa **CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO** LTDA, inscrita no CNPJ nº: 02.092.332/0001-79, estabelecida à Calçada das Hortências, 131 - Andar 2, Alphaville, São Paulo, SP - CEP: 06.453-017, forneceu os itens abaixo relacionados, cumprindo fielmente as obrigações assumidas.

Item	DESCRIÇÃO	Qdade	Nota Fiscal
1	Arista 7050X3, 48x10GbE SFP & 8x100GbE QSFP switch, rear-to-front air, 2 x AC DCS-7050SX3-48C8-R	2	N.F. nº 5677

Declaramos ainda, que os serviços de instalação, suporte e garantia foram executados satisfatoriamente, não existindo em nossos registros até a presente data, nada que desabone sua conduta e responsabilidade comercialmente ou tecnicamente.

Belo Horizonte, 03 de julho de 2024

ALMIR FRANZ DE LIMA:59191473691

Assinado de forma digital por ALMIR FRANZ DE LIMA:59191473691
Dados: 2024.07.03 10:32:10 -03'00'

Almir Franz de Lima
Diretor Comercial e de Estratégias
E-mail: comercial@altasnet.com.br
Tel: (31) 3449-4500

ATESTADO DE CAPACIDADE TÉCNICA

A **CONVERGE DATA TECNOLOGIA DA INFORMACAO - CDTI**, **CNPJ: 20.621.724/0001-60,** vem por meio deste **ATESTAR** que a empresa **CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO LTDA**, inscrita no CNPJ nº. 02.092.332/0001-79, estabelecida na Calçada das Hortências, 131 - Andar 2, Alphaville – SP - CEP: 06453-017, forneceu a os itens abaixo relacionados, cumprindo fielmente as obrigações assumidas.

FABRICANTE ARISTA

ITEM	DESCRIÇÃO	QUANTIDADE	N.F / DANFE
1	P1236582 - Arista 7050X3, 48x10GbE SFP & 8x100GbE QSFP switch, front-torear air, 2xAC	2	DANFE - 7368
2	P0000769 - 10GBASE-CR TWINAX COPPER CABLE WITH SFP+ CONNECTORS ON BOTH ENDS -3M	12	DANFE - 279
3	P0000785 - 40GBE QSFP+ TO QSFP+ TWINAX COPPER CABLE- 1M	2	DANFE - 7369
4	P1236483 - 10GBASE-SR SFP+ (Short Reach)	2	
5	P0000759 - 1000BASE-T SFP (RJ-45 Copper)	6	

Declaramos ainda, que o fornecimento foi executado satisfatoriamente, não existindo em nossos registros até a presente data, nada que desabone sua conduta e responsabilidade comercialmente ou tecnicamente.

Brasília (DF), 25 de março de 2025

MARCOS ALEX DE AGUIAR ALBANO:63489082168

Assinado de forma digital por MARCOS ALEX DE AGUIAR ALBANO:63489082168
Dados: 2025.03.25 16:29:00 -03'00'

Alex Aguiar
Diretor comercial
Converge Data Tecnologia da Informação

ATESTADO DE CAPACIDADE TÉCNICA

SESI - SERVIÇO SOCIAL DA INDÚSTRIA – DR/PA situado na Tv. Quintino Bocaiúva, 1588 - Nazaré - 66035-190 - Belém/PA, inscrito no CNPJ: 03.768.023/0001-39, tendo como representante a Gerente Executiva de Tecnologia da Informação – GETIC a Senhora **Dilma Farias Viana**, e-mail: dilma@senaipa.orr.br e contato: (091) 4009-4823/99146-1764, vem por meio deste ATESTAR que a empresa **CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO LTDA** , inscrita no CNPJ: 02.092.332/0001-79, estabelecida na Calçada das Hortências,131 – Andar 2, Alphaville – SP- CEP: 06453-017, forneceu os itens abaixo relacionados, objetos das Ordens de Compra: OC 1336-1 e OC 1337-1 (Adesão a ARP nº 02/2020 do SEBRAE NACIONAL), cumprindo fielmente as obrigações assumidas.

Item ATA	Descrição dos Itens	Quant.
2	Solução de Hiperconvergência Tipo 2 Marca: Lenovo Modelo: ThinkAgile HX5520 Appliance	3
3	Switch Topo de Rack 48 portas 1/10G Marca: Arista Modelo: 7050X3	2
5	Cabo DAC/Twinax 3M	12
6	Cabo DAC/Twinax 1M	2
7	Transceiver 10BASE-SR SFP+	4
8	Fibra Óptica 15M	4
9	Serviço de Instalação e Configuração da Solução de Hardware e Software de Hiperconvergência com Repasse de Conhecimento	10
10	Serviço de Treinamento (até 10 pessoas)	1
11	Unidade de Serviços Técnicos (UST)	40

Os serviços de instalação, configuração e treinamento, foram satisfatórias, por profissionais capacitados, dentro dos prazos estipulados, não existindo em nossos registros até a presente data, nada que desabone sua conduta e responsabilidade com as obrigações assumidas.

Belém - PA, 31 de agosto de 2022.

Atenciosamente,

Dilma Farias Viana
Gerente Executiva de Tecnologia da Informação
Dilma Farias Viana
Gerente Executiva-TI
SESI/SENAI/FIEPA/IEL-PA

Bruno Ormanes Tamer
Coordenador de Infraestrutura - TI
Matrícula: 3789
SESI / SENAI - PA

Anexo de Capacidade Técnica - GLM SOFTWARE (2052516) SEI 2025.007562 / pg. 3510

ATESTADO DE CAPACIDADE TÉCNICA

A **VIACAO AGUIA BRANCA S A, situado a Av. Mario Gurgel, 5030 - Vila Capixaba – Cariacica -ES CEP: 29145-901, inscrito sobre o CPNJ nº 27486182/0001-09**, vem por meio deste **ATESTAR** que a empresa **CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO** LTDA, inscrita no CNPJ nº. 02.092.332/0001-79, estabelecida na Calçada das Hortências, 131 - Andar 2, Alphaville – SP - CEP: 06453-017, forneceu os itens abaixo relacionados, referente ao contrato nº 07181SR01V6, cumprindo fielmente as obrigações assumidas.

ITEM	DESCRIÇÃO	QUANTIDADE	N.F/DANFE
1	HARDWARE - EX-25GBE-OPTICAL - 25 Gigabit Ethernet Dual Port SFP28 Optical Option for all ExaGrid models. Includes two qualified SFP28 short-range Modules	5	DANFE Nº 7161 DANFE Nº 7162 N.F Nº 11033
2	HARDWARE - EX84 - Disk Capacity: Raw: 192 TB, Useable: 168 TB. 84 TB Full Backup. Includes 1 10 Gigabit Add on Card	5	
3	SOFTWARE - EX84-SW - 168 TB Tiered Backup Storage Software - Software Only	5	
SERVIÇOS - CARE PACK - GARANTIA			
4	EX-5YR-MS-P - Five Year 7 x 24 Customer Support and product Maintenance	1	

Declaramos ainda, que os serviços de instalação, suporte e garantia, foram executados satisfatoriamente, não existindo em nossos registros até a presente data, nada que desabone sua conduta e responsabilidade comercialmente ou tecnicamente.

DocuSigned by:
William Stauffer Telles
82C603E6917546A...

MINISTÉRIO DA DEFESA
SECRETARIA-GERAL
SECRETARIA DE PESSOAL, SAÚDE, DESPORTO E PROJETOS SOCIAIS
HOSPITAL DAS FORÇAS ARMADAS
DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

ATESTADO DE CAPACIDADE TÉCNICA - PREGÃO 93/2023-UASG 112408/HFA

O **HOSPITAL DAS FORÇAS ARMADAS – HFA**, situado a SETOR HFA, S/N, SETOR SUDOESTE, Brasília/DF, inscrito sobre o CNPJ Nº 03.568.867/0001-36, vem por meio deste **ATESTAR** que a empresa **CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO** LTDA, inscrita no CNPJ nº. 02.092.332/0001-79, estabelecida na Calçada das Hortências, 131 - Andar 2, Alphaville – SP - CEP: 06453-017, **FORNECEU** Appliance de Backup de 256TB, licenciamento de uso de software para Appliancede Backup de 256TB, instalação da Solução de Backup, serviço de garantia do Appliance com a duração de 60 meses e licenciamento de uso de software de Gerenciamento de Backup, cumprindo fielmente as obrigações assumidas.

ITEM	DESCRIÇÃO	QUANTIDADE	N.F/DANFE
1	Appliance de Backup de 256TB Fabricante: ExaGrid Modelo: EX52-SEC (2 unidades) Suporte/Garantia por 60 meses	1	DANFE 7053 NF 10534 NF 10535 NF 10836 NF 10837 NF 10839
2	Licenciamento de uso de software para Appliance de Backup de 256TB Fabricante: ExaGrid Modelo: 104 TB Tiered Backup Storage Software - Software Only (2 unidades) Suporte/Garantia por 60 meses	1	
3	Instalação da Solução de Backup	1	
4	Serviço de Garantia do Appliance com duração de 60 meses	1	
5	Licenciamento de uso de software de Gerenciamento de Backup Fabricante: Veeam Modelo: Veeam Data Platform Advanced Universal Subscription License. Includes Enterprise Plus Edition features. 5 Years Subscription Upfront Billing & Production (24/7) Support. Suporte/Garantia por 60 meses	160	

Declaramos ainda, que os serviços de instalação, suporte e garantia, foram executados satisfatoriamente, não existindo em nossos registros até a presente data, nada que desabone sua conduta e responsabilidade comercialmente ou tecnicamente.

Brasília, DF, 27 de março de 2025

Documento assinado digitalmente
gov.br
MARCO ANTONIO DE SOUZA FARIAS
Data: 27/03/2025 14:26:17-0300
Verifique em https://validar.iti.gov.br

_____

MARCO ANTONIO DE SOUZA FARIAS – Tenente-coronel
Chefe da Subdivisão de Gestão de Tecnologia da Informação

Assembleia Legislativa do Estado de Rondônia - ALE/RO

ATESTADO DE CAPACIDADE TÉCNICA

PREGÃOELETRÔNICO N° 006/2024/CPP/ALE/RO
PROCESSO ADMISTRATIVO Nº 100.173.000058/2024-00
UASG: 926919

A **Assembleia Legislativa do Estado de Rondônia,** situado Av. Farquar nº 2562 Bairro: Olaria 7º Andar. Porto Velho-RO CEP: 76801-189**, inscrito sobre o CPNJ nº 04.794.681/001-68**, vem por meio deste **ATESTAR** que a empresa **CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO** LTDA, inscrita no CNPJ nº. 02.092.332/0001-79, estabelecida na Calçada das Hortências, 131 - Andar 2, Alphaville – SP - CEP: 06453-017, forneceu *AQUISIÇÃO DE SOLUÇÃO HIPERCONVERGENTE NUTANIX, BEM COMO UMA SOLUÇÃO DE BACKUP E SEGURANÇA, INCLUINDO LICENCIAMENTO, INSTALAÇÃO, HORAS DE SERVIÇOS TÉCNICOS E TREINAMENTO*, cumprindo fielmente as obrigações assumidas do **CONTRATO Nº 014/ALE-RO/2024.**

ITEM	DESCRIÇÃO	QUANTIDADE	N.F
1	Servidor Hiperconvergente Nutanix – LENOVO - ThinkAgile HX630 V3 Certified Node - 7D6MNCM3WW	4	DANFE 7239 DANFE 7240 DANFE 7298 N.F 11814 N.F 11568 N.F 11622 N.F 11569 N.F 11621
2	Solução de Virtualização e Sistema de Armazenamento Definido por Software - SW-NCI-ULT-PR (Subscription, Nutanix Cloud Infrastructure (NCI) Ultimate Software License & Production Software Support Service for 1 CPU Core)	4	
3	SW-NUS-PRO-PR - Licença para File Server e Armazenamento de Objetos (NUS) 1TB - SW-NUS-PRO-PR (Subscription, Nutanix Unified Storage (NUS) Pro Software License & Production Software Support Service for 1 TiB of data stored)	40	
4	Software de Backup e Proteção de Dados – 10 VMs – Veeam - 5 Years Upfront Billing & Production (24/7) Support.	5	
5	EX36 - EXAGRID - Appliance de Backup - Five Year 7 x 24 Customer Support and Product Maintenance	2	
6	EXAGRID - Software para Appliance de Backup	2	
7	Serviço de Instalação de Servidor Hiperconvergente (itens 1 e 2)	4	
8	Serviço de Instalação de File Server (item 3)	1	
9	Serviço de Instalação de Solução de Proteção de Dados e Appliance de Backup (itens 4, 5 e 6)	1	
10	Unidade de Serviço Técnico (UST) - 1 Hora	170	
11	Treinamento Hands-On	24	

12	Cabo de conexão DAC SFP28 25 GbE com 5 metros - Compatível com Switch Aruba modelos: 8360v2 e 8325	14	
13	Cabo de conexão AOC QSFP28 100 GbE com 10 metros - Compatível com Switch Aruba modelos: 8360v2 e 8325	2	

Declaramos ainda, que os serviços de instalação, suporte e garantia, foram executados satisfatoriamente, não existindo em nossos registros até a presente data, nada que desabone sua conduta e responsabilidade comercialmente ou tecnicamente.

Porto Velho, 02 de abril de 2025

gov.br
Documento assinado digitalmente
RAFAEL RIBEIRO DA FROTA
Data: 02/04/2025 16:22:56-0300
Verifique em https://validar.iti.gov.br

Rafael Ribeiro da Frota
Diretor de Departamento STI-ALE/RO

ATESTADO DE CAPACIDADE TÉCNICA

A **CONVERGE DATA TECNOLOGIA DA INFORMACAO - CDTI**, **CNPJ: 20.621.724/0001-60,** vem por meio deste **ATESTAR** que a empresa **CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO LTDA**, inscrita no CNPJ nº. 02.092.332/0001-79, estabelecida na Calçada das Hortências, 131 - Andar 2, Alphaville – SP - CEP: 06453-017, forneceu a os itens abaixo relacionados, cumprindo fielmente as obrigações assumidas.

FABRICANTE NUTANIX

ITEM	DESCRIÇÃO	QUANTIDADE	N.F / DANFE
1	PartNumber: SW-NCP-PRO-PR - Subscription, Nutanix Cloud Platform Pro Software License & Production Software Support Service for 1 CPU Core	96	N.F – 10640
2	PartNumber: SW-NCP-NCI-ULT-PR - Subscription, (included in NCP) Nutanix Cloud Infrastructure (NCI) Ultimate Software License & Production Software Support Service for 1 CPU Core	96	
3	PartNumber: SW-NCP-NCM-PRO-PR - Subscription, (included in NCP) Nutanix Cloud Manager (NCM) Pro Software License & Production Software Support Service for 1 CPU Core	96	
4	Term-Months	38	
5	PartNumber: CNS-INF-A-SVC-DEP-PRO - Infrastructure Modernization Service Offering. HCI Cluster Deployment at single site quantity of nodes to deploy. Includes choice of one: Files, Objects, or Volumes.	3	
SERVIÇO E TREINAMENTO			
6	PartNumber: CNS-INF-FST-PC - Nutanix FastTrack for Prism IT Operations - Configure custom reports, Dashboards, Runway, and VM Right-sizing via X-Play	1	N.F - 10640

Declaramos ainda, que os serviços de instalação, suporte e garantia, foram executados satisfatoriamente, não existindo em nossos registros até a presente data, nada que desabone sua conduta e responsabilidade comercialmente ou tecnicamente.

Brasília (DF), 25 de março de 2025

MARCOS ALEX DE AGUIAR ALBANO:63489082168
Assinado de forma digital por MARCOS ALEX DE AGUIAR ALBANO:63489082168
Dados: 2025.03.25 16:27:57 -03'00'

Alex Aguiar
Diretor comercial
Converge Data Tecnologia da Informação

GOVERNO DO DISTRITO FEDERAL

DEPARTAMENTO DE TRÂNSITO DO DISTRITO FEDERAL

Direção-Geral

Diretoria de Administração Geral

Atestado de Capacidade Técnica n.º 15/2022 - DETRAN/DG/DIRAG Brasília-DF, 14 de julho de 2022.

ATESTADO DE CAPACIDADE TÉCNICA

Atestamos para os devidos fins que se fizerem necessários, com base nas informações prestadas pela Diretora Substituta de Tecnologia da Informação e Comunicação, a servidora Sra. ELAINE NOGUEIRA DA SILVA, matrícula 251.247-5, que a empresa **CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO LTDA**, inscrita sob o CNPJ nº: 02.092.332/0001-79, situada na Calçada das Hortências, nº 131 – Andar Piso 2, Alphaville – SP, CEP: 06453-017, forneceu através das Notas Fiscais nº 5458 – 5459 – 5460 – 6156 – 6157 – 6158 – 6159 - 6160, os itens abaixo relacionados, objetos do Contrato nº 25/2020, referente Adesão a ARP nº 270/2019-SUPEL RO, cumprindo fielmente as obrigações assumidas:

Descrição dos Itens	**Quant.**
Servidor Tipo 1 Hiperconvergente NUTANIX NX-8035-G7 Suporte/Garantia de 36 Meses	04
Servidor Tipo 2 Hiperconvergente NUTANIX NX-5155-G7 Suporte/Garantia de 36 Meses	05
Switch Tipo 1 ARISTA 7050X3 Suporte/Garantia de 36 Meses	02
Softwares e Garantias:	
1 Month A-Care Software & NBD Hardware Replacement/Same Day Ship for 7	02
Commvault Backup and Replication for Virtual Environment	06
COMMVAULT SUPP & MAINTENANCE SUB	06
Commvault Backup and Replication for Virtual Environment	12

COMMVAULT SUPP & MAINTENANCE SUB	12
License, AOS ULT entitlement & Production 24/7 System support bundle f	108
License, AOS ULT entitlement & Production 24/7 System support bundle f	108
L-FLASHTiB-ULT-PRD-3YR	16
L-FLASHTiB-ULT-PRD-3YR	16
License, AOS ULT entitlement & Production 24/7 System support bundle f	36
License, AOS ULT entitlement & Production 24/7 System support bundle f	72
L-FLASHTiB-ULT-PRD-3YR	06
L-FLASHTiB-ULT-PRD-3YR	11

Ademais, destacamos que os serviços de instalação e configuração foram executados de forma satisfatória, por profissionais capacitados, nos prazos estipulados, não existindo em nossos registros até a presente data, nada que desabone sua conduta e responsabilidade com as obrigações assumidas.

ANDERSON MOURA E SOUSA

Diretor de Administração Geral - DETRAN/DF

Documento assinado eletronicamente por **ANDERSON MOURA E SOUSA - Matr.164731-8**, **Diretor(a) de Administração Geral**, em 14/07/2022, às 11:29, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

A autenticidade do documento pode ser conferida no site: http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 verificador= **91052036** código CRC= **862A4A2A**.

DocuSign Envelope ID: 229DE0AA-708D-4060-800F-D13A5B03CA4E

ATESTADO DE CAPACIDADE TÉCNICA

A **SUL AMERICA COMPANHIA DE SEGURO SAUDE, CNPJ nº 61.585.865/0001-51**, Rua Beatriz Larragoiti Lucas, 121, Cidade Nova, Rio de Janeiro-RJ, CEP 20211-903, vem por meio deste **ATESTAR** que a empresa **CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO** LTDA, inscrita no CNPJ nº. 02.092.332/0001-79, estabelecida na Calçada das Hortências, 131 - Andar 2, Alphaville – SP - CEP: 06453-017, forneceu através das Notas Fiscais 5271 – 52901 – 52902 – 52903, os itens abaixo relacionados, cumprindo fielmente as obrigações assumidas.

Descrição dos Itens	**Quant.**
SW Nutanix: SW-FILES-AOS-TiB-PRD-3YR	40
SW Nutanix: Calm Std, 25 VM, valid for 3 yr	04
SW Nutanix: Frame Subscription, Named User, Monthly	15
SW Nutanix: License, AOS ULT entitlement & Production 24/7 System support bundle f	320
SW Nutanix: L-FLASHTiB-ULT-PRD-3YR	196
SW Nutanix: Prism Pro, 1 node, valid for 3 years	08
SW Nutanix: License, AOS ULT entitlement & Production 24/7 System support bundle f	96
SW Nutanix: L-OBJECTS-DED-PRD-3YR	10
SW Nutanix: L-FLASHTiB-ULT-PRD-3YR	147
SW Nutanix: Prism Pro, 1 node, valid for 3 years	3
PLACA DE MEMORIA DE 43,2 CM² DDR4-2933, 32GB, 1.2V, DIMM 288-PIN 2933MHZ	60
PLACA DE MEMORIA DE 43,2 CM² DDR4-2933, 64GB, 1.2V, DIMM 288-PIN 2933MHZ	24

Os serviços de instalação e configuração foram executados de forma satisfatória, por profissionais capacitados, dentro dos prazos estipulados, não existindo em nossos registros até a presente data, nada que desabone sua conduta e responsabilidade com as obrigações assumidas.

Rio de Janeiro, 24 de Março de 2021.

Nome_____ Adriana Lemos Praça

Cargo_____ Coordenadora de Infraestrutura

Assinatura e Carimbo CNPJ

DocuSigned by:
Adriana Lemos Praça
68BA61F51EB14F9...

PREFEITURA DE SÃO LUÍS

SECRETARIA MUNICIPAL DA FAZENDA – SEMFAZ

SUPERINTENDÊNCIA DA ÁREA DE INFORMÁTICA

ATESTADO DE CAPACIDADE TÉCNICA

SECRETARIA MUNICIPAL DA FAZENDA, CNPJ nº 06.307.102/0001-30, com sede na Avenida Dom Pedro II, S/N, Centro, São Luiz, MA, CEP: 65030-470, em por meio deste **ATESTAR** que a empresa **CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO** LTDA, inscrita no CNPJ nº. 02.092.332/0001-79, estabelecida na Calçada das Hortências, nº 131 – Andar Piso 2, Alphaville – SP - CEP: 06453-017, forneceu através das Notas Fiscais nº 5256 – 5884, os itens abaixo relacionados, objetos do Contrato nº 009/2020-SEMFAZ, referente Adesão a ARP nº 270/2019-SUPEL RO, cumprindo fielmente as obrigações assumidas.

Descrição dos Itens	Quant.
Servidor Tipo 1 Hiperconvergente NUTANIX NX-8135-G7 NUTANIX NX-8235-G7 Suporte/Garantia de 36 Meses	03
Softwares e Garantias: License, AOS ULT entitlement & Production 24/7 System support bundle f	72
Lic, AOS ULT entitlement & Production 24/7 System sup bundle f	36
L-FLASHTiB-ULT-PRD-3YR	08
L-FLASHTiB-ULT-PRD-3YR	04
S-HW-PRD-8235-G7-3YR	01
S-HW-PRD-8135-G7-3YR - HW Support 3 years	01
Veeam Availability Suite Enter Plus Includes 1	06
Veeam Availability Suite Enterprise Plus 1 year of Produc 24/7 Sup	06

Os serviços de instalação e configuração foram executados de forma satisfatória, por profissionais capacitados, dentro dos prazos estipulados, não existindo em nossos registros até a presente data, nada que desabone sua conduta e responsabilidade com as obrigações assumidas.

Atenciosamente,

Diego Lima Falcão
Superintendente da Área de Informática-SEMFAZ
CPF: 921.811.393-34
Matrícula: 51576-3

DIEGO LIMA FALCÃO

Superintendente da Área de Informática – SUAINFO/SEMFAZ

Matrícula 51.578-3

Anexo Atestados de Capacidade Técnica_CLM SOFTWARE (2052516) SEI 2025.007562 / pg. 3520

ATESTADO DE CAPACIDADE TÉCNICA

A empresa **EXATA TECNOLOGIA DA INFORMAÇÃO LTDA**, CNPJ nº **73.730.871/0001-34**, estabelecida na **Av. José Alves Nendo, 467, Zona 28-Gleba Ribeirão Pinguim, Maringá, PR, CEP: 87055-000**, vem através deste, **ATESTAR** que a empresa **CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO LTDA**, CNPJ nº. **02.092.332/0001-79**, estabelecida na **Calçada das Hortências, nº 131 - Piso 2**, **Centro Comercial Alphaville, Barueri, SP, CEP: 06453-017,** forneceu solução de backup para proteção de dados, incluindo ambiente virtualizado, servidores físicos e Microsoft 365.

Itens Fornecidos	NF
803- 1 Year Volume Rental - Minimum of 800 points per month - Includes 24/7	8091
803-1 Year Volume Rental - Minimum of 800 points per month - Includes 24/7	8265
1505-Monthly Price per Point for 1-Year Volume Rental Agreement - Minimum o	8383
1526- Monthly Price per Point for 1 Year Volume Rental Agreement - Minimum o	8555
1526 - Monthly Price per Point for 1 Year Volume Rental Agreement - Minimum o	8677
1526 - Monthly Price per Point for 1 Year Volume Rental Agreement - Minimum o	8845
1526 - Monthly Price per Point for 1 Year Volume Rental Agreement - Minimum o	8925
1526 - Monthly Price per Point for 1 Year Volume Rental Agreement - Minimum	9098
1526 - Monthly Price per Point for 1 Year Volume Rental Agreement - Minimum o	9255
1526 - Monthly Price per Point for 1 Year Volume Rental Agreement - Minimum o	9425
1526 - Monthly Price per Point for 1 Year Volume Rental Agreement - Minimum o	9600
1526-Monthly Price per Point for 1 Year Volume Rental Agreement - Minimum o	9729
1526-Monthly Price per Point for 1 Year Volume Rental Agreement - Minimum o	9901
3504- Monthly Price per Point for 1 Year Volume Rental Agreement - Minimum o	10024

Foram licenciados os softwares abaixo relacionados e suas respectivas quantidades:

Veeam Backup & Replication Enterprise Plus – Quant: 1.756
Veeam Backup for Microsoft 365 – Quant: 1.500
Veeam Cloud Connect & Public Cloud – Quant: 147
Veeam Recovery Orchestrator – Quant: 40

O serviço de Fornecimento de Licenciamento de Software de Backup Veeam, com garantia e suporte do fabricante, foi prestado satisfatoriamente, não existindo em nossos registros nada que desabone sua conduta com as obrigações assumidas.

Maringá, 12 de dezembro de 2023.

ANTONIO CARLOS GHIZZI ROGOSKI:39764621953

Assinado de forma digital por ANTONIO CARLOS GHIZZI ROGOSKI:39764621953
Dados: 2023.12.12 15:45:37 -03'00'

Antonio Carlos Ghizzi Rogoski

Diretor Institucional

EXATA TECNOLOGIA DA INFORMACAO LTDA.:73730871000134

Assinado de forma digital por EXATA TECNOLOGIA DA INFORMACAO LTDA.:73730871000134
Dados: 2023.12.12 15:45:56 -03'00'

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

OFÍCIO Nº 34.2026.CPL.2052519.2025.007562

Manaus, 22 de janeiro de 2026.

Ao Senhor

EUDO DE LIMA ASSIS JUNIOR

Diretor de Tecnologia da Informação e Comunicação – DTIC

Assunto: Análise de documentos de habilitação - Pregão Eletrônico Nº 94.001/2026-CPL/MP/PGJ.

Ao cumprimentá-lo cordialmente, e no âmbito do **PREGÃO ELETRÔNICO Nº 94.001/2026-CPL/MP/PGJ**, cujo objeto é a *contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma* ***solução de datacenter,*** *contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com* ***garantia de 60 (sessenta) meses***, **encaminho,** com base no item 10.2 do instrumento convocatório, **a "DECLARAÇÃO DE INDICAÇÃO DE PESSOAL TÉCNICO, INSTALAÇÕES E APARELHAMENTO** " (**doc 2052494) e os ATESTADOS DE CAPACIDADE TÉCNICA (doc. 2052516)** apresentados pela empresa **CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA** , inscrita no CNPJ n.º 02.092.332/0003-30, **para análise e manifestação dessa Diretoria de Tecnologia da Informação e Comunicação – DTIC.**

Sarah Madalena B. Côrtes de Melo

Pregoeira - Portaria Nº 66/2026/SUBADM

Documento assinado eletronicamente por **Sarah Madalena Barbosa Santos Cortes**, **Presidente da Comissão Permanente de Licitação - CPL**, em 22/01/2026, às 15:52, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2052519** e o código CRC **72B38EC0**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

PARECER Nº 6.2026.DTIC.2054079.2025.007562

PROCESSO DE COMPRA: 2025.007562

OBJETO: Contratação de empresa especializada para o **fornecimento, implantação, configuração e transferência de conhecimento infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado backup**, com garantia de 60 (sessenta) meses, para atender as necessidades institucionais do Ministério Público do Estado do Amazonas (M

ORIGEM: Pregão Eletrônico n.º 94.001/2026-CPL/MP/PGJ, Termo de Referência n.º 28.2025.DTIC.2002143.2025.007562.

1. RELATÓRIO

Trata-se de análise técnica de compatibilização dos documentos de habilitação da licitante **CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA.** , inscrita no CNPJ (MF) n.º 02.092.332/0003-30, constante dos documentos 2052494 e 2052516, encaminhado por meio do Ofício Nº 34.2026.CPL.2052519.2025.007562, conforme exigido no Edital e no Termo de Referência do Pregão Eletrônico em epígrafe.

Foram analisados os seguintes documentos:

- Declaração de indicação de pessoal técnico, instalações e aparelhamento;
- Conjunto de atestados de capacidade técnica emitidos por entes públicos e privados.

2. DA ANÁLISE

A análise da documentação de habilitação foi realizada nos termos do **item 3.2.2 do Termo de Referência** , o qual estabelece que a licitante deveria comprovar que dispõe de:

a) Pessoal técnico qualificado;

b) Instalações e aparelhamento adequados;

c) Experiência anterior compatível com o objeto licitado, mediante apresentação de atestados de capacidade técnica.

2.1 Da Declaração de pessoal técnico, instalações e aparelhamento

A licitante apresentou declaração formal, assinada por sua representante legal, na qual informa dispor de:

a) Pessoal técnico-operacional qualificado;

b) Instalações, infraestrutura e aparelhamento compatíveis com a execução do objeto;

c) Indicação nominal dos profissionais responsáveis pela execução técnica, com especialização em:

- Hiperconvergência;
- Backup;
- Virtualização;
- Redes.

O documento atende formal e materialmente ao item 3.2.2 do Termo de Referência, bem como ao disposto no art. 67, inciso III, da Lei nº 14.133/2021.

2,2 Dos Atestados de Capacidade Técnica

Foram apresentados diversos atestados de capacidade técnica, emitidos por órgãos e entidades de reconhecida relevância, que comprovam de forma consistente que a licitante já executou, de maneira satisfatória, fornecimentos e serviços compatíveis em complexidade, tecnologia e natureza com o objeto licitado.

2.1 CONCLUSÃO TÉCNICA

Após análise da documentação apresentada, verifica-se que a empresa **CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA.** comprovou satisfatoriamente sua capacitação técnico-operacional, atendendo integralmente às exigências estabelecidas no Edital e no Termo de Referência.

Não foram identificadas falhas formais ou materiais que comprometam a aceitabilidade da documentação apresentada.

Diante do exposto, a equite técnica **OPINA PELA ACEITAÇÃO** da documentação de capacitação técnica apresentada pela licitante, por atender às exigências editalícias e demonstrar aptidão técnica compatível com o objeto licitado.

É o parecer.

Manaus, 26 de janeiro de 2026.

ANTOVLA FROTA BEZERRA JÚNIOR
Técnico em Computação

EUDO DE LIMA ASSIS JUNIOR
Diretor de Tecnologia da Informação e Comunicação

Documento assinado eletronicamente por **Antovila Frota Bezerra Junior**, **Requisitado**, em 26/01/2026, às 15:33, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Eudo de Lima Assis Júnior**, **Diretor de Tecnologia da Informação e Comunicação (DTIC)**, em 26/01/2026, às 15:38, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2054079** e o código CRC **46304746**.

REPÚBLICA FEDERATIVA DO BRASIL

CADASTRO NACIONAL DA PESSOA JURÍDICA

NÚMERO DE INSCRIÇÃO	COMPROVANTE DE INSCRIÇÃO E DE SITUAÇÃO CADASTRAL	DATA DE ABERTURA
02.092.332/0003-30 **FILIAL**		**01/07/2019**

NOME EMPRESARIAL
CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA.

TÍTULO DO ESTABELECIMENTO (NOME DE FANTASIA)	PORTE
********	**DEMAIS**

CÓDIGO E DESCRIÇÃO DA ATIVIDADE ECONÔMICA PRINCIPAL
46.69-9-99 - Comércio atacadista de outras máquinas e equipamentos não especificados anteriormente; partes e peças

CÓDIGO E DESCRIÇÃO DAS ATIVIDADES ECONÔMICAS SECUNDÁRIAS
47.51-2-01 - Comércio varejista especializado de equipamentos e suprimentos de informática
62.02-3-00 - Desenvolvimento e licenciamento de programas de computador customizáveis
62.04-0-00 - Consultoria em tecnologia da informação
62.09-1-00 - Suporte técnico, manutenção e outros serviços em tecnologia da informação
85.99-6-03 - Treinamento em informática

CÓDIGO E DESCRIÇÃO DA NATUREZA JURÍDICA
206-2 - Sociedade Empresária Limitada

LOGRADOURO	NÚMERO	COMPLEMENTO
R SAMUEL MEIRA BRASIL	**394**	**SALA 29.SERRA PARQ LOGIS CONJ CB5**

CEP	BAIRRO/DISTRITO	MUNICÍPIO	UF
29.167-650	**TAQUARA II**	**SERRA**	**ES**

ENDEREÇO ELETRÔNICO	TELEFONE
RECEBIMENTOFISCAL@CLM.TECH	**(11) 2125-6270**

ENTE FEDERATIVO RESPONSÁVEL (EFR)
*****

SITUAÇÃO CADASTRAL	DATA DA SITUAÇÃO CADASTRAL
ATIVA	**01/07/2019**

MOTIVO DE SITUAÇÃO CADASTRAL

SITUAÇÃO ESPECIAL	DATA DA SITUAÇÃO ESPECIAL
********	********

Aprovado pela Instrução Normativa RFB nº 2.119, de 06 de dezembro de 2022.

Emitido no dia **19/01/2026** às **10:46:54** (data e hora de Brasília). Página: **1/1**

REPÚBLICA FEDERATIVA DO BRASIL

CADASTRO NACIONAL DA PESSOA JURÍDICA

NÚMERO DE INSCRIÇÃO	COMPROVANTE DE INSCRIÇÃO E DE SITUAÇÃO CADASTRAL	DATA DE ABERTURA
02.092.332/0001-79 **MATRIZ**		**07/02/1997**

NOME EMPRESARIAL
CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA.

TÍTULO DO ESTABELECIMENTO (NOME DE FANTASIA)	PORTE
********	**DEMAIS**

CÓDIGO E DESCRIÇÃO DA ATIVIDADE ECONÔMICA PRINCIPAL
47.51-2-01 - Comércio varejista especializado de equipamentos e suprimentos de informática

CÓDIGO E DESCRIÇÃO DAS ATIVIDADES ECONÔMICAS SECUNDÁRIAS
46.69-9-99 - Comércio atacadista de outras máquinas e equipamentos não especificados anteriormente; partes e peças
62.02-3-00 - Desenvolvimento e licenciamento de programas de computador customizáveis
62.04-0-00 - Consultoria em tecnologia da informação
62.09-1-00 - Suporte técnico, manutenção e outros serviços em tecnologia da informação
74.90-1-04 - Atividades de intermediação e agenciamento de serviços e negócios em geral, exceto imobiliários
85.99-6-03 - Treinamento em informática

CÓDIGO E DESCRIÇÃO DA NATUREZA JURÍDICA
206-2 - Sociedade Empresária Limitada

LOGRADOURO	NÚMERO	COMPLEMENTO
CALC DAS HORTENCIAS	**131**	**ANDAR PISO 2**

CEP	BAIRRO/DISTRITO	MUNICÍPIO	UF
06.453-017	**CONDOMINIO CENTRO COMERCIAL ALPHAVILLE**	**BARUERI**	**SP**

ENDEREÇO ELETRÔNICO	TELEFONE
PAGAMENTOS@CLM.COM.BR	**(11) 4191-6585**

ENTE FEDERATIVO RESPONSÁVEL (EFR)
*****

SITUAÇÃO CADASTRAL	DATA DA SITUAÇÃO CADASTRAL
ATIVA	**03/11/2005**

MOTIVO DE SITUAÇÃO CADASTRAL

SITUAÇÃO ESPECIAL	DATA DA SITUAÇÃO ESPECIAL
********	********

Aprovado pela Instrução Normativa RFB nº 2.119, de 06 de dezembro de 2022.

Emitido no dia **30/01/2026** às **12:38:21** (data e hora de Brasília). Página: **1/1**

Consulta Quadro de Sócios e Administradores - QSA

CNPJ:	02.092.332/0001-79
NOME EMPRESARIAL:	CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA.
CAPITAL SOCIAL:	R$2.100.000,00 (Dois milhões, cem mil reais)

O Quadro de Sócios e Administradores(QSA) constante da base de dados do Cadastro Nacional da Pessoa Jurídica (CNPJ) é o seguinte:

Nome/Nome Empresarial:	CLM VAD EXPERTS LTDA.		
Qualificação:	22-Sócio		
Nome do Repres. Legal:	THOMAS AYRES DE ARRUDA CAMARGO	**Qualif. Rep. Legal:**	05-Administrador

Nome/Nome Empresarial:	FRANCISCO JOSE DE ARRUDA CAMARGO
Qualificação:	49-Sócio-Administrador

Para informações relativas à participação no QSA, acessar o e-CAC com certificado digital ou comparecer a uma unidade da RFB.

Emitido no dia **30/01/2026** às **12:38** (data e hora de Brasília).

JUCESP - Junta Comercial do Estado de São Paulo

Ministério da Indústria, Comércio Exterior e Serviços
Departamento de Registro Empresarial e Integração – DREI
Secretaria de Desenvolvimento Econômico

ETIQUETA PROTOCOLO

JUCESP PROTOCOLO
0.532.413/19-2

172

29/5/19

CONTROLE INTERNET
025686855-7

CAPA DO REQUERIMENTO

DADOS CADASTRAIS

ATO
Abertura de Filial; Consolidação da Matriz;

NOME EMPRESARIAL
CLM SOFTWARE COMERCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA.

PORTE
Normal

JUCESP
ER 172 - SINCOMÉRCIO JUNDIAÍ
27 MAIO 2019
PROTOCOLO

LOGRADOURO	NÚMERO	COMPLEMENTO	CEP
Calcada das Hortências	131	Piso 2o. And	06453-017

MUNICÍPIO	UF	TELEFONE	EMAIL
Barueri	SP		

NÚMERO EXIGÊNCIA (S)	CNPJ - SEDE	NIRE - SEDE
0	02.092.332/0001-79	3521422805-2

IDENTIFICAÇÃO SIGNATÁRIO ASSINANTE REQUERIMENTO CAPA

NOME: SERGIO LUIS DE SOUZA (Procurador)

ASSINATURA:

DATA: 24/05/2019

VALORES RECOLHIDOS
DARE: R$ 145,91
DARF: R$ 21,00

SEQ. DOC.
1 / 1

DECLARO, SOB AS PENAS DA LEI, QUE AS INFORMAÇÕES CONSTANTES DO REQUERIMENTO/PROCESSO SÃO EXPRESSÃO DA VERDADE.

PARA USO EXCLUSIVO DA JUNTA COMERCIAL DO ESTADO DE SÃO PAULO (INCLUSIVE VERSO)

CARIMBO PROTOCOLO

JUCESP
ER 172 - SINCOMÉRCIO JUNDIAÍ
27 MAIO 2019
PROTOCOLO

CARIMBO DISTRIBUIÇÃO

CARIMBO ANÁLISE

JUCESP
SINCOMÉRCIO JUNDIAÍ
DEFERIDO
29 MAIO 2019
Leda Maria da Jesus
Assessora Técnica de Registro Publico
RG: 33.105.562-4

ANEXOS:

EXCLUSIVO SETOR DE ANÁLISE

( ) DBE
( ) Procuração
( ) Alvará Judicial
( ) Formal de Partilha
( ) Balanço Patrimonial
( ) Outros
( ) Documentos Pessoais
( ) Laudo de Avaliação
( ) Jornal
( ) Protocolo / Justificação
( ) Certidão

ETIQUETAS DE REGISTRO + CARIMBO

SECRETARIA DE DESENVOLVIMENTO ECONÔMICO - JUCESP
CERTIFICO O REGISTRO SOB O NÚMERO
288.012/19-7
GISELA SIMIEMA CESCHIN
SECRETÁRIA GERAL

JUCESP
29 MAIO 2019
SINCOMÉRCIO JUNDIAÍ

OBSERVAÇÕES:

SEM VALOR DE CERTIDÃO

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.007562 / pg. 3530

E.R. JUNDIAÍ 172

JUCESP

29 +5 19

28

SP
MÉRCIO
019
LO

ALTERAÇÃO CONTRATUAL Nº 09 DA SOCIEDADE EMPRESÁRIA LIMITADA

CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO LTDA.
CNPJ/MF 02.092.332/0001-79
NIRE 35214228052

1) **FRANCISCO JOSÉ DE ARRUDA CAMARGO**, brasileiro, casado sob o regime de comunhão de bens, engenheiro, RG nº 3.678.343 SSP/SP, CPF (MF) nº 201.723.628-49, residente e domiciliado nesta na Rua Dona Alcide Rios de Castro nº 79 – Vila Clementino – São Paulo/SP- CEP 04027-030; e

2) **CLM INFORMATICA LTDA.**, sociedade empresária limitada com sede na Alameda dos Nhambiquaras, 1.500, Lojas 1 e 2, Bairro Indianápolis, CEP 04090-003, esquina com Avenida Iraí, 438, São Paulo – SP, inscrita no CNPJ/MF sob o nº 96.465.844/0001-87, com contrato social arquivado na Junta Comercial do Estado de São Paulo NIRE nº 35.211.503.532 em sessão de 02/04/93, e posteriores alterações contratuais, neste ato representada por **FRANCISCO JOSÉ DE ARRUDA CAMARGO**, retro qualificado.

Únicos sócios da **CLM SOFTWARE COMERCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA.**, com sede no Município de Barueri, Estado de São Paulo, na Calçada das Hortências, nº 131, Piso 2º Andar, Condomínio Centro Comercial Alphaville, CEP: 06453-017, registrado na Junta Comercial de São Paulo, sob o NIRE nº 35.214.228.052 em sessão de 07/02/97, inscrita no CNPJ sob o nº 02.092.332/0001-79, resolvem de pleno acordo, e na melhor forma de direito, alterar o contrato social mediante cláusula e condições seguintes:

CLÁUSULA PRIMEIRA – Constituir filial na Rua Samuel Meira Brasil, nº 394, Sala n º 29, Serra Parque Logístico, Conjunto CB5, Taquara II, Serra, ES, CEP: 29167-650, tendo como objeto social: (a) comércio atacadista de material de informática, software e programas aplicativos, importação e exportação (CNAE 46.69-9/99); (b) comércio varejista de material de informática, software e programas aplicativos, importação e exportação (CNAE 47.51-2/01); (c) prestação de serviços para terceiros em manutenção de equipamentos (CNAE 62.09-1/00); (d) assessoria e consultoria em informática (CNAE 62.04-0/00); (e) treinamento em informática (CNAE 85.99-6/03); e (f) licenciamento ou cessão de uso de programas de informática (CNAE 62.02-3/00).

CLÁUSULA SEGUNDA – As demais cláusulas e condições do contrato inicial e alterações posteriores, não modificadas pelo presente instrumento, continuam em pleno vigor;

VISTO
CONFERIDO

SEM VALOR REGISTRÁRIO

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.007562 / pg. 3531

JUCESP
29 +5 19
29

CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA.
CNPJ/MF 02.092.332/0001-79
NIRE 35214228052

À vista da modificação ora ajustada **CONSOLIDA-SE** o contrato social, com a seguinte redação:

SOCIEDADE CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA.
CNPJ/MF 02.092.332/0001-79
NIRE 35214228052

Pelo presente instrumento particular, os abaixo assinados:

1) **FRANCISCO JOSÉ DE ARRUDA CAMARGO**, brasileiro, casado sob o regime de comunhão de bens, engenheiro, RG nº 3.678.343 SSP/SP, CPF (MF) nº 201.723.628-49, residente e domiciliado nesta na Rua Dona Alcide Rios de Castro nº 79 – Vila Clementino – São Paulo/SP- CEP 04027-030; e

2) **CLM INFORMATICA LTDA.**, sociedade empresária limitada com sede na Alameda dos Nhambiquaras, 1.500, Lojas 1 e 2, Bairro Indianápolis, CEP 04090-003, esquina com Avenida Iraí, 438, São Paulo – SP, inscrita no CNPJ/MF sob o nº 96.465.844/0001-87, com contrato social arquivado na Junta Comercial do Estado de São Paulo NIRE nº 35.211.503.532 em sessão de 02/04/93, e posteriores alterações contratuais, neste ato representada por **FRANCISCO JOSÉ DE ARRUDA CAMARGO**, retro qualificado.

CAPÍTULO I – DA DENOMINAÇÃO, SEDE, DURAÇÃO E OBJETO.

CLÁUSULA PRIMEIRA – A sociedade gira sob o nome empresarial CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA., com sede e foro no Município de Barueri, Estado de São Paulo, na Calçada das Hortências, nº 131, Piso 2º. Andar, Condomínio Centro Comercial Alphaville, CEP: 06453-017.

Parágrafo Único – A sociedade possui as seguintes filiais:

Filial 1 – Na Rua Mario Lobo, nº 61 – sala 1309 – Bairro Centro – CEP 89201-330, Joinville/SC. Inscrita no CNPJ/MF sob o nº 02.092.332/0002-50, com registro na Junta Comercial do Estado de Santa Catarina sob o nº 42901098722 em 08/010/2015, tendo como objeto social a exploração dos ramos de: Comércio Varejista e atacadista de material de informática, software e programas aplicativos, importação e exportação; Prestação de serviços para terceiros em manutenção de equipamentos, locação e intermediação de negócios com

VISTO
CONFERIDO

SEM VALOR DE CERTIDÃO
Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.007562 / pg. 3532

JUCESP
29 +5 19
23

SEM VALOR DE CERTIDÃO

equipamento de informática; Assessoria, treinamento e consultoria em informática e licenciamento ou cessão de uso de programas de informática;

Filial 2 – Na Rua Samuel Meira Brasil, nº 394, Sala n º 29, Serra Parque Logístico, Conjunto CB5, Taquara II, Serra, ES, CEP: 29167-650., tendo como objeto social: (a) comércio atacadista de material de informática, software e programas aplicativos, importação e exportação (CNAE 46.69-9/99); (b) comércio varejista de material de informática, software e programas aplicativos, importação e exportação (CNAE 47.51-2/01); (c) prestação de serviços para terceiros em manutenção de equipamentos (CNAE 62.09-1/00); (d) assessoria e consultoria em informática (CNAE 62.04-0/00); (e) treinamento em informática (CNAE 85.99-6/03); e (f) licenciamento ou cessão de uso de programas de informática (CNAE 62.02-3/00)..

CLÁUSULA SEGUNDA – A sociedade tem por objeto social: Comércio Varejista e atacadista de material de informática, software e programas aplicativos, importação e exportação; Prestação de serviços para terceiros em manutenção de equipamentos, locação e intermediação de negócios com equipamento de informática; Assessoria, treinamento e consultoria em informática e licenciamento ou cessão de uso de programas de informática.

CLÁUSULA TERCEIRA – O prazo de duração da sociedade é indeterminado.

CAPÍTULO II – DO CAPITAL SOCIAL.

CLÁUSULA QUARTA - O capital social é de R$ 2.100.000,00 (dois milhões e cem mil reais), dividido em 2.100.000 (dois milhões e cem mil) quotas no valor nominal de R$ 1,00 (um real) cada uma, assim distribuídas entre os sócios:

SÓCIOS	QUOTAS	VALOR EM R$	PERCENTUAL
FRANCISCO JOSÉ DE ARRUDA CAMARGO	1.365.000	1.365.000,00	65,00%
CLM INFORMÁTICA LTDA.	735.000	735.000,00	35,00%
TOTAL	**2.100.000**	**2.100.000,00**	**100,00%**

Parágrafo 1º - Nenhuma quota poderá ser vendida, cedida, transferida ou, por qualquer forma alienada sem aprovação do outro sócio, além de lhe ficar assegurado, mediante aviso por escrito através de Cartório de Títulos e Documentos, com antecedência de 30 (trinta) dias, o direito de preferência na sua aquisição em igualdade de condições com terceiro interessado em adquiri-la, sendo nula e ineficaz em relação à sociedade a venda, cessão,

VISTO
CONFERIDO

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2020.0.[illegible].3533

JUCESP
29 *5 19
28

SEM VALOR DE CERTIDÃO

doação, transferência ou alienação, concluída com inobservância no disposto neste parágrafo.

Parágrafo 2º - A falta de resposta com relação ao exercício do direito de preferência implicará na decadência do direito de preferência.
Parágrafo 3º - A responsabilidade dos sócios é restrita ao valor de suas quotas, mas todos os sócios respondem solidariamente pela integralização do capital social.

Parágrafo 4º - As quotas são indivisíveis em relação à sociedade e cada quota dá direito a um voto em todas as decisões sociais.

CAPITULO III – DA ADMINISTRAÇÃO.

CLÁUSULA QUINTA - A sociedade será administrada **exclusiva e isoladamente** pelo sócio FRANCISCO DE ARRUDA CAMARGO que fica dispensado de prestar caução, e que usará a designação de sócio administrador, podendo praticar todos os atos necessários ao regular funcionamento da sociedade, firmar contratos de qualquer natureza em especial arrendamento, locação, empréstimos, abertura de contas correntes e crédito, nomear procuradores com clausula "ad judicia", representar a sociedade perante terceiros, enfim, terá o mais amplo e geral poder de administração, desde que enquadrados no objeto social.

Parágrafo 1º - A sociedade através do sócio administrador poderá nomear procuradores para praticar atos em nome da sociedade, sendo certo que os instrumentos de procuração deverão conter poderes específicos e prazos de validade limitados, executando-se, quanto a esta última exigência, as procurações com cláusulas *"Ad judiciais"*.

Parágrafo 2º - São expressamente vedados, sendo nulos e inoperantes em relação à sociedade, os atos quotistas, procuradores ou funcionários que a envolverem em obrigações relativas à negócios ou operações estranhas aos objetivos sociais, tais como, alienações ou alterações do ativo imobilizado da sociedade, renúncia de direitos, empréstimos bancários, fianças avais, endossos ou quaisquer outras garantias em favor de terceiros, exceto à empresas do mesmo grupo econômico desde que devidamente representada pelo sócio administrador.

Parágrafo 3º - Quando em exercício o Sócio Administrador receberá o "pró-labore" que for fixado pelos sócios em reunião geral.

VISTO
CONFERIDO

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.00[illegible] Pág. 3534

JUCESP
29 *5 19
28

SEM VALOR DE CERTIDÃO

CAPITULO IV – DO EXERCÍCIO SOCIAL E DEMONSTRAÇÕES FINANCEIRAS.

CLÁUSULA SEXTA - O exercício social coincidirá com o ano civil, encerrando-se em 31 de dezembro.

CLÁUSULA SÉTIMA - Ao fim de cada exercício social serão elaboradas as demonstrações financeiras, feitas as necessárias amortizações e deduções para as reservas legais e as julgadas convenientes.

Parágrafo 1º - As quotas da administração e a destinação dos lucros líquidos anualmente obtidos serão aprovadas por sócio ou sócios titulares de mais da metade do capital social, garantida a todos os sócios a sua participação obedecida a proporção das quotas detidas por cada sócio.

Parágrafo 2º - Os sócios participarão dos lucros e suportarão os prejuízos na proporção das respectivas participações no capital social, podendo a sociedade levantar balanços intermediários, intercalares ou em intervalos menores, para efeito de verificação e distribuição de lucros.

CAPITULO V – DAS DECISÕES SOCIAIS, DISSOLUÇÃO E EXCLUSÃO DE SÓCIOS.

CLÁUSULA OITAVA - Todas as decisões da sociedade serão tomadas por quotistas que representem a maioria do capital social, em reunião dos sócios convocada pelo administrador da sociedade, em especial as referentes à aprovação das contas, modificação dos estatutos, incorporação, fusão, transformação ou dissolução da sociedade, oneração de bens imóveis, que serão tomadas em assembleia especialmente convocada pela administração da sociedade.
Parágrafo 1º - As Assembleias de quotistas serão sempre convocadas pelo sócio administrador, através de carta ou comunicado aos demais quotistas com antecedência mínima de 10 (dez) dias da data de realização da assembleia.

Parágrafo 2º - A reunião dos sócios poderá ser dispensada nos casos expressamente previstos neste contrato social, assim como no caso de todos os sócios decidirem, por escrito, sobre a matéria a ela sujeita.

VISTO
CONFERIDO

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.007562 / pg. 3535

JUCESP
29 +5 19
28

Parágrafo 3º - Ficam dispensadas as formalidades da convocação sempre que todos os sócios comparecerem ou se declararem, por escrito, cientes do local, data, hora, e ordem do dia da reunião.

Parágrafo 4º - A reunião de sócios instala-se com a presença, em primeira convocação, de titulares de, no mínimo, mais da metade do capital social, e, em seguida convocação, com qualquer número.

Parágrafo 5º - As reuniões serão presididas por sócio, representante de sócio, administrador ou terceiro designado pela maioria dos presentes, cabendo ao presidente da reunião a escolha do secretário, sendo que dos trabalhos e deliberações será lavrada, no livro de atas de reunião, ata assinada pelos membros da mesa e pelos sócios presentes, quantos bastem para a validade das deliberações, mas sem prejuízo dos que queiram assiná-la.

Parágrafo 6º - Cópia da ata autenticada pela administração ou pela mesa será apresentada ao Registro de Empresas Mercantis para arquivamento e averbação.

Parágrafo 7º - Competirá a cada quota um voto nas deliberações sociais.

Parágrafo 8º - Serão realizadas, ordinariamente, reuniões de quotistas até o último dia útil do quarto mês seguinte ao encerramento do exercício social, para deliberar sobre o resultado do exercício encerrado, destinação do resultado e outros assuntos de interesse da sociedade e que conste da ordem do dia.

CLÁUSULA NONA - O contrato social poderá ser modificado, no todo ou em parte, por deliberação da Assembleia especialmente convocada para este fim, respeitando-se o disposto na clausula 8º e seus parágrafos.

CLÁUSULA DÉCIMA - A sociedade poderá entrar em liquidação por decisão dos sócios que representem a maioria do capital social, cabendo ao sócio Francisco Jose de Arruda Camargo indicar o liquidante. Nessa hipótese os haveres da sociedade serão empregados na liquidação de suas obrigações e o remanescente, se houver, será rateado entre os sócios em proporção ao número de quotas que cada um possuir. Encerrada a liquidação a sociedade será declarada extinta por deliberação do sócio ou sócios de mais da metade do capital social.

VISTO
CONFERIDO

SEM VALOR DE CERTIDÃO
Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.007562 / pg. 3536

JUCESP
29 *5 19
28

CLÁUSULA DÉCIMA PRIMEIRA - A morte, interdição, insolvência ou retirada de qualquer deles não importará na dissolução da sociedade. Na hipótese de falecimento de qualquer um dos sócios quotistas, os herdeiros do sócio falecido de comum acordo, exercerão o direito à quota. Entretanto, não havendo interesse destes em participar da sociedade, realizar-se à balanço especial, na data do evento, quando serão apurados os haveres, sendo feito o pagamento das quotas de capital em 36 (trinta e seis) parcelas mensais, iguais e consecutivas, acrescidas de juros e correções legais, pagáveis a primeira 90 (noventa) dias da abertura da sucessão ou da retirada do sócio.

Parágrafo 1º - No caso de falecimento de um sócio quotista havendo interesse de mais de um herdeiro em permanecer com as quotas, as mesmas serão transferidas em caráter *"pro-indiviso"* aos sucessores, os quais nomearão um só entre eles para representá-los junto a sociedade.

Parágrafo 2º - Os poderes de gerência, satisfeita a condição do parágrafo anterior, somente serão conferidos ao sócio substituído por alteração contratual.

Parágrafo 3º - No caso de dissolução de sociedade conjugal de quaisquer dos sócios, não poderá o sócio que vier a se separar partilhar suas quotas sociais sem previa e expressa autorização do outro sócio, autorização esta que em momento algum poderá ser presumida.

CLÁUSULA DÉCIMA SEGUNDA - De acordo com o artigo 1.085 do Código Civil, quando a maioria dos sócios, representativa de mais da metade do capital social, entender que um ou mais sócios estão pondo em risco a continuidade da empresa, em virtude de atos de inegável gravidade, poderão exclui-los da sociedade por justa causa e extrajudicialmente.

CAPITULO VI – FUSÃO, INCORPORAÇÃO, CISÃO E TRANSFORMAÇÃO.

CLAUSULA DÉCIMA TERCEIRA - A sociedade poderá ser fundida ou incorporada a qualquer tempo, por deliberação de sócios ou sócios titulares de, no mínimo, ¾ (três quartos) do capital social.

CLÁUSULA DÉCIMA QUARTA - A sociedade poderá ser cindida ou transformada, a qualquer tempo, por deliberação de sócios ou sócios titulares de mais da metade do capital social.

VISTO CONFERIDO

SEM VALOR DE CERTIDÃO
Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.007582 / pg. 3537

JUCESP
29 MAI 19
28

CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA.
CNPJ/MF 02.092.332/0001-79
NIRE 35214228052

CAPITULO VII - DAS DISPOSIÇÕES.

CLÁUSULA DÉCIMA QUINTA - A sociedade não terá Conselho Fiscal.

CLÁUSULA DÉCIMA SEXTA - Os sócios declaram que não estão incursos em nenhum dos crimes previstos em Lei, que os impeçam de exercer as atividades sociais, constantes do artigo 1011 do Código Civil Brasileiro.

CLÁUSULA DÉCIMA SÉTIMA - A sociedade será regida pelo disposto neste contrato social, bem como pelo estabelecido nos artigos 1.052 a 1.087 da Lei 10.406 de 10 de janeiro de 2002 (Código Civil), aplicando-se, nos termos do parágrafo único do artigo 1.053 do Código Civil, supletivamente, as disposições do presente contrato, no que couber, as normas da sociedade anônima.

CLÁUSULA DÉCIMA OITAVA - As partes indicam o foro da Comarca de São Paulo, Estado de São Paulo, para dirimir as dúvidas oriundas do presente instrumento.

E por acharem em perfeito acordo, em tudo quanto neste instrumento particular foi lavrado, obrigam-se a cumprir o presente contrato, assinando-o na presença de duas testemunhas abaixo, em 03 (três) vias de um só teor e efeito.

E, por estarem assim justos e contratados, lavram este instrumento.

Barueri/SP, 24 de maio de 2019

29º TABELIÃ DE NOTAS

Francisco José de Arruda Camargo

29º TABELIÃ DE NOTAS

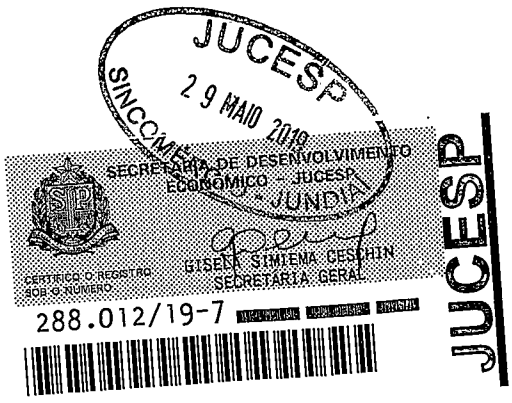
CLM INFORMÁTICA LTDA.
Representada por:
Francisco José de Arruda Camargo

VISTO CONFERIDO

SEM VALOR DE CERTIDÃO

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.007562 / pg. 3538

SEM VALOR DE CERTIDÃO



JUCESP

29 MAI 19

PROCURAÇÃO

28

Barueri, 6 de maio de 2.019.

OUTORGANTE:

CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA, com sede e foro no Município de Barueri/SP, Calçada das Hortências, nº 131 – Andar 2 – Centro Comercial Alphaville - CEP: 06.453-017, devidamente inscrita no CNPJ/MF sob o nº 02.092.332/0001-79, representada por **FRANCISCO JOSÉ DE ARRUDA CAMARGO**, brasileiro, maior, casado, Engenheiro, portador da cédula de identidade - RG nº 3.678.343 SSP/SP e devidamente inscrito no CPF n° 201.723.628-49, residente e domiciliado na Rua Alcide Rios de Castro, nº 79 – Indianópolis – São Paulo/SP – CEP: 04027-030.

OUTORGADOS:

JAIRO DOMINGUES LEITE, brasileiro, maior, casado, Administrador de empresas, residente e domiciliado à Avenida Jacutinga 343, apartamento 84, Bairro Moema, 04515-030 São Paulo/SP, portadora da cédula de identidade - RG n.º 6.272.749-7 - SSP/SP, e devidamente inscrita no CPF/MF sob o n.º 698.385.508-68.

SÉRGIO LUÍS DE SOUZA, brasileiro, maior, casado, Contabilista, residente e domiciliado à Rua Nicola Rivelli, 102, Bairro Vila Bela I, 13209-620, Jundiaí/SP, portador da cédula de identidade - RG n.º 16.365.544-3 - SSP/SP, devidamente inscrito no CPF/MF sob o n.º 047.884.368-25 e com inscrição no CRC/SP sob o n.º. 1SP164249/O-9.

ALEXANDRE NICACIO QUEIROZ, brasileiro, maior, casado, Administrador, residente e domiciliado à Rua Gaita de Foles, 99, Bairro Jardim Tangará, 04933-040 São Paulo/SP, portadora da cédula de identidade - RG n.º 22.742.871-7 - SSP/SP, e devidamente inscrito no CPF/MF sob o n.º 184.685.388-50.

CÍCERA RIBEIRO DE SOUZA, brasileira, maior, solteira, Contabilista, residente e domiciliada à Rua Eulo Maroni, 170, Bloco 08, apartamento 42, Bairro Jaguaré, 05338-100 São Paulo/SP, portadora da cédula de identidade - RG n.º 38.819.988-X - SSP/SP, e devidamente inscrita no CPF/MF sob o n.º 387.481.663-00.

CLM SOFTWARE
CALÇADA DAS HORTÊNCIAS, 131
OFFICE 2 º FLOOR, ALPHAVILLE,
BARUERI. SP, BRAZIL, 06453-017
PHONE· +55 11 4191 6585

FILIAL SANTA CATARINA
RUA MARIO LOBO, 61. SALA 1309 B
BAIRRO CENTRO 89201-330
JOINVILLE. SC

www.clm com br

CLMX CORPORATION
1310 PARK CENTRAL, BLVD
SOUTH, SUITE B89, 33064,
POMPANO BEACH, FL, USA,
PHONE: +1-305-716-9775
www clm10.com

CLM COLOMBIA
CALLE 97A # 9 - 45,
OFFICE 207, BOGOTÁ,
COLOMBIA
PHONE: +57-1-702-2011
www.clm.com.co

CLM PERU
AV PASEO DE LA REPÚBLICA,
3147, OFFICE 502, SAN ISIDRO,
LIMA PERU
PHONE: +51
www.clm.com

29º TABELIA DE NOTAS DA CAPITAL
PRESENTE DE C. T. P. L. AGAPITO
AUTENTICAÇÃO: AUTENTICO A PRESENTE
CÓPIA REPROGRÁFICA EXTRAIDA
NESSAS NOTAS CONFORME ORIGINAL
APRESENTADO, DOU FÉ.
16 MAIO 2019
PIAUÍ
R$ 3,60
VÁLIDO SOMENTE COM SELO DE AUTENTICIDADE
COLÉGIO NOTARIAL DO BRASIL
LEOMAR BEZERRA DOS SANTOS
ESCREVENTE AUTORIZADO
112383
AUTENTICAÇÃO
AU083AH07548688

SEM VALOR PROBATÓRIO
Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.007562 / pg. 3340

JUCESP
29 MAI 19

CLM

FINALIDADES DA PROCURAÇÃO:

PODERES PERTINENTES: Através do presente instrumento particular de mandato, a OUTORGANTE nomeia e constitui como seus procuradores os OUTORGADOS acima, para representá-la em conjunto ou separadamente, perante as autoridades e órgãos governamentais Federal, Estadual e Municipal defender os interesses da OUTORGANTE; efetuar regularização, alteração e encerramento perante qualquer órgão da administração pública abrangendo as três esferas, Federal, Estadual e Municipal; requerer o registro de sua Constituição, de suas alterações contratuais, e distratar, perante Juntas Comerciais, Ministério da Fazenda, Ministério da Justiça, Cartórios e demais órgãos públicos, onde se fizer necessário; providenciar requerimentos, juntar, apresentar documentos, solicitar extração de cópias; representá-la em entidades ou órgãos da Administração Pública direta e indireta, sejam elas federais, estaduais e municipais, autarquias, Ministérios, Departamentos e Secretarias Estaduais e Municipais, em especial nas Secretarias da Fazenda de todas as Unidades Federativas do Brasil, Delegacias, Inspetoria, Postos de Fiscalização, Previdência Social junto ao Instituto Nacional da Seguridade-INSS, Prefeituras, Vigilância Sanitária, Corpo de Bombeiros, Juntas Comerciais, Sindicatos de Classe, Procuradorias Federais, Estaduais e Municipais, e onde for mais mister, juntar e retirar papéis e documentos, solicitar informações, solicitar certidões, inclusive, certidões com finalidade de baixa nos órgãos públicos aqui mencionados, certificados, autorizações, permissões, cadastrar senhas eletrônicas, efetuar cadastros no Certificado de Regularidade Fiscal-CRF da Caixa Econômica Federal-CEF, inscrever, alterar e baixar registros, realizar inscrições, alterações e encerramentos nos Conselhos Regionais e Órgãos de Classe, receber correspondências, notificações, promover parcelamento de tributos municipais, estaduais e federais, efetuar pesquisas junto aos órgãos públicos incluindo as três esferas de poder (federal, estadual e municipal) e em especial, poderes amplos e gerais para pesquisas na Receita Federal do Brasil; substabelecer os poderes a terceiros, sem reservas; usar os fins deste mandato, tudo na defesa dos direitos e interesses da OUTORGANTE, obrigando-se à prestação de contas quando requisitada, a qualquer tempo. A procuração é firmada ainda com poderes para representação perante a Receita Federal do Brasil e o Banco Central. Podendo a outorgada praticar todos e quaisquer atos para o bom e fiel desempenho do presente mandato, que terá validade pelo prazo de 03 (três) anos a contar desta data.

29º TABELIÃ DE NOTAS

CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA
Representada por Francisco José de Arruda Camargo

Reconheço, por semelhança, a firma de: (1) FRANCISCO JOSE DE ARRUDA CAMARGO, em documento sem valor econômico, dou fé.
São Paulo, 08 de maio de 2019. (Otd 1 Total R$ 6,25)
Em Testº _____ da verdade. Cód. [2003031915541010810818-009287]
CLEOMAR BEZERRA DOS SANTOS - Escrevente Autorizada
Selo(s): 1 Ato: AA-08631

FIRMA 1
AA08631195

CLM SOFTWARE
CALÇADA DAS HORTÊNCIAS, 131
OFFICE 2º FLOOR ALPHAVILLE.
BARUERI SP BRAZIL. 06453 017
PHONE +55 11 4191 6585

FILIAL SANTA CATARINA
RUA MARIO LOBO 61 SALA 1309 B
BAIRRO CENTRO 89201 330
JOINVILLE SC

www.clm.com.br

CLMX CORPORATION
1310 PARK CENTRAL BLVD
SOUTH, SUITE B89. 33064
POMPANO BEACH FL. USA.
PHONE +1 305 716 9775
www.clm10.com

CLM COLOMBIA
CALLE 97A # 9-515,
OFFICE 207. BOGOTA
COLOMBIA
PHONE +57-1 702 2011
www.clm.com.co

CLM PERU
AV PASEO DE LA REPUBLICA
3147, OFFICE 502. SAN ISIDRO
LIMA PERU
PHONE +51 1 [illegible]
www.clm.com.pe

29º TABELIÃ DE NOTAS DA CAPITAL
PRISCILA DE C. T. P. L. AGAPITO
AUTENTICAÇÃO: AUTENTICO A PRESENTE CÓPIA REPROGRÁFICA EXTRAÍDA NESSAS NOTAS CONFORME ORIGINAL APRESENTADO, DOU FÉ.
16 MAIO 2019
PIAUÍ R$ 3,40
VALIDO SOMENTE COM SELO DE AUTENTICIDADE
COLÉGIO NOTARIAL DO BRASIL
CLEOMAR BEZERRA DOS SANTOS
ESCREVENTE AUTORIZADO
112383
AUTENTICAÇÃO
AU10831JL0754869

SEM VALOR FISCAL
Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.0075[illegible]

GOVERNO DO ESTADO DE SÃO PAULO
SECRETARIA DE DESENVOLVIMENTO ECONÔMICO
JUNTA COMERCIAL DO ESTADO DE SÃO PAULO

FICHA CADASTRAL COMPLETA

OS DADOS DESTA PRIMEIRA PAGINA CONSTANTES DOS QUADROS CAPITAL - ENDERECO - OBJETO E TITULAR/SOCIO/DIRETORIA REFEREM-SE A SITUACAO DA EMPRESA NO MOMENTO DE SUA CONSTITUICAO OU AO SEU PRIMEIRO REGISTRO CADASTRADO.

A SEGUIR, SÃO INFORMADOS OS EXTRATOS DOS ARQUIVAMENTOS POSTERIORMENTE REALIZADOS, SE HOUVER.

A AUTENTICIDADE DESTA FICHA CADASTRAL COMPLETA PODERÁ SER CONSULTADA NO SITE WWW.JUCESPONLINE.SP.GOV.BR, MEDIANTE O CÓDIGO DE AUTENTICIDADE INFORMADO AO FINAL DESTE DOCUMENTO.

PARA EMPRESAS CONSTITUÍDAS ANTES DE 1.992, OS ARQUIVAMENTOS ANTERIORES A ESTA DATA DEVEM SER CONSULTADOS NA FICHA DE BREVE RELATO (FBR).

EM SEGUIDA, SÃO APRESENTADOS TODOS ATOS ARQUIVADOS EM ORDEM CRONOLÓGICA

EMPRESA

CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA.

TITULO DE ESTABELECIMENTO		TIPO
		SOCIEDADE LIMITADA
NIRE MATRIZ	DATA DA CONSTITUIÇÃO	EMISSÃO
35214228052	07/02/1997	30/01/2026 12:15:31
INÍCIO DE ATIVIDADE	CNPJ	INSCRIÇÃO ESTADUAL
10/01/1997	02.092.332/0001-79	

CAPITAL

R$ 38.000,00 (TRINTA E OITO MIL REAIS)

ENDEREÇO

LOGRADOURO: RUA ABEL	NÚMERO: 15	
BAIRRO: JD. SAO PEDRO	COMPLEMENTO: SALA 01	
MUNICÍPIO: BARUERI	CEP: 06402-220	UF: SP

OBJETO SOCIAL

REPRESENTANTES COMERCIAIS E AGENTES DO COMÉRCIO DE MEDICAMENTOS, COSMÉTICOS E PRODUTOS DE PERFUMARIA
COMÉRCIO ATACADISTA DE MÁQUINAS E EQUIPAMENTOS PARA USO INDUSTRIAL; PARTES E PEÇAS
COMÉRCIO VAREJISTA DE OUTROS PRODUTOS NÃO ESPECIFICADOS ANTERIORMENTE

TITULAR / SÓCIOS / DIRETORIA

CLM INFORMATICA LTDA., NIRE: 35211503532, SITUADA À RUA ATICA, 150, AEROPORTO, SAO PAULO - SP, CEP 04634-040, OCUPANDO CARGO DE SÓCIO. COM VALOR DE PARTICIPAÇÃO NA SOCIEDADE DE $ 17.000,00.

FRANCISCO JOSE DE ARRUDA CAMARGO, RAÇA/COR: NÃO DECLARADA., NACIONALIDADE BRASILEIRA, CPF: 201.723.628-49, RG/RNE: 3678343, RESIDENTE À RUA ALCIDES RIOS DE CASTRO, 79, INDIANOPOLIS, SAO PAULO - SP, CEP 04027-030, OCUPANDO CARGO DE SÓCIO GERENTE E DIRETOR, ASSINANDO PELA EMPRESA. COM VALOR DE PARTICIPAÇÃO NA SOCIEDADE DE $ 21.000,00

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.007562 / pg. 3542

ARQUIVAMENTOS
SESSÃO: 07/02/1997
INCLUSÃO DE CNPJ 02.092.332/0001-79
NUM.DOC: 114.732/05-0 SESSÃO: 15/04/2005
CONSOLIDAÇÃO CONTRATUAL DA MATRIZ.
NUM.DOC: 265.641/05-6 SESSÃO: 15/09/2005
ENDEREÇO DA SEDE ALTERADO PARA PRACA DAS PAPOULAS, 30, CONJ. C 1 A, CENTRO COMERCIAL, BARUERI - SP, CEP 06453-000.
CONSOLIDAÇÃO CONTRATUAL DA MATRIZ.
NUM.DOC: 337.669/09-0 SESSÃO: 09/09/2009
ALTERAÇÃO DA ATIVIDADE ECONÔMICA / OBJETO SOCIAL DA SEDE PARA COMÉRCIO VAREJISTA ESPECIALIZADO DE EQUIPAMENTOS E SUPRIMENTOS DE INFORMÁTICA, SUPORTE TÉCNICO, MANUTENÇÃO E OUTROS SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO.
CONSOLIDAÇÃO CONTRATUAL DA MATRIZ.
NUM.DOC: 357.664/11-5 SESSÃO: 16/09/2011
CAPITAL DA SEDE ALTERADO PARA $ 238.000,00 (DUZENTOS E TRINTA E OITO MIL REAIS)CAPITAL INTEGRALIZADO DE $ 238.000,00 (DUZENTOS E TRINTA E OITO MIL REAIS).
REDISTRIBUICAO DO CAPITAL DE FRANCISCO JOSE DE ARRUDA CAMARGO, NACIONALIDADE BRASILEIRA, RAÇA/COR: NÃO DECLARADA., CPF: 201.723.628-49, RG/RNE: 3678343, RESIDENTE À RUA ALCIDES RIOS DE CASTRO, 79, INDIANOPOLIS, SAO PAULO - SP, CEP 04027-030, REPRESENTANDO CLM INFORMATICA LTDA., NA SITUAÇÃO DE SÓCIO E ADMINISTRADOR, ASSINANDO PELA EMPRESA, COM VALOR DE PARTICIPAÇÃO NA SOCIEDADE DE $ 130.900,00.
REDISTRIBUICAO DO CAPITAL DE CLM INFORMATICA LTDA. , DOCUMENTO: 35211503532, SITUADA À RUA ATICA, 150, AEROPORTO, SAO PAULO - SP, CEP 04634-040, NA SITUAÇÃO DE SÓCIO, COM VALOR DE PARTICIPAÇÃO NA SOCIEDADE DE $ 107.100,00.
ENDEREÇO DA SEDE ALTERADO PARA RUA PRACA DAS PAPOULAS, 30, 1 AN, ALPHAVILLE, BARUERI - SP, CEP 06453-000.
CONSOLIDAÇÃO CONTRATUAL DA MATRIZ.
NUM.DOC: 421.657/15-7 SESSÃO: 30/09/2015
ABERTURA DE FILIAL NIRE PROVISÓRIO 42999139261, CNPJ 02.092.332/0002-50, SITUADA À: RUA MARIO LOBO, 61, S- 1309 - B, CENTRO, JOINVILLE - SC, CEP 89201-330, COM OBJETO DESTACADO DE COMÉRCIO VAREJISTA ESPECIALIZADO DE EQUIPAMENTOS E SUPRIMENTOS DE INFORMÁTICA E SUPORTE TÉCNICO, MANUTENÇÃO E OUTROS SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO. COM INÍCIO DAS ATIVIDADES: 10/09/2015.
CONSOLIDAÇÃO CONTRATUAL DA MATRIZ.
NUM.DOC: 159.268/16-3 SESSÃO: 20/04/2016
ENDEREÇO DA FILIAL NIRE PROVISÓRIO 42999139261, CNPJ 02.092.332/0002-50, SITUADA À RUA MARIO LOBO, 61, S- 1309 - B, CENTRO, JOINVILLE - SC, CEP 89201-330. ALTERADO PARA RUA EVARISTO DA VEIGA, 101, SL L1 1 AND, GLORIA, JOINVILLE - SC, CEP 89216-215.
CONSOLIDAÇÃO CONTRATUAL DA MATRIZ.
NUM.DOC: 341.445/16-2 SESSÃO: 09/08/2016
CAPITAL DA SEDE ALTERADO PARA $ 2.100.000,00 (DOIS MILHÕES, CEM MIL REAIS).
REDISTRIBUICAO DO CAPITAL DE FRANCISCO JOSE DE ARRUDA CAMARGO, NACIONALIDADE BRASILEIRA, RAÇA/COR: NÃO DECLARADA., CPF: 201.723.628-49, RG/RNE: 3678343, RESIDENTE À RUA ALCIDES RIOS DE CASTRO, 79, INDIANOPOLIS, SAO PAULO - SP, CEP 04027-030, REPRESENTANDO CLM INFORMATICA LTDA, NA SITUAÇÃO DE SÓCIO E ADMINISTRADOR, ASSINANDO PELA EMPRESA, COM VALOR DE PARTICIPAÇÃO NA SOCIEDADE DE $ 1.155.000,00.
REDISTRIBUICAO DO CAPITAL DE CLM INFORMATICA LTDA , DOCUMENTO: 35211503532, SITUADA À ALAMEDA DOS NHAMBIQUARAS, 1770, CONJ.211/212, INDIANOPOLIS, SAO PAULO - SP, CEP 04090-004, NA SITUAÇÃO DE SÓCIO, COM VALOR DE PARTICIPAÇÃO NA SOCIEDADE DE $ 945.000,00.
INCLUSÃO/ALTERAÇÃO DE CNPJ: NIRE 42999139261, CNPJ 02.092.332/0002-50
ENDEREÇO DA FILIAL NIRE PROVISÓRIO 42999139261, CNPJ 02.092.332/0002-50, SITUADA À RUA EVARISTO DA VEIGA, 101, SL

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.007562 / pg. 3543

L1 1 AND, GLORIA, JOINVILLE - SC, CEP 89216-215. ALTERADO PARA RUA MARIO LOBO, 61, SALA 1309, CENTRO, JOINVILLE - SC, CEP 89201-330. , DATADA DE: 26/07/2016.

CONSOLIDAÇÃO CONTRATUAL DA MATRIZ.

NUM.DOC: 873.013/16-5 SESSÃO: 13/09/2016

ARQUIVAMENTO DE PROCURAÇÃO PÚBLICA, CONFORME DISPOSTO NA IN NO. 28 DE 06/10/2014 E RESOLUÇÃO CNJ NO. 42 DE 31/10/2014.

NUM.DOC: 514.616/17-9 SESSÃO: 13/12/2017

REDISTRIBUICAO DO CAPITAL DE FRANCISCO JOSE DE ARRUDA CAMARGO, NACIONALIDADE BRASILEIRA, RAÇA/COR: NÃO DECLARADA., CPF: 201.723.628-49, RG/RNE: 3678343, RESIDENTE À RUA ALCIDES RIOS DE CASTRO, 79, INDIANOPOLIS, SAO PAULO - SP, CEP 04027-030, REPRESENTANDO CLM INFORMATICA LTDA, NA SITUAÇÃO DE SÓCIO E ADMINISTRADOR, ASSINANDO PELA EMPRESA, COM VALOR DE PARTICIPAÇÃO NA SOCIEDADE DE $ 1.365.000,00.

REDISTRIBUICAO DO CAPITAL DE CLM INFORMATICA LTDA , DOCUMENTO: 35211503532, SITUADA À ALAMEDA DOS NHAMBIQUARAS, 1770, INDIANOPOLIS, SAO PAULO - SP, CEP 04090-004, NA SITUAÇÃO DE SÓCIO, COM VALOR DE PARTICIPAÇÃO NA SOCIEDADE DE $ 735.000,00.

ENDEREÇO DA SEDE ALTERADO PARA CALCADA DAS HORTENCIAS, 131, PISO 2 ANDAR, ALPHAVILLE COMERCIA, BARUERI - SP, CEP 06453-017. , DATADA DE: 09/11/2017.

CONSOLIDAÇÃO CONTRATUAL DA MATRIZ.

NUM.DOC: 288.012/19-7 SESSÃO: 29/05/2019

ABERTURA DE FILIAL NIRE PROVISÓRIO 32990008378, SITUADA À: RUA SAMUEL MEIRA BRASIL, 394, SALA 29, TAQUARAL II, SERRA - ES, CEP 29167-650, COM OBJETO DESTACADO DE COMÉRCIO ATACADISTA DE OUTRAS MÁQUINAS E EQUIPAMENTOS NÃO ESPECIFICADOS ANTERIORMENTE; PARTES E PEÇAS, CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO, DESENVOLVIMENTO E LICENCIAMENTO DE PROGRAMAS DE COMPUTADOR CUSTOMIZÁVEIS, SUPORTE TÉCNICO, MANUTENÇÃO E OUTROS SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO E TREINAMENTO EM INFORMÁTICA. COM INÍCIO DAS ATIVIDADES: 24/05/2019.

CONSOLIDAÇÃO CONTRATUAL DA MATRIZ.

NUM.DOC: 112.391/20-5 SESSÃO: 10/03/2020

INCLUSÃO/ALTERAÇÃO DE CNPJ: NIRE 42901098722, CNPJ 02.092.332/0002-50

ENDEREÇO DA FILIAL NIRE 42901098722, CNPJ 02.092.332/0002-50, ALTERADO PARA RUA MARIO LOBO, 61, 9O AND SL 910, CENTRO, JOINVILLE - SC, CEP 89201-330. , DATADA DE: 17/12/2019.

REDISTRIBUICAO DO CAPITAL DE FRANCISCO JOSE DE ARRUDA CAMARGO, NACIONALIDADE BRASILEIRA, RAÇA/COR: BRANCA, CPF: 201.723.628-49, RG/RNE: 3678343, RESIDENTE À RUA DONA ALCIDE RIOS DE CASTRO, 79, VILA CLEMENTINO, SAO PAULO - SP, CEP 04027-030, REPRESENTANDO CLM INFORMATICA LTDA E INTERACTION -SERVICOS EM INFORMATICA E TREINAMENTO LTDA., NA SITUAÇÃO DE SÓCIO E ADMINISTRADOR, ASSINANDO PELA EMPRESA, COM VALOR DE PARTICIPAÇÃO NA SOCIEDADE DE $ 838.950,00.

CADASTRO CLM INFORMATICA LTDA , DOCUMENTO: 35211503532, SITUADA À ALAMEDA DOS NHAMBIQUARAS, 1770, INDIANOPOLIS, SAO PAULO - SP, CEP 04090-004, NA SITUAÇÃO DE SÓCIO, COM VALOR DE PARTICIPAÇÃO NA SOCIEDADE DE $ 735.000,00.

ADMITIDO INTERACTION -SERVICOS EM INFORMATICA E TREINAMENTO LTDA. , NIRE 35231702069, SITUADA À ALEMEDA DOS NHAMBIQUARAS, 1500, LOJA 1, INDIANOPOLIS, SAO PAULO - SP, CEP 04090-003, NA SITUAÇÃO DE SÓCIO, COM VALOR DE PARTICIPAÇÃO NA SOCIEDADE DE $ 526.050,00.

CONSOLIDAÇÃO CONTRATUAL DA MATRIZ.

NUM.DOC: 461.976/23-7 SESSÃO: 07/12/2023

ALTERACAO DE SOCIOS/TITULAR/DIRETORIA: , DATADA DE: 24/10/2023.

REDISTRIBUICAO DO CAPITAL DE FRANCISCO JOSE DE ARRUDA CAMARGO, NACIONALIDADE BRASILEIRA, RAÇA/COR: NÃO DECLARADA, CPF: 201.723.628-49, RG/RNE: 3678343, RESIDENTE À RUA DONA ALCIDE RIOS DE CASTRO, 79, VILA CLEMENTINO, SAO PAULO - SP, CEP 04027-030, REPRESENTANDO CLM INFORMATICA LTDA E INTERACTION -SERVICOS EM INFORMATICA E TREINAMENTO LTDA., NA SITUAÇÃO DE SÓCIO E ADMINISTRADOR, ASSINANDO PELA EMPRESA, COM VALOR DE PARTICIPAÇÃO NA SOCIEDADE DE $ 1.573.950,00.

RETIRA-SE DA SOCIDEDADE CLM INFORMATICA LTDA , DOCUMENTO: 35211503532, SITUADA À ALAMEDA DOS NHAMBIQUARAS, 1770, INDIANOPOLIS, SAO PAULO - SP, CEP 04090-004, NA SITUAÇÃO DE SÓCIO, COM VALOR DE PARTICIPAÇÃO NA SOCIEDADE DE $ 735.000,00.

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.007562 / pg. 3544

REDISTRIBUICAO DO CAPITAL DE INTERACTION -SERVICOS EM INFORMATICA E TREINAMENTO LTDA. , NIRE 35231702069, SITUADA À ALEMEDA DOS NHAMBIQUARAS, 1500, INDIANOPOLIS, SAO PAULO - SP, CEP 04090-003, NA SITUAÇÃO DE SÓCIO, COM VALOR DE PARTICIPAÇÃO NA SOCIEDADE DE $ 526.050,00.

ABERTURA DE FILIAL NIRE 32900705597, CNPJ 02.092.332/0004-11, SITUADA À: RUA SAMUEL MEIRA BRASIL, 394, CONJUNTO C3 P, TAQUARA II, SERRA - ES, CEP 29167-650, COM OBJETO DESTACADO DE COMÉRCIO VAREJISTA ESPECIALIZADO DE EQUIPAMENTOS E SUPRIMENTOS DE INFORMÁTICA, COMÉRCIO ATACADISTA DE OUTRAS MÁQUINAS E EQUIPAMENTOS NÃO ESPECIFICADOS ANTERIORMENTE; PARTES E PEÇAS, CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO, DESENVOLVIMENTO E LICENCIAMENTO DE PROGRAMAS DE COMPUTADOR CUSTOMIZÁVEIS E SUPORTE TÉCNICO, MANUTENÇÃO E OUTROS SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO. COM INÍCIO DAS ATIVIDADES: 24/10/2023., DATADA DE: 24/10/2023.

CONSOLIDAÇÃO CONTRATUAL DA MATRIZ.

NUM.DOC: 374.432/24-7 SESSÃO: 09/10/2024

ABERTURA DE FILIAL NIRE 33901648733, CNPJ 02.092.332/0005-00, SITUADA À: RUA MEXICO, 119, SALA 504, CENTRO, RIO DE JANEIRO - RJ, CEP 20031-145, COM OBJETO DESTACADO DE COMÉRCIO VAREJISTA ESPECIALIZADO DE EQUIPAMENTOS E SUPRIMENTOS DE INFORMÁTICA, COMÉRCIO ATACADISTA DE OUTRAS MÁQUINAS E EQUIPAMENTOS NÃO ESPECIFICADOS ANTERIORMENTE; PARTES E PEÇAS, CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO, DESENVOLVIMENTO E LICENCIAMENTO DE PROGRAMAS DE COMPUTADOR CUSTOMIZÁVEIS E SUPORTE TÉCNICO, MANUTENÇÃO E OUTROS SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO. COM INÍCIO DAS ATIVIDADES: 24/09/2024., DATADA DE: 24/09/2024.

ALTERACAO DE SOCIOS/TITULAR/DIRETORIA: , DATADA DE: 24/09/2024.

ALTERAÇÃO DOS DADOS CADASTRAIS DE FRANCISCO JOSE DE ARRUDA CAMARGO, NACIONALIDADE BRASILEIRA, RAÇA/COR: NÃO DECLARADA, CPF: 201.723.628-49, RG/RNE: 3678343, RESIDENTE À RUA DONA ALCIDE RIOS DE CASTRO, 79, VILA CLEMENTINO, SAO PAULO - SP, CEP 04027-030, NA SITUAÇÃO DE SÓCIO E ADMINISTRADOR, ASSINANDO PELA EMPRESA, COM VALOR DE PARTICIPAÇÃO NA SOCIEDADE DE $ 1.573.950,00.

ALTERAÇÃO DOS DADOS CADASTRAIS DE CLM VAD EXPERTS LTDA , NIRE 35231702069, SITUADA À AV IBIRAPUERA, 2332, CJ 22 TORRE I, INDIANOPOLIS, SAO PAULO - SP, CEP 04028-900, NA SITUAÇÃO DE SÓCIO, COM VALOR DE PARTICIPAÇÃO NA SOCIEDADE DE $ 526.050,00.((COM DENOMINACAO ANTERIOR INTERACTION -SERVICOS EM INFORMATICA E TREINAMENTO LTDA.))

CITADO THOMAS AYRES DE ARRUDA CAMARGO, NACIONALIDADE BRASILEIRA, RAÇA/COR: NÃO DECLARADA, CPF: 290.370.518-63, RG/RNE: 29.832.472-6, RESIDENTE À RUA DONA ALCIDES RIOS DE CASTRO, 11, VL CLEMENTINO, SAO PAULO - SP, REPRESENTANDO CLM VAD EXPERTS LTDA.

CONSOLIDAÇÃO CONTRATUAL DA MATRIZ.

FIM DAS INFORMAÇÕES PARA NIRE: 35214228052
DATA DA ÚLTIMA ATUALIZAÇÃO DA BASE DE DADOS: 29/01/2026

JUCESP SÃO PAULO GOVERNO DO ESTADO documento assinado digitalmente

Ficha Cadastral Completa. Documento certificado por JUNTA COMERCIAL DO ESTADO DE SÃO PAULO. A Junta Comercial do Estado de São Paulo, garante a autenticidade deste documento quando visualizado diretamente no portal www.jucesponline.sp.gov.br sob o número de autenticidade 284843973, sexta-feira, 30 de janeiro de 2026 às 12:15:31.

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.007562 / pg. 3545

12ª ALTERAÇÃO CONTRATUAL DA SOCIEDADE EMPRESÁRIA LIMITADA

CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA.
CNPJ/MF 02.092.332/0001-79
NIRE 35.214.228.052

1) **FRANCISCO JOSÉ DE ARRUDA CAMARGO**, brasileiro, casado sob o regime de comunhão universal de bens, engenheiro, portador do documento de identidade RG nº 3.678.343 SSP/SP e do CPF/MF nº 201.723.628-49, residente e domiciliado em São Paulo – SP, na Rua Dona Alcide Rios de Castro, 79 – Vila Clementino – CEP 04027-030;

2) **CLM VAD EXPERTS LTDA.**, sociedade empresária limitada com sede na Avenida Ibirapuera, nº 2332, Conjunto 22, Torre I, sala Grace Hopper, Bairro Indianópolis, São Paulo/SP – CEP 04028-900, inscrita no CNPJ/MF sob o nº 57.653.818/0001-20, com contrato social arquivado na Junta Comercial do Estado de São Paulo sob o nº 35231702069, neste ato representada por **THOMAS AYRES DE ARRUDA CAMARGO**, brasileiro, natural de Paris, França, nascido em 23/08/1979, casado sob o regime de comunhão parcial de bens, engenheiro, portador do documento de identidade de RG nº 29.832.472-6 SSP/SP e do CPF nº 290.370.518-63, residente e domiciliado em São Paulo – SP, na Rua Dona Alcide Rios de Castro 11, Vila Clementino – CEP;

Únicos sócios componentes da sociedade empresária denominada **"CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA"**, com sede no município de Barueri/SP, na Calçada das Hortênsias, 131, Piso 2º Andar, Condomínio Centro Comercial Alphaville, CEP 06453-017, inscrita no CNPJ/MF sob o n° 02.092.332/0001-79, com contrato social arquivado na Junta Comercial do Estado de São Paulo sob o NIRE n° 35.214.228.052 em sessão de 07/02/1997 e posteriores alterações contratuais, resolvem de pleno acordo, e na melhor forma de direito, alterar o contrato social mediante as cláusulas e condições seguintes:

ABERTURA DE FILIAL

1. Os sócios resolvem abrir uma filial na Rua México, nº 119, sala 504, Centro, Rio de Janeiro/RJ, CEP 20031-145 tendo como objeto social a exploração dos ramos de: Comércio Varejista e atacadista de material de informática, software e programas aplicativos, importação e exportação; Prestação de serviços para terceiros em manutenção de equipamentos, locação e intermediação de negócios com equipamento de informática; Assessoria, treinamento e consultoria em informática e licenciamento ou cessão de uso de programas de informática.

FRANCISCO JOSE DE ARRUDA CAMARGO:20172362849 Assinado de forma digital por FRANCISCO JOSE DE ARRUDA CAMARGO:20172362849 Dados: 2024.10.02 11:24:44 -03'00'
THOMAS AYRES DE ARRUDA CAMARGO:29037051863 Assinado de forma digital por THOMAS AYRES DE ARRUDA CAMARGO:29037051863 Dados: 2024.10.02 11:20:21 -03'00'
Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) 24100207 10245

2. Em virtude da alteração acima realizada, resolvem os sócios consolidar o Contrato Social, o qual passará a vigorar com a seguinte redação:

CONSOLIDAÇÃO CONTRATUAL

CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA.
CNPJ/MF 02.092.332/0001-79
NIRE 35214228052

CAPÍTULO I
DA DENOMINAÇÃO, SEDE, DURAÇÃO E OBJETO.

CLÁUSULA PRIMEIRA - A sociedade tem a denominação de **CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA.**, com sede e foro no município de Barueri/SP, na Calçada das Hortênsias, 131, Piso 2º Andar, Condomínio Centro Comercial Alphaville, CEP 06453-017.

Parágrafo Único: A sociedade possui as seguintes filiais:

Filial 1 - no **município de Joinville/SC**, na Rua Mario Lobo, n° 61 – 9º Andar – Sala 910, Centro, CEP 89201-330, inscrita no CNPJ/MF sob o nº 02.092.332/0002-50, com registro na Junta Comercial do Estado de Santa Catarina sob o nº 42901098722 em 08/10/2015, tendo como objeto social a exploração dos ramos de: Comércio varejista e atacadista de material de informática, software e programas aplicativos, importação e exportação; Prestação de serviços para terceiros em manutenção de equipamentos, locação e intermediação de negócios com equipamento de informática; Assessoria, treinamento e consultoria em informática e licenciamento ou cessão de uso de programas de informática, tendo iniciado suas atividades em 08/10/2015.

Filial 2 - no **município de Serra/ES**, na Rua Samuel Meira Brasil, n° 394, Sala 29 – Serra Parque Logístico, Conjunto CB5, Taquara II, CEP 29167-650, inscrita no CNPJ/MF sob o nº 02.092.332/0003-30, com registro na Junta Comercial do Estado do Espírito Santo sob o nº 32900615351 em 01/07/2019, tendo como objeto social a exploração dos ramos de: (a) Comércio atacadista de material de informática, software e programas aplicativos, importação e exportação (CNAE 46.69-9/99); (b) comércio varejista de material de informática, software e programas aplicativos, importação e exportação (CNAE 4751-2/01); (c) Prestação de serviços para terceiros em manutenção de equipamentos (CNAE 6209-1/00); (d) assessoria e consultoria em informática; (CNAE 6204-0/00) e (f) licenciamento ou cessão de uso de programas de informática (CNAE 6202-3/00) .

FRANCISCO JOSE DE ARRUDA CAMARGO:20172362849 Assinado de forma digital por FRANCISCO JOSE DE ARRUDA CAMARGO:20172362849
THOMAS AYRES DE ARRUDA CAMARGO:29037051063 Assinado de forma digital por THOMAS AYRES DE ARRUDA CAMARGO:29037051063
Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) 25/03/2025 - 15:47

Filial 3 – no **município de Serra/ES,** Rua Samuel Meira Brasil, nº. 394, sala 37, Conjunto C3 parte, B1 a B6 parte, B7 parte a B11 Ecopark, Taquara II, CEP 29167.650, tendo como objeto social a exploração dos ramos de: Comércio varejista e atacadista de material de informática, software e programas aplicativos, importação e exportação; Prestação de serviços para terceiros em manutenção de equipamentos, locação e intermediação de negócios com equipamento de informática; Assessoria, treinamento e consultoria em informática e licenciamento ou cessão de uso de programas de informática.

Filial 4 – no **município do Rio de Janeiro/RJ,** Rua México, nº 119, sala 504, CEP 20031-145, tendo como objeto social a exploração dos ramos de: Comércio Varejista e atacadista de material de informática, software e programas aplicativos, importação e exportação; Prestação de serviços para terceiros em manutenção de equipamentos, locação e intermediação de negócios com equipamento de informática; Assessoria, treinamento e consultoria em informática e licenciamento ou cessão de uso de programas de informática.

CLÁUSULA SEGUNDA – A sociedade tem por objeto social: **Comércio varejista e atacadista de material de informática, software e programas aplicativos, importação e exportação; Prestação de serviços para terceiros em manutenção de equipamentos, locação e intermediação de negócios com equipamento de informática; Assessoria, treinamento e consultoria em informática e licenciamento ou cessão de uso de programas de informática.**

CLÁUSULA TERCEIRA – A sociedade iniciou suas atividades em 10 de janeiro de 1997 e o seu prazo de duração é indeterminado.

CAPÍTULO II
DO CAPITAL SOCIAL

CLÁUSULA QUARTA– O Capital Social é R$ 2.100.000,00 (dois milhões e cem mil reais), dividido em 2.100.000 (dois milhões e cem mil) quotas, no valor nominal de R$ 1,00 (um real) cada uma, assim distribuídas entre os sócios:

SÓCIOS	%	QUOTAS	VALOR TOTAL
FRANCISCO JOSÉ DE ARRUDA CAMARGO	75%	1.573.950	**R$ 1.573.950,00**
CLM VAD EXPERTS LTDA	25%	526.050	R$ 526.050,00
TOTAL	**100%**	**2.100.000**	**R$ 2.100.000,00**

FRANCISCO JOSE DE ARRUDA CAMARGO:20172362849 Assinado de forma digital por FRANCISCO JOSE DE ARRUDA CAMARGO:20172362849 Dados: 2024.10.02 11:25:44 -03'00'

THOMAS AYRES DE ARRUDA CAMARGO:29037651163 Assinado de forma digital por THOMAS AYRES DE ARRUDA CAMARGO:29037651163 Dados: 2024.10.02 11:26:37 -03'00'

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) 07 48

Parágrafo 1º: Nenhuma quota poderá ser vendida, cedida, transferida ou, por qualquer forma alienada sem aprovação do outro sócio, além de lhe ficar assegurado, mediante aviso por escrito através de Cartório de Títulos e Documentos, com antecedência de 30 (trinta) dias, o direito de preferência na sua aquisição em igualdade de condições com terceiro interessado em adquiri-la, sendo nula e ineficaz em relação à sociedade a venda, cessão, doação, transferência ou alienação, concluída com inobservância no disposto neste parágrafo.

Parágrafo 2º: A falta de resposta em relação ao exercício do direito de preferência implicará na decadência do direito de preferência.

Parágrafo 3°: A responsabilidade dos sócios é restrita ao valor de suas quotas, mas todos os sócios são solidariamente responsáveis pela integralização do capital social.

Parágrafo 4°: As quotas são indivisíveis em relação à sociedade e cada quota dá direito a um voto em todas as decisões sociais.

CAPÍTULO III
DA ADMINISTRAÇÃO

CLÁUSULA QUINTA – A sociedade é administrada pelo sócio **FRANCISCO JOSÉ DE ARRUDA CAMARGO** que fica dispensado de prestar caução, e que usará a designação de sócio administrador, podendo praticar todos os atos necessários ao regular funcionamento da sociedade, firmar contratos de qualquer natureza em especial arrendamento, locação, empréstimos, abertura de contas correntes e crédito, nomear procuradores com cláusula *"ad judicia"* , representar a sociedade perante terceiros, enfim, terá o mais amplo e geral poder de administração, desde que enquadrados no objeto social.

Parágrafo 1º: A sociedade através do sócio administrador poderá nomear procuradores para praticar atos em nome da sociedade, sendo certo que os instrumentos de procuração deverão conter poderes específicos e prazos de validade limitados, excetuando-se, quanto a esta última exigência, as procurações com cláusulas *"ad judiciais"*.

Parágrafo 2º: São expressamente vedados, sendo nulos e inoperantes em relação à sociedade, os atos de quotistas, procuradores ou funcionários que a envolverem em obrigações relativas à negócios ou operações estranhas aos objetivos sociais, tais como, alienações ou alterações do ativo imobilizado da sociedade, renuncia a direitos, empréstimos bancários, fianças ou avais, endossos ou quaisquer outras garantias em favor de terceiros, exceto à empresas do mesmo grupo econômico desde que devidamente representada pelo sócio administrador.

Parágrafo 3°: Quando em exercício o Sócio Administrador receberá *"pró-labore"* que for fixado pelos sócios em reunião geral.

FRANCISCO JOSE DE ARRUDA CAMARGO:20172362849 Assinado de forma digital por FRANCISCO JOSE DE ARRUDA CAMARGO:20172362849 Dados: 2024.10.02 11:26:02 -03'00'
THOMAS AYRES DE ARRUDA CAMARGO:29037053863 Assinado de forma digital por THOMAS AYRES DE ARRUDA CAMARGO:29037053863 Dados: 2024.10.02 15:29:14 -03'00'
Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SOLICITAÇÃO 55 - 49

CAPITULO IV
EXERCÍCIO SOCIAL, BALANÇO E DISTRIBUIÇÃO DE LUCROS

CLÁUSULA SEXTA – O exercício social coincidirá com o ano civil, encerrando-se em 31 de dezembro.

CLÁUSULA SÉTIMA – Ao fim de cada exercício social serão elaboradas as demonstrações financeiras, feitas as necessárias amortizações e deduções para as reservas legais e as julgadas convenientes.

Parágrafo 1º: As quotas da administração e a destinação dos lucros líquidos anualmente obtidos serão aprovados por sócio ou sócios titulares de mais da metade do capital social, garantida a todos os sócios a sua participação obedecida a proporção das quotas detidas por cada sócio.

Parágrafo 2º: Os sócios participarão dos lucros e suportarão os prejuízos na proporção das respectivas participações no capital social, podendo a sociedade levantar balanços intermediários, intercalares ou em intervalos menores, para efeito de verificação e distribuição de lucros.

Parágrafo 3º: Desde que acordado entre os sócios, os lucros apurados poderão ser distribuídos de forma desproporcional à participação societária, nunca podendo, todavia, nenhum sócio deixar de receber parte dos lucros apurados (artigos 1.007 e 1.008 do Código Civil).

CAPÍTULO V
DAS DECIÇÕES SOCIAIS, DISSOLUÇÃO E EXCLUSÃO DE SÓCIOS

CLÁUSULA OITAVA – Todas as decisões da sociedade serão tomadas por quotistas que representem a maioria do capital social, em reunião dos sócios, convocada pelo administrador da sociedade, em especial os referentes a aprovação das contas, modificação dos estatutos, incorporação, fusão, transformação ou dissolução da sociedade, oneração de bens imóveis, que serão tomadas em assembleia especialmente convocada pela administração da sociedade.
Parágrafo 1º: As reuniões de quotistas serão sempre convocadas pelo sócio administrador, através de carta ou comunicado aos demais quotistas com antecedência mínima de 10 (Dez) dias da data de realização da assembleia.

Parágrafo 2º: A reunião dos sócios poderá ser dispensada nos casos expressamente previstos neste contrato social, assim como no caso de todos os sócios decidirem, por escrito, sobre a matéria a ela sujeita.

Parágrafo 3º: Ficam dispensadas as formalidades da convocação sempre que todos os sócios comparecerem ou se declararem, por escrito, cientes do local, data, hora e ordem do dia da reunião.

FRANCISCO JOSE DE ARRUDA CAMARGO:20172362849
THOMAS AYRES DE ARRUDA CAMARGO:29037051953
Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) 06/0003550

Parágrafo 4º: A reunião de sócios instala-se com a presença, em primeira convocação, de titulares de, no mínimo, mais da metade do capital social, e, em segunda convocação, com qualquer número.

Parágrafo 5º: As reuniões serão presididas por sócio, representante de sócio, administrador ou terceiro designado pela maioria dos presentes, cabendo ao presidente da reunião a escolha do secretário, sendo que dos trabalhos e deliberações será lavrada, no livro de atas de reunião, ata assinada pelos membros da mesa e pelos sócios presentes, quantos bastem para a validade das deliberações, mas sem prejuízo dos que queiram assiná-la.

Parágrafo 6º: Cópia da ata autenticada pela administração ou pela mesa será apresentada ao Registro de Empresas Mercantis para arquivamento e averbação.

Parágrafo 7º: Competirá a cada quota um voto nas deliberações sociais.

Parágrafo 8º: Serão realizadas, ordinariamente, reuniões de quotistas até o último dia útil do quarto mês seguinte ao encerramento do exercício social, para deliberar sobre o resultado do exercício encerrado, destinação do resultado e outros assuntos de interesse da sociedade e que consta da ordem do dia.

CLÁUSULA NONA – O contrato social poderá ser modificado, no todo ou em parte, por deliberação da assembleia especialmente convocada para este fim, respeitando-se o disposto na clausula 8ª e seus parágrafos.

CLÁUSULA DÉCIMA – A sociedade poderá entrar em liquidação por decisão dos sócios que representem a maioria do capital social, cabendo ao sócio **Francisco José de Arruda Camargo** indicar o liquidante. Nessa hipótese os haveres da sociedade serão empregados na liquidação de suas obrigações e o remanescente, se houver, será rateado entre os sócios em proporção ao número de quotas que cada um possuir. Encerrada a liquidação a sociedade será declarada extinta por deliberação do sócio ou sócios de mais da metade do capital social.

CLÁUSULA DÉCIMA PRIMEIRA – A morte, interdição, insolvência ou retirada de qualquer deles não importará na dissolução da sociedade. Na hipótese de falecimento de qualquer um dos sócios quotistas, os herdeiros do sócio falecido de comum acordo, exercerão o direito à quota. Entretanto, não havendo interesse destes em participar da sociedade, realizar-se-á balanço especial, na data do evento, quando serão apurados os haveres, sendo feito o pagamento das quotas de capital em 36 (trinta e seis) parcelas mensais, iguais e consecutivas, acrescidas de juros e correções legais, pagáveis a primeira 90 (noventa) dias da abertura da sucessão ou da retirada do sócio.

FRANCISCO JOSE DE ARRUDA CAMARGO:20172362849 Assinado de forma digital por FRANCISCO JOSE DE ARRUDA CAMARGO:20172362849 Dados: 2024-10-02 11:26:49 -03'00'

THOMAS AYRES DE ARRUDA CAMARGO:29037051863 Assinado de forma digital por THOMAS AYRES DE ARRUDA CAMARGO:29037051863 Dados: 2024-10-02 11:26:18 -03'00'

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) 02/10/2024 - 0001

Parágrafo 1º: No caso de falecimento de um sócio quotista havendo interesse de mais de um herdeiro em permanecer com as quotas, as mesmas serão transferidas em caráter *"pró-indiviso"* aos sucessores, os quais nomearão um só entre eles para representa-los junto a sociedade.

Parágrafo 2º: Os poderes de gerencia, satisfeita a condição do parágrafo anterior, somente serão conferidos ao sócio substituído por alteração contratual.

Parágrafo 3º: No caso de dissolução de sociedade conjugal de quaisquer dos sócios, não poderá o sócio que vier a se separar partilhar suas quotas sociais sem prévia e expressa autorização do outro sócio, autorização esta que em momento algum poderá ser presumida.

CLÁUSULA DÉCIMA SEGUNDA – De acordo com o artigo 1.085 do Código Civil, quando a maioria dos sócios, representativa de mais da metade do capital social, entender que um ou mais sócios estão pondo em risco a continuidade da empresa, em virtude de atos de inegável gravidade, poderão excluí-los da sociedade por justa causa e extrajudicialmente.

CAPITULO VI
FUSÃO, INCORPORAÇÃO, CISÃO E TRANSFORMAÇÃO

CLÁUSULA DÉCIMA TERCEIRA – A sociedade poderá ser fundida ou incorporada a qualquer tempo, por deliberação de sócios ou sócios titulares de, no mínimo ¾ (três quartos) do capital social.

CLÁUSULA DÉCIMA QUARTA – A sociedade poderá ser cindida ou transformada, a qualquer tempo, por deliberação de sócios ou sócios titulares de mais da metade do capital social.

CAPITULO VII
DAS DISPOSIÇÕES

CLÁUSULA DÉCIMA QUINTA – A sociedade não terá Conselho Fiscal.

CLÁUSULA DÉCIMA SEXTA – Os sócios declaram que não estão incursos em nenhum dos crimes previstos em Lei, que os impeçam de exercer as atividades sociais, constantes do artigo 1011 do Código Civil Brasileiro.

CLÁUSULA DÉCIMA SÉTIMA – A sociedade será regida pelo disposto neste contrato social, bem como pelo estabelecido nos artigos 1.052 a 1.087 da Lei 10.406 de 10 de janeiro de 2002 (Código Civil), aplicando-se, nos termos do parágrafo único do artigo 1.053 do Código Civil, supletivamente, às disposições do presente contrato, no que couber, as normas da sociedade anônima.

FRANCISCO JOSE DE ARRUDA CAMARGO:20172362849 Assinado de forma digital por FRANCISCO JOSE DE ARRUDA CAMARGO:20172362849 Dados: 2024.10.02 11:27:10 -03'00'

THOMAS AYRES DE ARRUDA CAMARGO:29037051303 Assinado de forma digital por THOMAS AYRES DE ARRUDA CAMARGO:29037051303 Dados: 2024.10.02 11:27:41 -03'00'

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) 0 [illegible]552

CLÁUSULA DÉCIMA OITAVA – As partes indicam o foro da Comarca de Barueri, Estado de São Paulo, para dirimir as dúvidas oriundas do presente instrumento.

E por acharem em perfeito acordo, em tudo quanto neste instrumento particular foi lavrado, obrigam-se a cumprir o presente contrato, assinando-o abaixo, em 03 (três) vias de um só teor e efeito.

Barueri/SP, 24 de setembro de 2024.

FRANCISCO JOSE DE ARRUDA CAMARGO:20172362849
Assinado de forma digital por FRANCISCO JOSE DE ARRUDA CAMARGO:20172362849
Dados: 2024.10.02 11:16:40 -03'00'

FRANCISCO JOSÉ DE ARRUDA CAMARGO

THOMAS AYRES DE ARRUDA CAMARGO:29037051863
Assinado de forma digital por THOMAS AYRES DE ARRUDA CAMARGO:29037051863
Dados: 2024.10.02 11:15:54 -03'00'

CLM VAD EXPERTS LTDA
Representada por **THOMAS AYRES DE ARRUDA CAMARGO**

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.007562 / pg. 3553

Declaração

Eu, FRANCISCO JOSE DE ARRUDA CAMARGO, portador da Cédula de Identidade nº 3678343, inscrito no Cadastro de Pessoas Físicas - CPF sob nº 201.723.628-49, na qualidade de titular, sócio ou responsável legal da empresa CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., **DECLARO** estar ciente que o **ESTABELECIMENTO** situado no(a) Rua Mexico, 119, SALA 504, Centro, RJ, Rio de Janeiro, CEP 20031-145, para exercer suas atividades regularmente, **DEVERÁ OBTER** parecer municipal sobre a viabilidade de instalação e funcionamento no local indicado, conforme diretrizes estabelecidas na legislação de uso e ocupação do solo, posturas municipais e restrições das áreas de proteção ambiental, nos termos do art. 24, §2º, do Decreto Estadual nº 56.660/2010, bem como **CERTIFICADO DE LICENCIAMENTO INTEGRADO VÁLIDO**, obtido pelo sistema Via Rápida Empresa – Módulo de Licenciamento Estadual.

Declaro ainda estar ciente que qualquer alteração no endereço do estabelecimento, em sua atividade ou grupo de atividades, ou qualquer outra das condições determinantes à expedição do Certificado de Licenciamento Integrado, implica na perda de sua validade, assumindo, desde o momento da alteração, a obrigação de renová-lo.

Por fim, declaro estar ciente que a emissão do Certificado de Licenciamento Integrado poderá ser solicitada por representante legal devidamente habilitado, presencialmente e no ato da retirada das certidões relativas ao registro empresarial na Prefeitura, ou pelo titular, sócio, ou contabilista vinculado no Cadastro Nacional da Pessoa Jurídica (CNPJ) diretamente no site da Jucesp, através do módulo de licenciamento, mediante uso da respectiva certificação digital.

FRANCISCO JOSE DE ARRUDA CAMARGO

FRANCISCO JOSE DE ARRUDA CAMARGO

RG: 3678343

CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA.

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.007562 / pg. 3554

Declaração

Eu, FRANCISCO JOSE DE ARRUDA CAMARGO, portador da Cédula de Identidade nº 3678343, inscrito no Cadastro de Pessoas Físicas - CPF sob nº 201.723.628-49, na qualidade de titular, sócio ou responsável legal da empresa CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., **DECLARO** estar ciente que o **ESTABELECIMENTO** situado no(a) Calcada das Hortencias, 131, ANDAR PISO 2, Condominio Centro Comercial Alphaville, SP, Barueri, CEP 06453-017, para exercer suas atividades regularmente, **DEVERÁ OBTER** parecer municipal sobre a viabilidade de instalação e funcionamento no local indicado, conforme diretrizes estabelecidas na legislação de uso e ocupação do solo, posturas municipais e restrições das áreas de proteção ambiental, nos termos do art. 24, §2º, do Decreto Estadual nº 56.660/2010, bem como **CERTIFICADO DE LICENCIAMENTO INTEGRADO VÁLIDO**, obtido pelo sistema Via Rápida Empresa – Módulo de Licenciamento Estadual.

Declaro ainda estar ciente que qualquer alteração no endereço do estabelecimento, em sua atividade ou grupo de atividades, ou qualquer outra das condições determinantes à expedição do Certificado de Licenciamento Integrado, implica na perda de sua validade, assumindo, desde o momento da alteração, a obrigação de renová-lo.

Por fim, declaro estar ciente que a emissão do Certificado de Licenciamento Integrado poderá ser solicitada por representante legal devidamente habilitado, presencialmente e no ato da retirada das certidões relativas ao registro empresarial na Prefeitura, ou pelo titular, sócio, ou contabilista vinculado no Cadastro Nacional da Pessoa Jurídica (CNPJ) diretamente no site da Jucesp, através do módulo de licenciamento, mediante uso da respectiva certificação digital.

FRANCISCO JOSE DE ARRUDA CAMARGO

FRANCISCO JOSE DE ARRUDA CAMARGO

RG: 3678343

CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA.

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.007562 / pg. 3555

MINISTÉRIO DA FAZENDA
Secretaria da Receita Federal do Brasil
Procuradoria-Geral da Fazenda Nacional

CERTIDÃO POSITIVA COM EFEITOS DE NEGATIVA DE DÉBITOS RELATIVOS AOS TRIBUTOS FEDERAIS E À DÍVIDA ATIVA DA UNIÃO

Nome: CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA.
CNPJ: 02.092.332/0001-79

Ressalvado o direito de a Fazenda Nacional cobrar e inscrever quaisquer dívidas de responsabilidade do sujeito passivo acima identificado que vierem a ser apuradas, é certificado que:

1. constam débitos administrados pela Secretaria da Receita Federal do Brasil (RFB) com exigibilidade suspensa nos termos do art. 151 da Lei nº 5.172, de 25 de outubro de 1966 - Código Tributário Nacional (CTN), ou objeto de decisão judicial que determina sua desconsideração para fins de certificação da regularidade fiscal, ou ainda não vencidos; e

2. não constam inscrições em Dívida Ativa da União (DAU) na Procuradoria-Geral da Fazenda Nacional (PGFN).

Conforme disposto nos arts. 205 e 206 do CTN, este documento tem os mesmos efeitos da certidão negativa.

Esta certidão é válida para o estabelecimento matriz e suas filiais e, no caso de ente federativo, para todos os órgãos e fundos públicos da administração direta a ele vinculados. Refere-se à situação do sujeito passivo no âmbito da RFB e da PGFN e abrange inclusive as contribuições sociais previstas nas alíneas 'a' a 'd' do parágrafo único do art. 11 da Lei nº 8.212, de 24 de julho de 1991.

A aceitação desta certidão está condicionada à verificação de sua autenticidade na Internet, nos endereços <http://rfb.gov.br> ou <http://www.pgfn.gov.br>.

Certidão emitida gratuitamente com base na Portaria Conjunta RFB/PGFN nº 1.751, de 2/10/2014.
Emitida às 15:10:01 do dia 07/01/2026 <hora e data de Brasília>.
Válida até 06/07/2026.
Código de controle da certidão: **5653.5F68.6877.320C**
Qualquer rasura ou emenda invalidará este documento.

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO

CERTIDÃO NEGATIVA DE DÉBITOS TRABALHISTAS

Nome: CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. (MATRIZ E FILIAIS)
CNPJ: 02.092.332/0003-30
Certidão nº: 1363944/2026
Expedição: 07/01/2026, às 15:12:43
Validade: 06/07/2026 - 180 (cento e oitenta) dias, contados da data de sua expedição.

Certifica-se que **CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. (MATRIZ E FILIAIS)**, inscrito(a) no CNPJ sob o nº **02.092.332/0003-30**, **NÃO CONSTA** como inadimplente no Banco Nacional de Devedores Trabalhistas.
Certidão emitida com base nos arts. 642-A e 883-A da Consolidação das Leis do Trabalho, acrescentados pelas Leis ns.° 12.440/2011 e 13.467/2017, e no Ato 01/2022 da CGJT, de 21 de janeiro de 2022.
Os dados constantes desta Certidão são de responsabilidade dos Tribunais do Trabalho.
No caso de pessoa jurídica, a Certidão atesta a empresa em relação a todos os seus estabelecimentos, agências ou filiais.
A aceitação desta certidão condiciona-se à verificação de sua autenticidade no portal do Tribunal Superior do Trabalho na Internet (http://www.tst.jus.br).
Certidão emitida gratuitamente.

INFORMAÇÃO IMPORTANTE
Do Banco Nacional de Devedores Trabalhistas constam os dados necessários à identificação das pessoas naturais e jurídicas inadimplentes perante a Justiça do Trabalho quanto às obrigações estabelecidas em sentença condenatória transitada em julgado ou em acordos judiciais trabalhistas, inclusive no concernente aos recolhimentos previdenciários, a honorários, a custas, a emolumentos ou a recolhimentos determinados em lei; ou decorrentes de execução de acordos firmados perante o Ministério Público do Trabalho, Comissão de Conciliação Prévia ou demais títulos que, por disposição legal, contiver força executiva.

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.007562 / pg. 3557

Histórico do Empregador

O Histórico do Empregador apresenta os registros dos CRF concedidos nos últimos 24 meses, conforme Manual de Orientações Regularidade do Empregador.

Inscrição: 02.092.332/0003-30
Razão social: CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA.

Data de Emissão/ Leitura	Data de Validade	Número do CRF
27/01/2026	27/01/2026 a 25/02/2026	2026012704220694301555
08/01/2026	08/01/2026 a 06/02/2026	2026010803110694301503
20/12/2025	20/12/2025 a 18/01/2026	2025122001450694301500
01/12/2025	01/12/2025 a 30/12/2025	2025120102510694301586
12/11/2025	12/11/2025 a 11/12/2025	2025111219170694301530
24/10/2025	24/10/2025 a 22/11/2025	2025102404430694301553
05/10/2025	05/10/2025 a 03/11/2025	2025100512120694301559
16/09/2025	16/09/2025 a 15/10/2025	2025091604510694301540
28/08/2025	28/08/2025 a 26/09/2025	2025082819170694301513
09/08/2025	09/08/2025 a 07/09/2025	2025080901450694301585
21/07/2025	21/07/2025 a 19/08/2025	2025072119340694301576
02/07/2025	02/07/2025 a 31/07/2025	2025070222400694301500
13/06/2025	13/06/2025 a 12/07/2025	2025061319220694301560
25/05/2025	25/05/2025 a 23/06/2025	2025052501510694301537
06/05/2025	06/05/2025 a 04/06/2025	2025050602050694301538
17/04/2025	17/04/2025 a 16/05/2025	2025041708200694301507
29/03/2025	29/03/2025 a 27/04/2025	2025032901280694301513
10/03/2025	10/03/2025 a 08/04/2025	2025031021260694301512
19/02/2025	19/02/2025 a 20/03/2025	2025021907380694301500
31/01/2025	31/01/2025 a 01/03/2025	2025013108140694301583
12/01/2025	12/01/2025 a 10/02/2025	2025011201470694301576
24/12/2024	24/12/2024 a 22/01/2025	2024122402170694301508
05/12/2024	05/12/2024 a 03/01/2025	2024120502120694301577
16/11/2024	16/11/2024 a 15/12/2024	2024111601370694301516
28/10/2024	28/10/2024 a 26/11/2024	2024102808430694301501
09/10/2024	09/10/2024 a 07/11/2024	2024100905020694301519
20/09/2024	20/09/2024 a 19/10/2024	2024092019210694301589
01/09/2024	01/09/2024 a 30/09/2024	2024090101320694301540
13/08/2024	13/08/2024 a 11/09/2024	2024081306100694301556
25/07/2024	25/07/2024 a 23/08/2024	2024072508010694301599

Data de Emissão/ Leitura	Data de Validade	Número do CRF
06/07/2024	06/07/2024 a 04/08/2024	202407060146069430151 5
17/06/2024	17/06/2024 a 16/07/2024	20240617070706943015 49
29/05/2024	29/05/2024 a 27/06/2024	20240529053006943015 60
10/05/2024	10/05/2024 a 08/06/2024	20240510185906943015 48
21/04/2024	21/04/2024 a 20/05/2024	2024042101105300369298
02/04/2024	02/04/2024 a 01/05/2024	2024040207301293580902
14/03/2024	14/03/2024 a 12/04/2024	2024031404220112956214
23/02/2024	23/02/2024 a 23/03/2024	2024022307003966586437
04/02/2024	04/02/2024 a 04/03/2024	2024020401245942601464
31/03/2001	31/03/2001 a 30/04/2001	
28/02/2001	28/02/2001 a 31/03/2001	
31/01/2001	31/01/2001 a 28/02/2001	

Resultado da consulta em 30/01/2026 12:32:22

Voltar

Voltar Imprimir

CAIXA ECONÔMICA FEDERAL

Certificado de Regularidade do FGTS - CRF

Inscrição: 02.092.332/0003-30

Razão Social: CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA.

Endereço: R SAMUEL MEIRA BRASIL 394 SALA 29.SERRA PARQ / TAQUARA II / SERRA / ES / 29167-650

A Caixa Econômica Federal, no uso da atribuição que lhe confere o Art. 7, da Lei 8.036, de 11 de maio de 1990, certifica que, nesta data, a empresa acima identificada encontra-se em situação regular perante o Fundo de Garantia do Tempo de Servico - FGTS.

O presente Certificado não servirá de prova contra cobrança de quaisquer débitos referentes a contribuições e/ou encargos devidos, decorrentes das obrigações com o FGTS.

Validade:08/01/2026 a 06/02/2026

Certificação Número: 2026010803110694301503

Informação obtida em 15/01/2026 15:32:10

A utilização deste Certificado para os fins previstos em Lei esta condicionada a verificação de autenticidade no site da Caixa: **www.caixa.gov.br**

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.007562 / pg. 3560

PREFEITURA MUNICIPAL DA SERRA
Secretaria Municipal da Fazenda

CEP: 29176-439 - RUA MAESTRO ANTONIO CICERO, N° 111 CACAROCA Serra ES

Certidão Negativa de Débitos

N° da Certidão: 12114828/2025 **Data Geração:10/12/2025** **Data Validade:10/02/2026**

CERTIFICAMOS, que não constam em nome do sujeito passivo identificado, nesta data, débitos com a Fazenda Pública Municipal, ressalvando o direito do município de cobrar quaisquer débitos que vierem a ser conhecidos e apurados após a expedição.

Essa certidão com base no art. 178 da Lei 3833, de 29 de dezembro de 2011, Código Tributário Municipal (CTM).

Identificação

CRC	**8384401 Crc Original: 8384401 Situação: Ativo**
Razão Social/Nome	**CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA.**
CNPJ / CPF	**02.092.332/0003-30**
Inscrição Estadual/RG	
Endereço	**29167650 - Rua Samuel Meira Brasil, 394 SALA 29.SERRA PARQ LOGIS CONJ CB5**
Bairro	**Taquara II Cidade Serra Estado ES**

Serra, Quarta-feira, 10 de Dezembro de 2025

N° da Certidão: 12114828/2025

Inscrição: 8384401

Tanto a veracidade da informação quanto a manutenção da condição de não devedor poderá ser verificada na seguinte página da Internet:
http://www.serra.es.gov.br/

ATENÇÃO: Qualquer rasura ou emenda **INVALIDARÁ** este documento.

ESTADO DO ESPÍRITO SANTO
SECRETARIA DE ESTADO DA FAZENDA

Certidão Negativa de Débitos para com a Fazenda Pública Estadual - MOD. 2

Certidão Nº 20260000028273

Identificação do Requerente: CNPJ N° 02.092.332/0003-30

Certificamos que, até a presente data, não existe débito contra o portador do Cadastro de Pessoa Jurídica acima especificado, ficando ressalvada à Fazenda Pública Estadual o direito de cobrar quaisquer dívidas que venham a ser apuradas.

Certidão emitida via Sistema Eletrônico de Processamento de Dados, nos termos do Regulamento do ICMS/ES, aprovado pelo Decreto nº 1.090-R, de 25 de outubro de 2002.

Certidão emitida em **07/01/2026**, válida até **07/04/2026**.

A autenticidade deste documento poderá ser confirmada via internet por meio do endereço **www.sefaz.es.gov.br** ou em qualquer Agência da Receita Estadual.

Vitória, 07/01/2026.

Autenticação eletrônica: **001F.4B3F.80B0.DA2B**

PREFEITURA MUNICIPAL DA SERRA

RUA MAESTRO ANTONIO CICERO, 111 CEP 29176-439 - CACAROCA - Serra - ES

Comprovante de inscrição e de situação cadastral

Cadastro - CCM	Inscrição Municipal	CPF/CNPJ	Inscrição Estadual	Data Inicio Atividade
4689721	**4689721**	**02.092.332/0003-30**		**01/07/2019**

Nome
CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA.

Nome Fantasia

Endereço	CEP
29167-650 - R SAMUEL MEIRA BRASIL, 394 SALA 29.Serra Parq Logis ;CONJ CB5	**29167-650**

Bairro	CIdade	U.F
TAQUARA II	**SERRA**	**ES**

Situação Cadastral	Simples Nacional	Tipo ISS	Data de Encerramento Ccm
Ativo	**Nao**	**4 - ISS Variável**	

Atividade Livre

Código e descrição da atividade econômica principal

4669-9/99 - Comércio atacadista de outras máquinas e equipamentos não especificados anteriormente; partes e peças

Código e descrição da atividade de licença

4669-9/99 - Comércio atacadista de outras máquinas e equipamentos não especificados anteriormente; partes e peças

Código e descrição das atividades de licença

4669-9/99 - Comércio atacadista de outras máquinas e equipamentos não especificados anteriormente; partes e peças

Código e descrição das atividades de serviço

Código e descrição dos CNAEs	Data Encerramento
4669-9/99 - Comércio atacadista de outras máquinas e equipamentos não especificados anteriormente; partes e peças **4751-2/01 - Comércio verejista especializado de equipamentos e suprimento de informática** **6209-1/00 - Suporte técnico, manutenção e outros serviços em tecnologia da informação** **6202-3/00 - Desenvolvimento e licenciamento de programas de computador customizáveis** **8599-6/03 - Treinamento em informática** **6204-0/00 - Consultoria em tecnologia da informação**	

A veracidade da informação poderá ser verificada na seguinte página da Internet: https://www.serra.es.gov.br/

Chave de Verificação: FVLCG-RHVOF

SINTEGRA/ICMS
Consulta Pública ao Cadastro
Estado do Espírito Santo

Cadastro atualizado até: 19/12/2025

IDENTIFICAÇÃO - PESSOA JURÍDICA

CNPJ:	02092332000330	**Inscrição Estadual:**	083.577.37-8
Razão Social:	CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA.		

ENDEREÇO

Logradouro:	RUA SAMUEL MEIRA BRASIL		
Número:	394	**Complemento:**	SALA 29.SERRA PARQ LOGIS ,CONJ CB5,
Bairro:	TAQUARA II		
Município:	SERRA	**UF:**	ES
CEP:	29167650	**Telefone:**	(0011) 21256270

INFORMAÇÕES COMPLEMENTARES

Atividade Econômica:

COM ATACADOUTRAS MAQ/EQUIP NAO ESPEC ANTERIORMENTE PARTES E PECAS

COM VAREJ ESPECIALIZADO DE EQUIPAMENTOS E SUPRIMENTOS DE INFORMATICA.

SUPORTE TECNICO,MANUTENCAO E OUTROS SERVICOS EM TECNOLOGIA DA INFORMAC

CONSULTORIA EM TECNOLOGIA DA INFORMACAO

TREINAMENTO EM INFORMATICA

DESENVOLVIMENTO E LICENCIAMENTO PROGRAMAS COMPUTADOR CUSTOMIZAVEIS

Data de Inicio de Atividade:	03/07/2019
Situação Cadastral Vigente:	HABILITADO
Data desta Situação Cadastral:	03/07/2019
Regime de Apuração:	ORDINÁRIO
Devedor contumaz:	Não

A Inscrição Estadual (IE) com situação cadastral vigente **HABILITADO** indica que a empresa está **APTA** a realizar operações como contribuinte do ICMS.

Já a IE com situação cadastral **NÃO HABILITADA** indica que a empresa **NÃO** está **APTA** a realizar operações como contribuinte do ICMS, caso mantenha entre as suas atividades pelo menos um CNAE cuja inscrição estadual seja obrigatória. Caso a empresa não pertença a um CNAE cuja inscrição seja obrigatória e o CNPJ esteja ATIVO (consultar o site da Receita Federal do Brasil ? http://www.receita.fazenda.gov.br), a empresa poderá ser destinatária de mercadorias, bens e serviços **como CONSUMIDOR FINAL**. Neste caso, o número da Inscrição Estadual NÃO deverá constar em documentos que acobertem operações tributáveis pelo ICMS.

A lista dos CNAEs obrigados à Inscrição Estadual está disponível no endereço:
ftp://ftp.sefaz.es.gov.br/CNAE-F/cnaes_obrigadas_a_inscricao.pdf

OBSERVAÇÃO: Os dados acima são baseados em informações fornecidas pelo contribuinte, estando sujeitos a posterior confirmação pelo Fisco.

Data da Consulta: 19/12/2025

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.007562 / pg. 3565

VOLTAR

© Copyright 2003/2025 **Secretaria de Estado da Fazenda do Espírito Santo**
Av. João Batista Parra . nº600 . Ed. Aureliano Hoffman . Enseada do Suá . Vitória-ES
CEP: 29050-375 . CNPJ: 27.080.571/0001-30

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.007562 / pg. 3566

TERMOS DE ABERTURA E ENCERRAMENTO

Entidade:	CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO LTDA		
Período da Escrituração:	01/01/2024 a 31/12/2024	CNPJ:	02.092.332/0001-79
Número de Ordem do Livro:	28		
Período Selecionado:	01 de janeiro de 2024 a 31 de dezembro de 2024		

TERMO DE ABERTURA

Nome Empresarial	CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO LTDA
NIRE	35214228052
CNPJ	02.092.332/0001-79
Número de Ordem	28
Natureza do Livro	Diario
Município	BARUERI
Data do arquivamento dos atos constitutivos	07/02/1997
Data de arquivamento do ato de conversão de sociedade simples em sociedade empresária	
Data de encerramento do exercício social	31/12/2024
Quantidade total de linhas do arquivo digital	205

TERMO DE ENCERRAMENTO

Nome Empresarial	CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO LTDA
Natureza do Livro	Diario
Número de ordem	28
Quantidade total de linhas do arquivo digital	205
Data de inicio	01/01/2024
Data de término	31/12/2024

BALANÇO PATRIMONIAL

Entidade:	CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO LTDA
Período da Escrituração:	01/01/2024 a 31/12/2024
CNPJ:	02.092.332/0001-79
Número de Ordem do Livro:	28
Período Selecionado:	01 de janeiro de 2024 a 31 de dezembro de 2024

Descrição	Nota	Saldo Inicial	Saldo Final
ATIVO		R$ 202.378.577,41	R$ 215.230.734,40
ATIVO CIRCULANTE		R$ 194.927.856,23	R$ 202.537.545,06
DISPONIBILIDADES		R$ 20.597.073,74	R$ 24.800.612,26
CAIXA GERAL		R$ 0,03	R$ 0,03
Caixa Matriz		R$ 0,03	R$ 0,03
DEPÓSITOS BANCÁRIOS À VISTA		R$ 225.360,96	R$ 479.569,50
Bancos Conta Movimento - No País		R$ 225.360,96	R$ 479.569,50
VALORES MOBILIÁRIOS - NÃO HEDGE - NO PAÍS		R$ 20.260.036,00	R$ 24.209.365,98
Títulos para Negociação - Mensurados a Valor Justo Por Meio do Resultado (VJPR) - No País		R$ 20.208.333,07	R$ 24.169.663,05
Outros Empréstimos e Recebíveis - No País		R$ 51.702,93	R$ 39.702,93
OUTRAS DISPONIBILIDADES		R$ 111.676,75	R$ 111.676,75
Outras Disponibilidades		R$ 111.676,75	R$ 111.676,75
CRÉDITOS		R$ 78.706.155,70	R$ 118.596.353,45
ADIANTAMENTOS		R$ 621.369,19	R$ 488.495,57
Adiantamentos a Fornecedores - no País - Circulante		R$ 610.412,16	R$ 488.495,57
Adiantamentos a Funcionários - Circulante		R$ 10.957,03	R$ 0,00
DUPLICATAS A RECEBER		R$ 71.509.035,25	R$ 114.149.092,07
Duplicatas a Receber - Operações com Partes Não Relacionadas - no País		R$ 71.509.035,25	R$ 114.149.092,07
TRIBUTOS A RECUPERAR		R$ 718.599,40	R$ 1.242.706,51
IPI a Recuperar		R$ 859,56	R$ 244.850,81
ICMS a Recuperar		R$ 717.739,84	R$ 997.855,70
TRIBUTOS A COMPENSAR		R$ 1.095.180,25	R$ 2.716.059,30
Imposto de Renda Retido na Fonte (IRRF)		R$ 964.413,75	R$ 1.097.827,59
IRPJ Saldo Negativo		R$ 942,39	R$ 942,39
CSLL Retida na Fonte		R$ 129.604,04	R$ 130.060,28
CSLL Recolhida por Estimativa		R$ 0,00	R$ 11.894,36
PIS/PASEP Retido na Fonte		R$ 0,00	R$ 28.791,28
COFINS Retida na Fonte		R$ 0,00	R$ 134.639,85
Outros Tributos a Compensar		R$ 220,07	R$ 1.311.903,55
OUTROS CRÉDITOS - CIRCULANTE		R$ 4.761.971,61	R$ 0,00
Demais Créditos a Receber - Circulante		R$ 4.761.971,61	R$ 0,00
ESTOQUES		R$ 95.472.458,61	R$ 58.967.032,16
ESTOQUES DE MERCADORIAS		R$ 21.099.371,77	R$ 25.372.510,63
Mercadorias para Revenda		R$ 21.099.371,77	R$ 25.372.510,63
ESTOQUES SERVIÇOS		R$ 74.373.086,84	R$ 33.594.521,53
Serviços em Andamento		R$ 74.373.086,84	R$ 33.594.521,53
DESPESAS DO EXERCÍCIO SEGUINTE		R$ 152.168,18	R$ 173.547,19
DESPESAS DO EXERCÍCIO SEGUINTE		R$ 152.168,18	R$ 173.547,19
Outros Custos e Despesas Pagos Antecipadamente		R$ 152.168,18	R$ 173.547,19
ATIVO NÃO CIRCULANTE		R$ 7.450.721,18	R$ 12.693.189,34
REALIZÁVEL A LONGO PRAZO		R$ 4.222.826,95	R$ 9.125.419,32
CRÉDITOS E VALORES - LONGO PRAZO		R$ 4.164.764,41	R$ 9.125.419,32
Mútuos com Partes Não Relacionadas - Ativo- Longo Prazo		R$ 1.288.101,80	R$ 1.430.923,33
Mútuos com Partes Relacionadas - Ativo - Longo Prazo		R$ 2.876.662,61	R$ 7.694.495,99
DESPESAS PAGAS ANTECIPADAMENTE - LONGO PRAZO		R$ 58.062,54	R$ 0,00
Prêmios de Seguros a Apropriar - Longo Prazo		R$ 58.062,54	R$ 0,00
INVESTIMENTOS		R$ 1.315.623,28	R$ 0,00
PARTICIPAÇÕES PERMANENTES EM SOCIEDADES - NO PAÍS		R$ 1.315.623,28	R$ 0,00
Participações Permanentes em Controladas - no País		R$ 1.315.623,28	R$ 0,00
IMOBILIZADO		R$ 1.912.270,98	R$ 3.567.770,05
IMOBILIZADO - AQUISIÇÃO		R$ 1.912.270,98	R$ 3.567.770,05
Máquinas, Equipamentos e Instalações Industriais		R$ 5.808.395,10	R$ 8.636.582,32
Móveis, Utensílios e Instalações Comerciais		R$ 121.581,20	R$ 123.710,62
Veículos		R$ 997.581,16	R$ 861.731,19
Outras Imobilizações por Aquisição		R$ 70.408,88	R$ 72.114,66
(-) (-) Depreciação Acumulada - Imobilizado		R$ (5.085.695,36)	R$ (6.126.368,74)
(-) INTANGÍVEL		R$ (0,03)	R$ (0,03)
(-) ATIVOS INTANGÍVEIS		R$ (0,03)	R$ (0,03)
Software ou Programas de Computador		R$ 229.787,40	R$ 229.787,40
(-) (-) Amortização Acumulada - Intangível		R$ (229.787,43)	R$ (229.787,43)
PASSIVO		R$ 202.378.577,41	R$ 215.230.734,40
PASSIVO CIRCULANTE		R$ 162.432.769,80	R$ 172.339.042,76
OBRIGAÇÕES DO CIRCULANTE		R$ 162.432.769,80	R$ 172.339.042,76
BENEFÍCIOS E ENCARGOS SOCIAIS - CIRCULANTE		R$ 305.127,40	R$ 319.049,08
Salários e Remunerações a Pagar		R$ 126.776,30	R$ 108.940,09
INSS a Recolher		R$ 135.876,09	R$ 140.588,30
FGTS a Recolher		R$ 42.475,01	R$ 47.163,13
Benefícios Rescisórios		R$ 0,00	R$ 22.357,56
FORNECEDORES - CIRCULANTE		R$ 131.439.470,20	R$ 127.512.995,25
Fornecedores - Operações com Partes Não Relacionadas - No País - Circulante		R$ 46.349.541,12	R$ 70.895.406,78
Fornecedores - Operações com Partes Não Relacionadas - No Exterior - Circulante		R$ 85.089.929,08	R$ 56.617.588,47
CONTAS A PAGAR - CIRCULANTE		R$ 680.791,22	R$ 674.381,55
Adiantamentos de Clientes - no País		R$ 680.791,22	R$ 674.381,55
EMPRÉSTIMOS OU FINANCIAMENTOS - CIRCULANTE		R$ 16.331.312,20	R$ 27.782.488,92
Empréstimos ou Financiamentos - no País - Circulante		R$ 16.331.312,20	R$ 27.782.488,92
OBRIGAÇÕES FISCAIS - CIRCULANTE		R$ 11.934.525,78	R$ 14.708.644,64
IRRF a Recolher - Circulante		R$ 137.174,52	R$ 134.873,52
IPI a Recolher - Circulante		R$ 24.175,06	R$ 68.703,49
ICMS a Recolher - Circulante		R$ 1.229.816,79	R$ 64.159,94
PIS a Recolher - Circulante		R$ 893.439,52	R$ 1.268.245,04
COFINS a Recolher - Circulante		R$ 4.120.898,20	R$ 5.849.152,68
Tributos Municipais a Recolher		R$ 1.095.913,40	R$ 1.910.034,12
Tributos Retidos a Recolher - Circulante		R$ 3.379.739,54	R$ 3.832.465,55
IRPJ a Recolher - Circulante		R$ 872.187,12	R$ 861.491,18
CSLL a Recolher - Circulante		R$ 181.181,63	R$ 719.519,12
PROVISÕES - CIRCULANTE		R$ 1.115.493,00	R$ 703.633,32
Férias a Pagar		R$ 800.092,92	R$ 703.633,32
Provisões de Natureza Tributária - Circulante		R$ 315.400,08	R$ 0,00
OUTRAS OBRIGAÇÕES - CIRCULANTE		R$ 626.050,00	R$ 637.850,00
Outras Obrigações - Circulante		R$ 626.050,00	R$ 637.850,00
PASSIVO NÃO-CIRCULANTE		R$ 11.232.016,15	R$ 13.339.999,16
OBRIGAÇÕES A LONGO PRAZO		R$ 11.232.016,15	R$ 13.339.999,16
EMPRÉSTIMOS E FINANCIAMENTOS - LONGO PRAZO		R$ 8.307.650,38	R$ 9.760.544,02
Empréstimos ou Financiamentos - no País - Longo Prazo		R$ 8.307.650,38	R$ 9.760.544,02
OBRIGAÇÕES FISCAIS - LONGO PRAZO		R$ 1.134.779,37	R$ 978.971,52
Parcelamentos Especiais e Ordinários a Recolher - Tributos Federais - Longo Prazo		R$ 1.134.779,37	R$ 978.971,52
OBRIGAÇÕES FISCAIS - LONGO PRAZO		R$ 579.262,99	R$ 0,00
Parcelamentos Especiais a Recolher - Tributos Federais - Longo Prazo		R$ 579.262,99	R$ 0,00
OUTRAS OBRIGAÇÕES - LONGO PRAZO		R$ 1.210.323,41	R$ 2.600.483,62
Mútuos - Partes Relacionadas - No Exterior - Longo Prazo		R$ 242.065,00	R$ 0,00
Outras Obrigações - Longo Prazo		R$ 968.258,41	R$ 2.600.483,62
PATRIMÔNIO LÍQUIDO		R$ 28.713.791,46	R$ 29.551.692,48
CAPITAL SOCIAL		R$ 2.100.000,00	R$ 2.100.000,00
CAPITAL REALIZADO - DE RESIDENTE NO PAÍS		R$ 2.100.000,00	R$ 2.100.000,00
Capital Subscrito de Domiciliados e Residentes no País		R$ 2.100.000,00	R$ 2.100.000,00
RESERVAS		R$ 20.322.658,31	R$ 20.322.658,31
RESERVAS DE CAPITAL		R$ 312.479,44	R$ 312.479,44
Doações e Subvenções para Investimentos (Reserva constituída até 31/12/2007)		R$ 312.479,44	R$ 312.479,44
RESERVAS DE LUCROS		R$ 20.010.178,87	R$ 20.010.178,87
Reserva Estatutária		R$ 3.365,27	R$ 3.365,27
Reserva de Prêmio na Emissão de Debêntures		R$ 6.813,60	R$ 6.813,60
Reserva para Aumento de Capital (Lei nº 9.249/1995, art. 9º, § 9º)		R$ 20.000.000,00	R$ 20.000.000,00
OUTRAS CONTAS DO PATRIMÔNIO LÍQUIDO		R$ 6.291.133,15	R$ 7.129.034,17
OUTRAS CONTAS DO PATRIMÔNIO LÍQUIDO		R$ 6.291.133,15	R$ 7.129.034,17
Lucros Acumulados e/ou Saldo à Disposição da Assembléia		R$ 6.291.133,15	R$ 7.129.034,17

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.007562 / pg. 3568

DEMONSTRAÇÃO DE RESULTADO DO EXERCÍCIO

Entidade:	CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO LTDA		
Período da Escrituração:	01/01/2024 a 31/12/2024	CNPJ:	02.092.332/0001-79
Número de Ordem do Livro:	28		
Período Selecionado:	01 de janeiro de 2024 a 31 de dezembro de 2024		

Descrição	Nota	Saldo anterior	Saldo atual
RESULTADO LÍQUIDO DO PERÍODO		R$ 7.906.003,51	R$ 3.237.901,02
RESULTADO LÍQUIDO DO PERÍODO ANTES DO IRPJ E DA CSLL - ATIVIDADE GERAL		R$ 11.978.982,76	R$ 8.490.460,36
RESULTADO OPERACIONAL		R$ 11.978.982,76	R$ 8.490.460,36
RECEITA LIQUIDA		R$ 325.056.235,47	R$ 366.972.520,15
RECEITA BRUTA		R$ 349.413.792,55	R$ 392.792.187,25
Receita da Revenda de Mercadorias no Mercado Interno		R$ 66.143.834,09	R$ 76.359.088,68
Receita da Prestação de Serviços no Mercado Interno		R$ 280.065.463,51	R$ 311.273.930,27
Receita da Locação de Bens Móveis e Imóveis		R$ 3.204.494,95	R$ 5.159.168,30
(-) DEDUÇÕES DA RECEITA BRUTA		R$ (24.357.557,08)	R$ (25.819.667,10)
(-) (-) Vendas Canceladas e Devoluções de Vendas		R$ (3.826.515,02)	R$ (3.574.972,58)
(-) (-) ICMS		R$ (6.534.418,71)	R$ (6.591.356,59)
(-) (-) COFINS Sobre Receita Bruta		R$ (2.379.233,19)	R$ (534.757,38)
(-) (-) PIS/PASEP Sobre Receita Bruta		R$ (4.701.632,04)	R$ (6.228.846,52)
(-) (-) ISS		R$ (5.516.439,73)	R$ (6.319.089,25)
(-) (-) Demais Impostos e Contribuições Incidentes sobre Vendas e Serviços		R$ (1.399.318,39)	R$ (2.570.644,78)
(-) CUSTO DOS BENS E SERVIÇOS		R$ (259.587.255,22)	R$ (277.452.578,34)
(-) CUSTO DOS BENS E SERVIÇOS VENDIDOS DAS ATIVIDADES EM GERAL		R$ (259.587.255,22)	R$ (277.452.578,34)
(-) (-) Custo das Mercadorias Revendidas		R$ (33.121.244,66)	R$ (31.332.945,49)
(-) (-) Custo dos Serviços Prestados		R$ (226.466.010,56)	R$ (246.119.632,85)
OUTRAS RECEITAS OPERACIONAIS		R$ 17.672.979,63	R$ 10.315.759,77
OUTRAS RECEITAS OPERACIONAIS DAS ATIVIDADES EM GERAL		R$ 17.672.979,63	R$ 10.315.759,77
Variações Cambiais Ativas		R$ 12.554.608,17	R$ 4.363.687,75
Outras Receitas Financeiras		R$ 2.186.421,00	R$ 1.662.014,45
Outras Receitas Operacionais		R$ 2.931.950,46	R$ 4.290.057,57
(-) DESPESAS OPERACIONAIS		R$ (33.028.315,71)	R$ (43.349.431,49)
(-) DESPESAS OPERACIONAIS DAS ATIVIDADES EM GERAL		R$ (33.028.315,71)	R$ (43.349.431,49)
(-) (-) Ordenados, Salários, Gratificações e Outras Remunerações a Empregados		R$ (4.314.232,45)	R$ (4.317.014,33)
(-) (-) Outros Gastos com Pessoal		R$ (987.943,68)	R$ (1.353.756,23)
(-) (-) Encargos Sociais - Previdência Social		R$ (1.304.894,00)	R$ (1.359.741,70)
(-) (-) Encargos Sociais - FGTS		R$ (399.861,25)	R$ (469.434,92)
(-) (-) Alimentação do Trabalhador		R$ (517.486,04)	R$ (543.163,63)
(-) (-) COFINS		R$ (19.299.611,34)	R$ (28.176.522,85)
(-) (-) Demais Impostos, Taxas e Contribuições, exceto IR e CSLL		R$ (933.967,80)	R$ (894.102,96)
(-) (-) Aluguéis		R$ (115.941,46)	R$ (142.804,29)
(-) (-) Despesas com Veículos e de Conservação de Bens e Instalações		R$ (136.356,27)	R$ (87.802,25)
(-) (-) Propaganda, Publicidade e Patrocínio		R$ (3.383.211,64)	R$ (4.366.936,20)
(-) (-) Encargos de Depreciação		R$ (1.136.954,13)	R$ (1.225.333,35)
(-) (-) Assistência Médica, Odontológica e Farmacêutica a Empregados		R$ (4.510,78)	R$ (2.105,40)
(-) (-) Despesas com Energia Elétrica		R$ (10.379,76)	R$ (27.910,42)
(-) (-) Despesas com Telefone e Internet		R$ (196.775,98)	R$ (125.713,52)
(-) (-) Despesas com Seguros		R$ (286.189,13)	R$ (257.089,44)
(-) OUTRAS DESPESAS OPERACIONAIS		R$ (38.256.761,41)	R$ (48.234.619,73)
(-) OUTRAS DESPESAS OPERACIONAIS DAS ATIVIDADES EM GERAL		R$ (38.256.761,41)	R$ (48.234.619,73)
(-) (-) Variações Cambiais Passivas		R$ (9.866.720,92)	R$ (14.324.876,34)
(-) (-) Outras Despesas Financeiras		R$ (4.376.131,47)	R$ (5.899.108,04)
(-) (-) Outras Despesas Operacionais		R$ (24.013.909,02)	R$ (28.010.635,35)
OUTRAS RECEITAS, OUTRAS DESPESAS E RESULTADO DE OPERAÇÕES DESCONTINUADAS		R$ 122.100,00	R$ 238.810,00
OUTRAS RECEITAS, OUTRAS DESPESAS E RESULTADO DE OPERAÇÕES DESCONTINUADAS DAS ATIVIDADES EM GERAL		R$ 122.100,00	R$ 238.810,00
Receitas de Alienações de Bens e Direitos do Ativo Não Circulante Investimentos, Imobilizado e Intangível		R$ 135.500,00	R$ 252.000,00
(-) (-) Valor Contábil dos Bens e Direitos do Ativo Não Circulante Investimentos, Intangível e Imobilizado Alienados		R$ (13.400,00)	R$ (13.190,00)
(-) PROVISÃO PARA CSLL E IRPJ		R$ (4.072.979,25)	R$ (5.252.559,34)
(-) PROVISÃO PARA CSLL E IRPJ		R$ (4.072.979,25)	R$ (5.252.559,34)
(-) PROVISÃO PARA CSLL E IRPJ		R$ (4.072.979,25)	R$ (5.252.559,34)
(-) PROVISÃO PARA CSLL E IRPJ		R$ (4.072.979,25)	R$ (5.252.559,34)
(-) (-) Provisão para Contribuição Social sobre o Lucro Líquido (Atividade Geral)		R$ (1.099.841,03)	R$ (1.396.736,30)
(-) (-) Provisão para Imposto de Renda - Pessoa Jurídica (Atividade Geral e Rural)		R$ (2.973.138,22)	R$ (3.855.823,04)

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.007562 / pg. 3569

MINISTÉRIO DA FAZENDA
SECRETARIA DA RECEITA FEDERAL DO BRASIL
SISTEMA PÚBLICO DE ESCRITURAÇÃO DIGITAL – Sped Versão: 10.3.3

RECIBO DE ENTREGA DE ESCRITURAÇÃO CONTÁBIL DIGITAL

IDENTIFICAÇÃO DO TITULAR DA ESCRITURAÇÃO

NIRE	CNPJ	
35214228052	02.092.332/0001-79	

NOME EMPRESARIAL
CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO LTDA

IDENTIFICAÇÃO DA ESCRITURAÇÃO

FORMA DA ESCRITURAÇÃO CONTÁBIL	PERÍODO DA ESCRITURAÇÃO
Livro Diário (Completo - sem escrituração Auxiliar)	01/01/2024 a 31/12/2024
NATUREZA DO LIVRO	**NÚMERO DO LIVRO**
Diario	28

IDENTIFICAÇÃO DO ARQUIVO (HASH)
F0.48.9E.7F.70.C7.30.CB.3B.67.9A.E6.71.59.79.18.75.5B.81.BA

ARQUIVOS SUBSTITUÍDOS (HASH)

ESTE LIVRO FOI ASSINADO COM OS SEGUINTES CERTIFICADOS DIGITAIS:

QUALIFICAÇÃO DO SIGNATARIO	CPF/CNPJ	NOME	Nº SÉRIE DO CERTIFICADO	VALIDADE	RESPONSÁVEL LEGAL
Contador	38636784867	BRUNA DA SILVA VIG:38636784867	680952307935435543 6	30/01/2025 a 30/01/2028	Não
Procurador	38636784867	BRUNA DA SILVA VIG:38636784867	680952307935435543 6	30/01/2025 a 30/01/2028	Sim

NÚMERO DO RECIBO:

F0.48.9E.7F.70.C7.30.CB.3B.67.9A.E6.
71.59.79.18.75.5B.81.BA-3

Escrituração recebida via Internet
pelo Agente Receptor SERPRO

em 30/06/2025 às 10:31:27

0D.B6.10.14.BB.2C.B1.9C
69.7B.36.4D.5B.18.95.C3

Considera-se autenticado o livro contábil a que se refere este recibo, dispensando-se a autenticação de que trata o art. 39 da Lei nº 8.934/1994. Este recibo comprova a autenticação.

BASE LEGAL: Decreto nº 1.800/1996, com a alteração do Decreto nº 8.683/2016, e arts. 39, 39-A, 39-B da Lei nº 8.934/1994 com a alteração da Lei Complementar nº 1247/2014.

CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO LTDA.
CNPJ: 02.092.332/0001-79
Índices
Valores em Reais

EBITDA	**2024**
Lucro líquido contábil	3.238
(+) Imposto de Renda e CSSLL	5.253
(+) Depreciações e Amortizações	1.225
(+) Resultado financeiro líquido	14.627
	24.343

ÍNDICES DE LIQUIDEZ

Liquidez Corrente = Ativo Circulante / Passivo Circulante

Ativo Circulante	201.114	**1,17**
Passivo Circulante	171.701	

Liquidez Seca = (Ativo Circulante - Estoques) / Passivo Circulante

Ativo Circulante (-) Estoques	142.147	**0,83**
Passivo Circulante	171.701	

Liquidez Imediata = Disponível / Passivo Circulante

Disponível	26.205	**0,15**
Passivo Circulante	171.701	

Liquidez Geral = (Ativo Circulante + Realizável a Longo Prazo) / (Passivo Circulante + Passivo Não Circulante)

Ativo Circulante (+) Realizável a Longo Prazo	211.662	**1,14**
Passivo Circulante (+) Passivo Não Circulante	185.679	

Solvência Geral = Ativo Total / (Passivo Circulante + Passivo Não Circulante)

Ativo Total	215.231	**1,16**
Passivo Circulante (+) Passivo Não Circulante	185.679	

FRANCISCO JOSE DE ARRUDA CAMARGO:20172362849
Assinado de forma digital por FRANCISCO JOSE DE ARRUDA CAMARGO:20172362849
Dados: 2025.08.01 11:44:55 -03'00'

Fancisco José de Arruda Camargo
CPF: 201.723.628-49
Representante Legal

BRUNA DA SILVA VIG:38636784867
Assinado de forma digital por BRUNA DA SILVA VIG:38636784867
Dados: 2025.08.01 11:28:50 -03'00'

Bruna da Silva Vig
CRC: 1SP-329828/O-5
Contador

TERMOS DE ABERTURA E ENCERRAMENTO

Entidade:	CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO LTDA		
Período da Escrituração:	01/01/2023 a 31/12/2023	CNPJ:	02.092.332/0001-79
Número de Ordem do Livro:	27		

TERMO DE ABERTURA

Nome Empresarial	CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO LTDA
NIRE	35214228052
CNPJ	02.092.332/0001-79
Número de Ordem	27
Natureza do Livro	Diario
Município	BARUERI
Data do arquivamento dos atos constitutivos	07/02/1997
Data de arquivamento do ato de conversão de sociedade simples em sociedade empresária	
Data de encerramento do exercício social	31/12/2023
Quantidade total de linhas do arquivo digital	103133

TERMO DE ENCERRAMENTO

Nome Empresarial	CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO LTDA
Natureza do Livro	Diário
Número de ordem	27
Quantidade total de linhas do arquivo digital	103133
Data de inicio	01/01/2023
Data de término	31/12/2023

Este documento é parte integrante de escrituração cuja autenticação se comprova pelo recibo de número CF.76.98.CC.21.6B.66.0E.89.4F.61.A9.97.D0.BF.F6.B5.16.1F.99-9, nos termos do Decreto nº 8.683/2016.

Este relatório foi gerado pelo Sistema Público de Escrituração Digital – Sped

DEMONSTRAÇÃO DE RESULTADO DO EXERCÍCIO

Entidade:	CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO LTDA
Período da Escrituração:	01/01/2023 a 31/12/2023 — CNPJ: 02.092.332/0001-79
Número de Ordem do Livro:	27
Período Selecionado:	01 de Janeiro de 2023 a 31 de Dezembro de 2023

Descrição	Nota	Saldo anterior	Saldo atual
RESULTADO LÍQUIDO DO PERÍODO		R$ 14.020.006,97	R$ 7.906.003,51
RESULTADO LÍQUIDO DO PERÍODO ANTES DO IRPJ E DA CSLL - ATIVIDADE GERAL		R$ 20.058.174,44	R$ 11.978.982,76
RESULTADO OPERACIONAL		R$ 20.058.174,44	R$ 11.978.982,76
RECEITA LIQUIDA		R$ 279.165.064,59	R$ 325.056.235,47
RECEITA BRUTA		R$ 301.612.630,17	R$ 349.413.792,55
Receita da Revenda de Mercadorias no Mercado Interno		R$ 49.113.948,41	R$ 66.143.834,09
Receita da Prestação de Serviços no Mercado Interno		R$ 250.100.035,47	R$ 280.065.463,51
Receita da Locação de Bens Móveis e Imóveis		R$ 2.398.646,29	R$ 3.204.494,95
(-) DEDUÇÕES DA RECEITA BRUTA		R$ (22.447.565,58)	R$ (24.357.557,08)
(-) (-) Vendas Canceladas e Devoluções de Vendas		R$ (898.228,52)	R$ (3.826.515,02)
(-) (-) ICMS		R$ (4.873.913,34)	R$ (6.534.418,71)
(-) (-) COFINS Sobre Receita Bruta		R$ (7.550.652,76)	R$ (2.379.233,19)
(-) (-) PIS/PASEP Sobre Receita Bruta		R$ (2.585.879,59)	R$ (4.701.632,04)
(-) (-) ISS		R$ (5.036.465,79)	R$ (5.516.439,73)
(-) (-) Demais Impostos e Contribuições Incidentes sobre Vendas e Serviços		R$ (1.502.425,58)	R$ (1.399.318,39)
(-) CUSTO DOS BENS E SERVIÇOS		R$ (233.192.547,87)	R$ (259.587.255,22)
(-) CUSTO DOS BENS E SERVIÇOS VENDIDOS DAS ATIVIDADES EM GERAL		R$ (233.192.547,87)	R$ (259.587.255,22)
(-) (-) Custo das Mercadorias Revendidas		R$ (29.501.100,08)	R$ (33.121.244,66)
(-) (-) Custo dos Serviços Prestados		R$ (203.691.447,79)	R$ (226.466.010,56)
OUTRAS RECEITAS OPERACIONAIS		R$ 16.137.489,84	R$ 17.672.979,63
OUTRAS RECEITAS OPERACIONAIS DAS ATIVIDADES EM GERAL		R$ 16.137.489,84	R$ 17.672.979,63
Variações Cambiais Ativas		R$ 12.643.814,58	R$ 12.554.608,17
Outras Receitas Financeiras		R$ 1.464.224,66	R$ 2.186.421,00
Outras Receitas Operacionais		R$ 2.029.450,60	R$ 2.931.950,46
(-) DESPESAS OPERACIONAIS		R$ (14.189.886,28)	R$ (33.028.315,71)
(-) DESPESAS OPERACIONAIS DAS ATIVIDADES EM GERAL		R$ (14.189.886,28)	R$ (33.028.315,71)
(-) (-) Ordenados, Salários, Gratificações e Outras Remunerações a Empregados		R$ (3.345.298,10)	R$ (4.314.232,45)
(-) (-) Outros Gastos com Pessoal		R$ (666.160,17)	R$ (987.943,68)
(-) (-) Encargos Sociais - Previdência Social		R$ (1.101.125,09)	R$ (1.304.894,00)
(-) (-) Encargos Sociais - FGTS		R$ (350.509,39)	R$ (399.861,25)
(-) Encargos Sociais - Outros		R$ (3.195,44)	R$ 0,00
(-) (-) Alimentação do Trabalhador		R$ (355.202,00)	R$ (517.486,04)
(-) (-) COFINS		R$ (4.390.083,08)	R$ (19.299.611,34)
(-) (-) Demais Impostos, Taxas e Contribuições, exceto IR e CSLL		R$ (637.446,90)	R$ (933.967,80)
(-) (-) Aluguéis		R$ (103.737,13)	R$ (115.941,46)
(-) (-) Despesas com Veículos e de Conservação de Bens e Instalações		R$ (122.870,02)	R$ (136.356,27)
(-) (-) Propaganda, Publicidade e Patrocínio		R$ (1.430.041,89)	R$ (3.383.211,64)
(-) (-) Encargos de Depreciação		R$ (1.268.512,77)	R$ (1.136.954,13)
(-) (-) Assistência Médica, Odontológica e Farmacêutica a Empregados		R$ (4.926,63)	R$ (4.510,78)
(-) (-) Despesas com Energia Elétrica		R$ (6.029,97)	R$ (10.379,76)
(-) (-) Despesas com Telefone e Internet		R$ (141.766,99)	R$ (196.775,98)
(-) (-) Despesas com Seguros		R$ (262.980,71)	R$ (286.189,13)
(-) OUTRAS DESPESAS OPERACIONAIS		R$ (27.861.945,84)	R$ (38.256.761,41)
(-) OUTRAS DESPESAS OPERACIONAIS DAS ATIVIDADES EM GERAL		R$ (27.861.945,84)	R$ (38.256.761,41)
(-) (-) Variações Cambiais Passivas		R$ (9.457.816,59)	R$ (9.866.720,92)
(-) (-) Outras Despesas Financeiras		R$ (3.661.290,89)	R$ (4.376.131,47)
(-) (-) Outras Despesas Operacionais		R$ (14.742.838,36)	R$ (24.013.909,02)
OUTRAS RECEITAS, OUTRAS DESPESAS E RESULTADO DE OPERAÇÕES DESCONTINUADAS		R$ 0,00	R$ 122.100,00
OUTRAS RECEITAS, OUTRAS DESPESAS E RESULTADO DE OPERAÇÕES DESCONTINUADAS DAS ATIVIDADES EM GERAL		R$ (0,00)	R$ 122.100,00
Receitas de Alienações de Bens e Direitos do Ativo Não Circulante Investimentos, Imobilizado e Intangível		R$ (0,00)	R$ 135.500,00
(-) (-) Valor Contábil dos Bens e Direitos do Ativo Não Circulante Investimentos, Intangível e Imobilizado Alienados		R$ 0,00	R$ (13.400,00)
(-) PROVISÃO PARA CSLL E IRPJ		R$ (6.038.167,47)	R$ (4.072.979,25)
(-) PROVISÃO PARA CSLL E IRPJ		R$ (6.038.167,47)	R$ (4.072.979,25)
(-) PROVISÃO PARA CSLL E IRPJ		R$ (6.038.167,47)	R$ (4.072.979,25)
(-) PROVISÃO PARA CSLL E IRPJ		R$ (6.038.167,47)	R$ (4.072.979,25)
(-) (-) Provisão para Contribuição Social sobre o Lucro Líquido (Atividade Geral)		R$ (1.604.691,39)	R$ (1.099.841,03)
(-) (-) Provisão para Imposto de Renda - Pessoa Jurídica (Atividade Geral e Rural)		R$ (4.433.476,08)	R$ (2.973.138,22)

Este documento é parte integrante de escrituração cuja autenticação se comprova pelo recibo de número CF.76.98.CC.21.6B.66.0E.89.4F.61.A9.97.D0.BF.F6.B5.16.1F.99-9, nos termos do Decreto nº 8.683/2016.

Este relatório foi gerado pelo Sistema Público de Escrituração Digital – Sped

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.007562 / pg. 3573

BALANÇO PATRIMONIAL

Entidade:	CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO LTDA
Período da Escrituração:	01/01/2023 a 31/12/2023
CNPJ:	02.092.332/0001-79
Número de Ordem do Livro:	27
Período Selecionado:	01 de Janeiro de 2023 a 31 de Dezembro de 2023

Descrição	Nota	Saldo Inicial	Saldo Final
ATIVO		R$ 160.826.445,33	R$ 202.378.577,41
ATIVO CIRCULANTE		R$ 148.862.400,87	R$ 194.927.856,23
DISPONIBILIDADES		R$ 20.759.007,01	R$ 20.597.073,74
CAIXA GERAL		R$ 0,03	R$ 0,03
Caixa Matriz		R$ 0,03	R$ 0,03
DEPÓSITOS BANCÁRIOS À VISTA		R$ 298.892,28	R$ 225.360,96
Bancos Conta Movimento - No País		R$ 298.892,28	R$ 225.360,96
VALORES MOBILIÁRIOS - NÃO HEDGE - NO PAÍS		R$ 19.459.913,16	R$ 20.260.036,00
Títulos para Negociação - Mensurados a Valor Justo Por Meio do Resultado (VJPR) - No País		R$ 19.459.913,03	R$ 20.208.333,07
Outros Empréstimos e Recebíveis - No País		R$ 0,13	R$ 51.702,93
OUTRAS DISPONIBILIDADES		R$ 1.000.201,54	R$ 111.676,75
Outras Disponibilidades		R$ 1.000.201,54	R$ 111.676,75
CRÉDITOS		R$ 60.619.582,12	R$ 78.706.155,70
ADIANTAMENTOS		R$ 1.132.154,42	R$ 621.369,19
Adiantamentos a Fornecedores - no País - Circulante		R$ 1.123.592,22	R$ 610.412,16
Adiantamentos a Funcionários - Circulante		R$ 8.562,20	R$ 10.957,03
DUPLICATAS A RECEBER		R$ 58.337.787,52	R$ 71.509.035,25
Duplicatas a Receber - Operações com Partes Não Relacionadas - no País		R$ 58.337.787,52	R$ 71.509.035,25
TRIBUTOS A RECUPERAR		R$ 1.148.477,72	R$ 718.599,40
IPI a Recuperar		R$ 9.207,39	R$ 859,56
ICMS a Recuperar		R$ 1.139.270,33	R$ 717.739,84
TRIBUTOS A COMPENSAR		R$ 1.162,46	R$ 1.095.180,25
Imposto de Renda Retido na Fonte (IRRF)		R$ 0,00	R$ 964.413,75
IRPJ Saldo Negativo		R$ 942,39	R$ 942,39
CSLL Retida na Fonte		R$ 0,00	R$ 129.604,04
Outros Tributos a Compensar		R$ 220,07	R$ 220,07
OUTROS CRÉDITOS - CIRCULANTE		R$ 0,00	R$ 4.761.971,61
Demais Créditos a Receber - Circulante		R$ 0,00	R$ 4.761.971,61
ESTOQUES		R$ 67.483.811,74	R$ 95.472.458,61
ESTOQUES DE MERCADORIAS		R$ 26.948.051,94	R$ 21.099.371,77
Mercadorias para Revenda		R$ 26.948.051,94	R$ 21.099.371,77
ESTOQUES SERVIÇOS		R$ 40.535.759,80	R$ 74.373.086,84
Serviços em Andamento		R$ 40.535.759,80	R$ 74.373.086,84
DESPESAS DO EXERCÍCIO SEGUINTE		R$ 0,00	R$ 152.168,18
DESPESAS DO EXERCÍCIO SEGUINTE		R$ 0,00	R$ 152.168,18
Outros Custos e Despesas Pagos Antecipadamente		R$ 0,00	R$ 152.168,18
ATIVO NÃO CIRCULANTE		R$ 11.964.044,46	R$ 7.450.721,18
REALIZÁVEL A LONGO PRAZO		R$ 8.253.735,75	R$ 4.222.826,95
CRÉDITOS E VALORES - LONGO PRAZO		R$ 8.253.735,75	R$ 4.164.764,41
Mútuos com Partes Não Relacionadas - Ativo- Longo Prazo		R$ 1.064.140,20	R$ 1.288.101,80
Mútuos com Partes Relacionadas - Ativo - Longo Prazo		R$ 7.189.595,55	R$ 2.876.662,61
DESPESAS PAGAS ANTECIPADAMENTE - LONGO PRAZO		R$ 0,00	R$ 58.062,54
Prêmios de Seguros a Apropriar - Longo Prazo		R$ 0,00	R$ 58.062,54
INVESTIMENTOS		R$ 1.417.909,98	R$ 1.315.623,28
PARTICIPAÇÕES PERMANENTES EM SOCIEDADES - NO PAIS		R$ 1.417.909,98	R$ 1.315.623,28
Participações Permanentes em Controladas - no País		R$ 1.417.909,98	R$ 1.315.623,28
IMOBILIZADO		R$ 2.265.312,65	R$ 1.912.270,98
IMOBILIZADO - AQUISIÇÃO		R$ 2.265.312,65	R$ 1.912.270,98
Máquinas, Equipamentos e Instalações Industriais		R$ 4.963.909,00	R$ 5.808.395,10
Móveis, Utensílios e Instalações Comerciais		R$ 114.281,20	R$ 121.581,20
Veículos		R$ 1.130.581,16	R$ 997.581,16
Outras Imobilizações por Aquisição		R$ 151.968,63	R$ 70.408,88
(-) (-) Depreciação Acumulada - Imobilizado		R$ (4.095.427,34)	R$ (5.085.695,36)
INTANGÍVEL		R$ 27.086,08	R$ (0,03)
ATIVOS INTANGÍVEIS		R$ 27.086,08	R$ (0,03)
Software ou Programas de Computador		R$ 229.787,40	R$ 229.787,40
(-) (-) Amortização Acumulada - Intangível		R$ (202.701,32)	R$ (229.787,43)
PASSIVO		R$ 160.826.445,33	R$ 202.378.577,41
PASSIVO CIRCULANTE		R$ 122.753.882,38	R$ 162.432.769,80
OBRIGAÇÕES DO CIRCULANTE		R$ 122.753.882,38	R$ 162.432.769,80
BENEFÍCIOS E ENCARGOS SOCIAIS - CIRCULANTE		R$ 241.020,05	R$ 305.127,40
Salários e Remunerações a Pagar		R$ 92.935,80	R$ 126.776,30
INSS a Recolher		R$ 108.949,42	R$ 135.876,09
FGTS a Recolher		R$ 37.388,20	R$ 42.475,01
Demais Encargos a Recolher		R$ 1.746,63	R$ 0,00
FORNECEDORES - CIRCULANTE		R$ 102.043.000,33	R$ 131.439.470,20
Fornecedores - Operações com Partes Não Relacionadas - No País - Circulante		R$ 37.385.885,70	R$ 46.349.541,12
Fornecedores - Operações com Partes Não Relacionadas - No Exterior - Circulante		R$ 64.657.114,63	R$ 85.089.929,08
CONTAS A PAGAR - CIRCULANTE		R$ 1.247.488,97	R$ 680.791,22
Adiantamentos de Clientes - no País		R$ 1.247.488,97	R$ 680.791,22
EMPRÉSTIMOS OU FINANCIAMENTOS - CIRCULANTE		R$ 12.417.644,03	R$ 16.331.312,20
Empréstimos ou Financiamentos - no País - Circulante		R$ 12.417.644,03	R$ 16.331.312,20
OBRIGAÇÕES FISCAIS - CIRCULANTE		R$ 5.702.994,82	R$ 11.934.525,78
IRRF a Recolher - Circulante		R$ 108.416,09	R$ 137.174,52
IPI a Recolher - Circulante		R$ 46.918,45	R$ 24.175,06
ICMS a Recolher - Circulante		R$ 190.254,33	R$ 1.229.816,79
PIS a Recolher - Circulante		R$ 280.167,54	R$ 893.439,52
COFINS a Recolher - Circulante		R$ 1.292.095,82	R$ 4.120.898,20
Tributos Municipais a Recolher		R$ 577.531,39	R$ 1.095.913,40
Tributos Retidos a Recolher - Circulante		R$ 280.759,95	R$ 3.379.739,54
IRPJ a Recolher - Circulante		R$ 2.450.641,20	R$ 872.187,12
CSLL a Recolher - Circulante		R$ 476.210,05	R$ 181.181,63
PROVISÕES - CIRCULANTE		R$ 1.001.734,18	R$ 1.115.493,00
Férias a Pagar		R$ 565.830,46	R$ 800.092,92
Provisões de Natureza Tributária - Circulante		R$ 435.903,72	R$ 315.400,08
OUTRAS OBRIGAÇÕES - CIRCULANTE		R$ 100.000,00	R$ 626.050,00
Outras Obrigações - Circulante		R$ 100.000,00	R$ 626.050,00
PASSIVO NÃO-CIRCULANTE		R$ 10.184.220,03	R$ 11.232.016,15
OBRIGAÇÕES A LONGO PRAZO		R$ 10.184.220,03	R$ 11.232.016,15
EMPRÉSTIMOS E FINANCIAMENTOS - LONGO PRAZO		R$ 6.784.572,06	R$ 8.307.650,38
Empréstimos ou Financiamentos - no País - Longo Prazo		R$ 6.784.572,06	R$ 8.307.650,38
OBRIGAÇÕES FISCAIS - LONGO PRAZO		R$ 1.260.152,22	R$ 1.134.779,37
Parcelamentos Especiais e Ordinários a Recolher - Tributos Federais - Longo Prazo		R$ 1.260.152,22	R$ 1.134.779,37
OBRIGAÇÕES FISCAIS - LONGO PRAZO		R$ 1.095.955,75	R$ 579.262,99
Parcelamentos Especiais a Recolher - Tributos Federais - Longo Prazo		R$ 1.095.955,75	R$ 579.262,99
OUTRAS OBRIGAÇÕES - LONGO PRAZO		R$ 1.043.540,00	R$ 1.210.323,41
Mútuos - Partes Relacionadas - No Exterior - Longo Prazo		R$ 1.043.540,00	R$ 242.065,00
Outras Obrigações - Longo Prazo		R$ 0,00	R$ 968.258,41
PATRIMÔNIO LÍQUIDO		R$ 27.888.342,92	R$ 28.713.791,46
CAPITAL SOCIAL		R$ 2.100.000,00	R$ 2.100.000,00
CAPITAL REALIZADO - DE RESIDENTE NO PAÍS		R$ 2.100.000,00	R$ 2.100.000,00
Capital Subscrito de Domiciliados e Residentes no País		R$ 2.100.000,00	R$ 2.100.000,00
RESERVAS		R$ 322.658,31	R$ 20.322.658,31
RESERVAS DE CAPITAL		R$ 312.479,44	R$ 312.479,44
Doações e Subvenções para Investimentos (Reserva constituída até 31/12/2007)		R$ 312.479,44	R$ 312.479,44
RESERVAS DE LUCROS		R$ 10.178,87	R$ 20.010.178,87
Reserva Estatutária		R$ 3.365,27	R$ 3.365,27
Reserva de Prêmio na Emissão de Debêntures		R$ 6.813,60	R$ 6.813,60
Reserva para Aumento de Capital (Lei nº 9.249/1995, art. 9º, § 9º)		R$ 0,00	R$ 20.000.000,00
OUTRAS CONTAS DO PATRIMÔNIO LÍQUIDO		R$ 25.465.684,61	R$ 6.291.133,15
OUTRAS CONTAS DO PATRIMÔNIO LÍQUIDO		R$ 25.465.684,61	R$ 6.291.133,15
Lucros Acumulados e/ou Saldo à Disposição da Assembléia		R$ 25.465.684,61	R$ 6.291.133,15

Este documento é parte integrante de escrituração cuja autenticação se comprova pelo recibo de número CF.76.98.CC.21.6B.66.0E.89.4F.61.A9.97.D0.BF.F6.B5.16.1F.99-9, nos termos do Decreto nº 8.683/2016.

Este relatório foi gerado pelo Sistema Público de Escrituração Digital – Sped

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.007562 / pg. 3574

MINISTÉRIO DA FAZENDA
SECRETARIA DA RECEITA FEDERAL DO BRASIL
SISTEMA PÚBLICO DE ESCRITURAÇÃO DIGITAL – Sped Versão: 10.2.1

RECIBO DE ENTREGA DE ESCRITURAÇÃO CONTÁBIL DIGITAL

IDENTIFICAÇÃO DO TITULAR DA ESCRITURAÇÃO

NIRE	CNPJ	
35214228052	02.092.332/0001-79	

NOME EMPRESARIAL
CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO LTDA

IDENTIFICAÇÃO DA ESCRITURAÇÃO

FORMA DA ESCRITURAÇÃO CONTÁBIL	PERÍODO DA ESCRITURAÇÃO
Livro Diário (Completo - sem escrituração Auxiliar)	01/01/2023 a 31/12/2023
NATUREZA DO LIVRO	**NÚMERO DO LIVRO**
Diario	27

IDENTIFICAÇÃO DO ARQUIVO (HASH)
CF.76.98.CC.21.6B.66.0E.89.4F.61.A9.97.D0.BF.F6.B5.16.1F.99

ESTE LIVRO FOI ASSINADO COM OS SEGUINTES CERTIFICADOS DIGITAIS:

QUALIFICAÇÃO DO SIGNATARIO	CPF/CNPJ	NOME	Nº SÉRIE DO CERTIFICADO	VALIDADE	RESPONSÁVEL LEGAL
PROCURADOR	03640170822	EDUARDO MARQUES DE ASSIS:03640170822	519317200595027996 0	26/08/2021 a 26/08/2024	Sim
CONTADOR	03640170822	EDUARDO MARQUES DE ASSIS:03640170822	519317200595027996 0	26/08/2021 a 26/08/2024	Não

NÚMERO DO RECIBO:

CF.76.98.CC.21.6B.66.0E.89.4F.61.A9.
97.D0.BF.F6.B5.16.1F.99-9

Escrituração recebida via Internet
pelo Agente Receptor SERPRO

em 19/06/2024 às 15:01:05

EA.24.B9.D0.04.C4.5C.08
7D.5F.81.2D.C7.EC.0F.D0

Considera-se autenticado o livro contábil a que se refere este recibo, dispensando-se a autenticação de que trata o art. 39 da Lei nº 8.934/1994. Este recibo comprova a autenticação.

BASE LEGAL: Decreto nº 1.800/1996, com a alteração do Decreto nº 8.683/2016, e arts. 39, 39-A, 39-B da Lei nº 8.934/1994 com a alteração da Lei Complementar nº 1247/2014.

CLM SOFTWARE COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO LTDA.
CNPJ: 02.092.332/0001-79
Índices
Valores em Reais

EBITDA	2023	2022	2021
Lucro líquido contábil	7.906	14.020	8.615
(+) Imposto de Renda e CSSLL	4.072	6.038	5.728
(+) Depreciações e Amortizações	1.136	1.269	329
(+) Resultado financeiro líquido	-3.552	-3.280	8.379
	9.562	18.047	23.051

ÍNDICES DE LIQUIDEZ

Liquidez Corrente = Ativo Circulante / Passivo Circulante

Ativo Circulante	194.927	**1,20**	148.862	**1,21**	125.305	**1,15**
Passivo Circulante	162.432		122.754		108.587	

Liquidez Seca = (Ativo Circulante - Estoques) / Passivo Circulante

Ativo Circulante (-) Estoques	99.455	**0,61**	81.379	**0,66**	86.926	**0,80**
Passivo Circulante	162.432		122.754		108.587	

Liquidez Imediata = Disponível / Passivo Circulante

Disponível	20.597	**0,13**	20.759	**0,17**	11.206	**0,10**
Passivo Circulante	162.432		122.754		108.587	

Liquidez Geral = (Ativo Circulante + Realizável a Longo Prazo) / (Passivo Circulante + Passivo Não Circulante)

Ativo Circulante (+) Realizável a Longo Prazo	199.149	**1,15**	157.116	**1,18**	132.886.304	**1,08**
Passivo Circulante (+) Passivo Não Circulante	173.664		132.938		122.760.498	

Solvência Geral = Ativo Total / (Passivo Circulante + Passivo Não Circulante)

Ativo Total	202.378	**1,17**	160.826	**1,21**	136.733	**1,11**
Passivo Circulante (+) Passivo Não Circulante	173.664		132.938		122.760	

FRANCISCO JOSE DE ARRUDA CAMARGO:20172362849
Assinado de forma digital por FRANCISCO JOSE DE ARRUDA CAMARGO:20172362849 Dados: 2024.09.26 09:04:41 -03'00'

Francisco José de Arruda Camargo
CPF: 201.723.628-49
Representant Legal

EDUARDO MARQUES DE ASSIS:03640170822
Assinado de forma digital por EDUARDO MARQUES DE ASSIS:03640170822 Dados: 2024.09.26 08:51:48 -03'00'

Eduardo Marques de Assis
Contador CRC 1SP174937/O-0
CPF: 036.401.708-22

PODER JUDICIÁRIO

TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO

CERTIDÃO ESTADUAL DE DISTRIBUIÇÕES CÍVEIS

CERTIDÃO Nº: 7954265 **FOLHA: 1/1**

A autenticidade desta certidão poderá ser confirmada pela internet no site do Tribunal de Justiça.

A Diretoria de Serviço Técnico de Informações Cíveis do(a) Comarca de São Paulo - Capital, no uso de suas atribuições legais,

CERTIFICA E DÁ FÉ que, pesquisando os registros de distribuições de **PEDIDOS DE FALÊNCIA, CONCORDATAS, RECUPERAÇÕES JUDICIAIS E EXTRAJUDICIAIS**, anteriores a 29/01/2026, verificou **NADA CONSTAR** como réu/requerido/interessado em nome de: **********

CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ: 02.092.332/0001-79, conforme indicação constante do pedido de certidão.**********

Esta certidão não aponta ordinariamente os processos em que a pessoa cujo nome foi pesquisado figura como autor (a). São apontados os feitos com situação em tramitação já cadastrados no sistema SAJ referentes a todas as Comarcas/Foros Regionais e Distritais do Estado de São Paulo.

A data de informatização de cada Comarca/Foro pode ser verificada no Comunicado SPI nº 22/2019.

Esta certidão considera os feitos distribuídos na 1ª Instância, mesmo que estejam em Grau de Recurso.

Não existe conexão com qualquer outra base de dados de instituição pública ou com a Receita Federal que verifique a identidade do NOME/RAZÃO SOCIAL com o CPF/CNPJ. A conferência dos dados pessoais fornecidos pelo pesquisado é de responsabilidade exclusiva do destinatário da certidão.

A certidão em nome de pessoa jurídica considera os processos referentes à matriz e às filiais e poderá apontar feitos de homônimos não qualificados com tipos empresariais diferentes do nome indicado na certidão (EIRELI, S/C, S/S, EPP, ME, MEI, LTDA).

Necessário complementar com a certidão Comarcas e Turmas Recursais (Primeiro Grau) Cível.

Esta certidão só tem validade mediante assinatura digital.

Esta certidão é sem custas.

São Paulo, 30 de janeiro de 2026.

PEDIDO N°: ***0093642537***

PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO ESTADO DO ESPÍRITO SANTO
R. Des. Homero Mafra, 60 Enseada do Suá, Vitória - ES | CEP: 29.050-275 | Tel: (27) 3334-2000.

CERTIDÃO NEGATIVA DE PRIMEIRA INSTÂNCIA
NATUREZA CÍVEL

Dados da Certidão

Razão Social: CLM SOFTWARE COM IMP E EXP LTDA

CNPJ:	02.092.332/0003-30		
Data de Expedição:	16/01/2026 09:16:10	**Validade:**	30 DIAS
N° da Certidão:	**** 2025549581 ****		
-- ENDEREÇO --			
Município:	SERRA	**Bairro:**	TAQUARA II
Logradouro:	RUA SAMUEL MEIRA BRASIL	**Número:**	394
Complemento:	SALA 29	**CEP:**	*- NÃO INFORMADO -*
-- CONTATO --			
Email:	PUBLIC.SECTOR@CLM.TECH	**Telefone Fixo:**	*- NÃO INFORMADO -*
		Telefone Celular:	*- NÃO INFORMADO -*

CERTIFICA que, consultando a base de dados do Sistema de Gerenciamento de Processos do Poder Judiciário do Estado do Espírito Santo (E-Jud, SIEP, PROJUDI e PJe) até a presente data e hora, **NADA CONSTA** contra o solicitante .

Observações

a. Certidão expedida gratuitamente através da Internet;
b. Os dados do(a) solicitante acima informados são de sua responsabilidade, devendo a titularidade ser conferida pelo interessado e/ou destinatário;
c. O prazo de validade desta certidão é de 30 (trinta) dias, contados da data da expedição, conforme disposto no art. 467 do Código de Normas da Corregedoria Geral da Justiça. Após essa data será necessária a emissão de uma nova certidão;
d. A autenticidade desta certidão poderá ser confirmada na página do Tribunal de Justiça do Estado do Espírito Santo - www.tjes.jus.br -, utilizando o número da certidão acima identificado;
e. Em relação as comarcas da entrância especial (Vitória/Vila Velha/Cariacica/Serra/Viana), as ações de: execução fiscal estadual, falência e recuperação judicial, e auditoria militar, tramitam, apenas, no juízo de Vitória;
f. As ações de natureza cível abrangem inclusive aquelas que tramitam nas varas de Órfãos e Sucessões (Tutela, Curatela, Interdição,...), Juizado Especial Cível, Juizado Especial da Fazenda Pública, Execução Fiscal e Execução Patrimonial (observado o item **e**);
g. As ações de natureza criminal abrangem, dentre outras: as de auditoria militar e de juizados especiais criminais;
h. As matérias atinentes as varas de família e infância e juventude são objeto de certidão específica;
i. A base de dados do sistema de gerenciamento processual (1ª INSTÂNCIA: eJUD, SIEP, PROJUDI, PJe-1G; 2ª INSTÂNCIA: Sistema de Segunda Instância, PJe-2G) contém o registro de todos os processos distribuídos no Judiciário do Estado do Espírito Santo, com exceção do SEEU;
j. A certidão negativa referente ao Sistema Eletrônico de Execução Unificado – SEEU deverá ser requerida ao Cartório do Ofício de Distribuidor da Comarca, conforme Ato Normativo Conjunto n°. 009/2021.

PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO ESTADO DO ESPÍRITO SANTO
R. Des. Homero Mafra, 60 Enseada do Suá, Vitória - ES | CEP: 29.050-275 | Tel: (27) 3334-2000.

CERTIDÃO NEGATIVA DE PRIMEIRA INSTÂNCIA
NATUREZA DE RECUPERAÇÃO JUDICIAL E EXTRAJUDICIAL (FALÊNCIA E CONCORDATA)

Dados da Certidão

Razão Social: CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA.

CNPJ:	02.092.332/0003-30		
Data de Expedição:	09/01/2026 10:39:00	**Validade:**	30 DIAS
N° da Certidão:	**** 2025518167 ****		
-- ENDEREÇO --			
Município:	SERRA	**Bairro:**	TAQUARA II
Logradouro:	R SAMUEL MEIRA BRASIL	**Número:**	394
Complemento:	SALA 29.SERRA PARQ LOGIS CONJ CB5	**CEP:**	29.167-650
-- CONTATO --			
Email:	RECEBIMENTOFISCAL@CLM.TECH	**Telefone Fixo:**	(11) 2125-6270
		Telefone Celular:	*- NÃO INFORMADO -*

CERTIFICA que, consultando a base de dados do Sistema de Gerenciamento de Processos do Poder Judiciário do Estado do Espírito Santo (E-Jud, SIEP, PROJUDI e PJe) até a presente data e hora, **NADA CONSTA** contra o solicitante .

Observações

a. Certidão expedida gratuitamente através da Internet;
b. Os dados do(a) solicitante acima informados são de sua responsabilidade, devendo a titularidade ser conferida pelo interessado e/ou destinatário;
c. O prazo de validade desta certidão é de 30 (trinta) dias, contados da data da expedição, conforme disposto no art. 467 do Código de Normas da Corregedoria Geral da Justiça. Após essa data será necessária a emissão de uma nova certidão;
d. A autenticidade desta certidão poderá ser confirmada na página do Tribunal de Justiça do Estado do Espírito Santo - www.tjes.jus.br -, utilizando o número da certidão acima identificado;
e. Em relação as comarcas da entrância especial (Vitória/Vila Velha/Cariacica/Serra/Viana), as ações de: execução fiscal estadual, falência e recuperação judicial, e auditoria militar, tramitam, apenas, no juízo de Vitória;
f. As ações de natureza cível abrangem inclusive aquelas que tramitam nas varas de Órfãos e Sucessões (Tutela, Curatela, Interdição,...), Juizado Especial Cível, Juizado Especial da Fazenda Pública, Execução Fiscal e Execução Patrimonial (observado o item **e**);
g. As ações de natureza criminal abrangem, dentre outras: as de auditoria militar e de juizados especiais criminais;
h. As matérias atinentes as varas de família e infância e juventude são objeto de certidão específica;
i. A base de dados do sistema de gerenciamento processual (1ª INSTÂNCIA: eJUD, SIEP, PROJUDI, PJe-1G; 2ª INSTÂNCIA: Sistema de Segunda Instância, PJe-2G) contém o registro de todos os processos distribuídos no Judiciário do Estado do Espírito Santo, com exceção do SEEU;
j. A certidão negativa referente ao Sistema Eletrônico de Execução Unificado – SEEU deverá ser requerida ao Cartório do Ofício de Distribuidor da Comarca, conforme Ato Normativo Conjunto n°. 009/2021.

Documento(s) HABILITAÇÃO_CLM SOFTWARE (2060318) SEI 2025.0075627 pg. 3579

Ao
MPAM
P.E 94.001/2026

DECLARAÇÃO DE CUMPRIMENTO DO DISPOSTO NO INCISO XXXIII DO ART. 7º DA CONSTITUIÇÃO FEDERAL

A empresa **CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA,** pessoa jurídica de direito privado, inscrita no CNPJ sob nº 02.092.332/0003-30, com sede na Rua Samuel Meira, nº 394, sala 29, Bairro Taquara II, Serra/ES, CEP 29167-650, por intermédio de sua representante legal, o Sra. Tatiana Monteiro Montroze , brasileira, casada, portador da cédula de identidade nº 40.183.211-9 SSP/SP, inscrito no CPF/MF sob o nº 354.042.638-81, **DECLARA**, para fins do disposto no inciso V do art 27 da Lei nº 8.666, de 21 de junho de 1993, acrescido pela Lei nº 9.854, de 27 de outubro de 1999, que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos.
Ressalva: emprega menor, a partir de quatorze anos, na condição de aprendiz (x).

Serra (ES), 19 de janeiro de 2026.

gov.br
Documento assinado digitalmente
TATIANA MONTEIRO MONTROZE
Data: 16/01/2026 08:44:28-0300
Verifique em https://validar.iti.gov.br

CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA
Tatiana Monteiro Montroze
RG: 40.183.211-9
CPF: 354.042.638-81

Sistema de Cadastramento Unificado de Fornecedores - SICAF

Declaração

Declaramos para os fins exigidos na legislação, conforme documentação registrada no SICAF, que a situação do fornecedor no momento é a seguinte:

Dados do Fornecedor

CNPJ:	**02.092.332/0003-30**	DUNS®:	**893836225**
Razão Social:	**CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA.**		
Nome Fantasia:			
Situação do Fornecedor:	**Credenciado**	Data de Vencimento do Cadastro:	**13/10/2026**
Natureza Jurídica:	**SOCIEDADE EMPRESÁRIA LIMITADA**		
MEI:	**Não**		
Porte da Empresa:	**Demais**		

Ocorrências e Impedimentos

Ocorrência:	**Nada Consta**
Impedimento de Licitar:	**Nada Consta**
Ocorrências Impeditivas indiretas:	**Nada Consta**
Vínculo com "Serviço Público":	**Nada Consta**

Níveis cadastrados:

Automática: a certidão foi obtida através de integração direta com o sistema emissor. Manual: a certidão foi inserida manualmente pelo fornecedor.

I - Credenciamento

II - Habilitação Juridica

III - Regularidade Fiscal e Trabalhista Federal

Receita Federal e PGFN		Validade:	**07/07/2026**	**Automática**
FGTS		Validade:	**06/02/2026**	**Automática**
Trabalhista	**(http://www.tst.jus.br/certidao)**	Validade:	**07/07/2026**	**Automática**

IV - Regularidade Fiscal Estadual/Distrital e Municipal

Receita Estadual/Distrital	Validade:	**03/02/2026**
Receita Municipal	Validade:	**08/03/2026**

VI - Qualificação Econômico-Financeira

	Validade:	**30/06/2026**

TRIBUNAL DE CONTAS DA UNIÃO

Consulta Consolidada de Pessoa Jurídica

Este relatório tem por objetivo apresentar os resultados consolidados de consultas eletrônicas realizadas diretamente nos bancos de dados dos respectivos cadastros. A responsabilidade pela veracidade do resultado da consulta é do Órgão gestor de cada cadastro consultado. A informação relativa à razão social da Pessoa Jurídica é extraída do Cadastro Nacional da Pessoa Jurídica, mantido pela Receita Federal do Brasil.

Consulta realizada em: 30/01/2026 15:48:03

Informações da Pessoa Jurídica:

Razão Social: **CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA.**
CNPJ: **02.092.332/0003-30**

Resultados da Consulta Eletrônica:

Órgão Gestor: **TCU**
Cadastro: **Licitantes Inidôneos**
Resultado da consulta: **Nada Consta**

Para acessar a certidão original no portal do órgão gestor, clique AQUI.

Órgão Gestor: **CNJ**
Cadastro: **CNIA - Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade**
Resultado da consulta: **Nada Consta**

Para acessar a certidão original no portal do órgão gestor, clique AQUI.

Órgão Gestor: **Portal da Transparência**
Cadastro: **Cadastro Nacional de Empresas Inidôneas e Suspensas**
Resultado da consulta: **Nada Consta**

Para acessar a certidão original no portal do órgão gestor, clique AQUI.

Órgão Gestor: **Portal da Transparência**
Cadastro: **CNEP - Cadastro Nacional de Empresas Punidas**
Resultado da consulta: **Nada Consta**

Para acessar a certidão original no portal do órgão gestor, clique AQUI.

Obs: A consulta consolidada de pessoa jurídica visa atender aos princípios de simplificação e racionalização de serviços públicos digitais. Fundamento legal: Lei nº 12.965, de 23 de abril de 2014, Lei nº 13.460, de 26 de junho de 2017, Lei nº 13.726, de 8 de outubro de 2018, Decreto nº 8.638 de 15, de janeiro de 2016.

1. RELATÓRIO DE DECLARAÇÕES

i. Condições de participação

Manifesto ciência em relação ao inteiro teor do ato convocatório e dos seus anexos, concordo com suas condições, respondendo pela veracidade das informações prestadas, na forma da lei.

Declaro que minha proposta econômica compreenderá a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal de 1988, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data da sua entrega em definitivo.

ii. Declarações para fins de habilitação

Atendo aos requisitos de habilitação previstos em lei e no instrumento convocatório.

Inexiste impedimento à minha habilitação e comunicarei a superveniência de ocorrência impeditiva ao órgão ou entidade contratante.

Cumpro as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas, quando cabíveis.

Manifesto ciência em relação a todas as informações e condições locais para o cumprimento das obrigações objeto da licitação.

Cumpro o disposto no inciso XXXIII do art. 7º da Constituição Federal de 1988, que proíbe o trabalho noturno, perigoso ou insalubre a menores de dezoito e de qualquer trabalho a menores de dezesseis anos, salvo na condição de aprendiz, a partir de quatorze anos.

iii. Declarações de cumprimento à legislação trabalhista

Observo os incisos III e IV do art. 1º e cumpro o disposto no inciso III do art. 5º, todos da Constituição Federal de 1988, que veda o tratamento desumano ou degradante.

Cumpro a reserva de cargos prevista em lei para aprendiz, bem como as reservas de cargos previstas em outras normas específicas, quando cabíveis.

iv. Profissionais organizados sob a forma de cooperativa (1)

Participo da licitação sob a forma de cooperativa, que atende ao disposto no art. 16 da Lei n.º 14.133, de 1º de abril de 2021.

(1) Declaração válida apenas para cooperativas

v. Relação de fornecedores que declararam que cumprem e estão cientes de todas as declarações acima:

Fornecedor	Data declaração	Outras declarações (2)
02.092.332/0003-30 - CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. Porte Empresa: Grande Empresa	16/01/2026 14:59	Tratamento diferenciado ME/EPP: Não Equidade de Gênero: Bronze Programa de Integridade: Sim
39.532.571/0001-02 - GIUSEPPE ANTONIO FOGACA GERBALDO Porte Empresa: ME ou EPP	05/01/2026 10:52	Tratamento diferenciado ME/EPP: Sim Equidade de Gênero: Nenhum Programa de Integridade: Não

Declarações referentes ao art. 3ª da lei complementar nª 123/2006, no Decreto nª 11.430/2023 e no Decreto nª 12.304/2024 respectivamente

Copyright Compras.gov.br

PROCURADORIA GERAL DE JUSTIÇA

TERMO DE JULGAMENTO

UASG 925849 - PROCURADORIA GERAL DE JUSTIÇA - AM

PREGÃO 94001/2026

Fundamentação legal:	Lei 14.133/2021	Característica:	SISPP - Tradicional
Critério de julgamento:	Menor Preço / Maior Desconto	Modo de disputa:	Aberto
Compra emergencial:	Não	UF da UASG:	AM
Objeto da compra:	Contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses.		
Entrega de propostas:	De 05/01/2026 às 08:00 até 19/01/2026 às 10:00		
Abertura da sessão pública:	Dia 19/01/2026 às 10:00 (horário de Brasília)		

Mensagens do chat da compra

Responsável	Data/Hora	Mensagem
Sistema	19/01/2026 às 10:00:06	A sessão pública está aberta. Até 20 itens poderão estar em disputa simultaneamente e o período de abertura para disputa será entre 08:00 e 18:00. Haverá aviso prévio de abertura dos itens de 10 minutos. Mantenham-se conectados.
Sistema	19/01/2026 às 10:05:55	Bom dia, senhores!
Sistema	19/01/2026 às 10:06:25	Estamos iniciando a sessão pública do pregão eletrônico n.ª 94.001/2026-CPL/MP/PGJ, promovido pelo Ministério Público do Estado do Amazonas/Procuradoria-Geral de Justiça do Amazonas. Antes de iniciar a fase competitiva, peço a atenção de todos para alguns breves avisos a respeito da presente licitação.
Sistema	19/01/2026 às 10:07:12	Senhores, o Pregão Eletrônico n.ª 94.001/2026-CPL/MP/PGJ tem por objeto a contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses.
Sistema	19/01/2026 às 10:07:40	A licitação será pelo MENOR PREÇO GLOBAL.
Sistema	19/01/2026 às 10:09:07	A especificação técnica dos produtos consta do Termo de Referência Nª 28.2025.DTIC.2002143.2025.007562 (Anexo I do Edital).
Sistema	19/01/2026 às 10:10:19	O envio de lances, sejam eles intermediários ou destinados a cobrir a melhor oferta, devem respeitar o intervalo mínimo de R$ 10,00 (dez reais).de modo que as ofertas em desacordo com este critério não serão processadas pelo sistema (item 8.8 do Edital).
Sistema	19/01/2026 às 10:10:41	É importante destacar que o licitante é responsável por todas as transações efetuadas em seu nome, especialmente o cadastramento de proposta e o oferecimento de lances, ainda que o acesso ao sistema seja realizado por terceiros.
Sistema	19/01/2026 às 10:13:59	Prezados, os valores ofertados ainda estão acima do valor estimado pela Administração.
Sistema	19/01/2026 às 10:30:43	A etapa de julgamento de propostas foi iniciada. Para acompanhá-la acesse a opção "Seleção de fornecedores" na linha do tempo.
Sistema	19/01/2026 às 10:31:52	Senhores, encerrada a fase de lances, passemos à fase de julgamento das propostas.

Termo de JULGAMENTO_PE 94001/2026_Compras.gov (2060330) SEI 2025.007562 / pg. 3584

Responsável	Data/Hora	Mensagem
Sistema	19/01/2026 às 10:33:55	Assim, o licitante mais bem classificado na fase de lances será convocado, nos termos dos itens 9 e 10 do instrumento convocatório, a encaminhar, por meio do Sistema, sua proposta e os documentos complementares, no prazo de 02 (duas) horas.
Sistema	19/01/2026 às 10:50:45	Senhores, em verificação preliminar, a equipe de apoio constatou que alguns itens apresentam valores superiores ao estimado pela Administração.
Sistema	19/01/2026 às 10:50:51	Portanto, será aberta a etapa de negociação, previamente à solicitação da proposta formal.
Sistema	19/01/2026 às 11:38:28	Senhor, nesses valores a empresa está considerando o preço unitário do item?
Sistema	19/01/2026 às 14:43:39	Boa tarde, senhores. Em instantes, retomaremos os trabalhos.
Sistema	19/01/2026 às 15:02:26	Senhores, dando prosseguimento ao certame, uma vez concluída a negociação dos valores de determinados itens, a empresa será convocada, nos termos dos itens 9 e 10 do instrumento convocatório, a encaminhar, por meio do Sistema Compras.gov, a proposta e os respectivos documentos complementares, no prazo de 02 (duas) horas.
Sistema	19/01/2026 às 15:08:19	Senhores, a sessão fica suspensa, sem prejuízo do atendimento ao prazo de convocação. A reabertura ocorrerá amanhã, dia 20/01/2026, às 10h30.
Sistema	20/01/2026 às 10:36:02	Bom dia, senhores!
Sistema	20/01/2026 às 10:56:39	Senhores, verificado o atendimento, pela empresa CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA., inscrita no CNPJ nª 02.092.332/0003-30, à convocação realizada, os documentos apresentados serão encaminhados para análise técnica pela equipe da Diretoria de Tecnologia da Informação e Comunicação - DTIC, nos termos do item 10.2 do Edital.
Sistema	20/01/2026 às 13:09:51	Senhores, considerando que a proposta encontra-se em análise pela equipe técnica, ficam encerrados os trabalhos na presente data. A reabertura da sessão será oportunamente informada por meio do chat, com antecedência mínima de 24 (vinte e quatro) horas.
Sistema	27/01/2026 às 09:38:25	Bom dia, Senhores! Informo que a reabertura da sessão está agendada para amanhã, 28/01/2026, às 10h30.
Sistema	28/01/2026 às 10:28:13	Bom dia, senhores! Em instantes, retomaremos os trabalhos.
Sistema	28/01/2026 às 12:05:57	Senhores, em razão de compromisso institucional, a reabertura da sessão fica adiada para hoje, às 14h. Agradeço a todos pela compreensão.
Sistema	28/01/2026 às 14:06:22	Senhores, boa tarde! Como providência anterior, a proposta apresentada pela empresa CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA., inscrita no CNPJ (MF) nª 02.092.332/0003-30, foi encaminhada à Diretoria de Tecnologia da Informação e Comunicação - DTIC para análise técnica e manifestação conclusiva.
Sistema	28/01/2026 às 14:06:43	Em resposta, conforme consignado no Parecer nª 5.2026.DTIC.2050482.2025.007562, a unidade técnica concluiu que, após análise individualizada dos itens constantes do Termo de Referência, a proposta apresentada atende integralmente às exigências técnicas estabelecidas, não tendo sido identificadas não conformidades, sejam sanáveis ou insanáveis.
Sistema	28/01/2026 às 14:07:13	Assim, a proposta foi considerada tecnicamente compatível com o objeto licitado, encontrando-se apta ao prosseguimento do certame, motivo pelo qual a equipe técnica opinou pela sua aceitação.
Sistema	28/01/2026 às 14:07:22	A íntegra do referido parecer encontra-se disponível para consulta na página eletrônica de acompanhamento deste certame, por meio do seguinte link:
Sistema	28/01/2026 às 14:07:29	https://www.mpam.mp.br/licitacoes/licitacoes-em-andamento?view=article&id=31037:pe-94-001-2026-cpl-mp-pgj-contratacao-de-empresa-especializada-para-fornecimento-de-solucao-de-datacenter&catid=47
Sistema	28/01/2026 às 14:31:07	Diante do exposto, e considerando o atendimento às exigências do instrumento convocatório, decido aceitar a proposta apresentada pela empresa CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA., CNPJ (MF) nª 02.092.332/0003-30.
Sistema	28/01/2026 às 14:33:12	Dando prosseguimento ao certame, passa-se à fase de verificação das condições de habilitação da empresa CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA., CNPJ (MF) nª 02.092.332/0003-30.

Termo de JULGAMENTO_PE 94001/2026_Compras.gov (2060330) SEI 2025.007562 / pg. 3585

Responsável	Data/Hora	Mensagem
Sistema	28/01/2026 às 16:22:32	Senhores, considerando a necessidade de análise detalhada dos documentos de habilitação apresentados pela empresa CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA., CNPJ (MF) nª 02.092.332/0003-30, a sessão será suspensa para realização da respectiva verificação. A reabertura da sessão fica designada para o dia 30/01/2026, sexta-feira, às 11h.
Sistema	30/01/2026 às 10:56:15	Bom dia, senhores!
Sistema	30/01/2026 às 11:01:19	Senhores, informo que a equipe de apoio encontra-se em fase de conclusão da conferência e convalidação das certidões apresentadas pela empresa.
Sistema	30/01/2026 às 13:10:55	Senhores, informo que, a partir de 14h30, será divulgado o resultado da análise dos documentos de habilitação da empresa.
Sistema	30/01/2026 às 14:56:29	Boa tarde, senhores!
Sistema	30/01/2026 às 15:29:35	Senhores, dando prosseguimento ao certame, destaco que a documentação de habilitação da empresa CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA., inscrita no CNPJ (MF) nª 02.092.332/0003-30, também foi encaminhada à Diretoria de Tecnologia da Informação e Comunicação – DTIC para análise técnica e manifestação.
Sistema	30/01/2026 às 15:37:07	Em resposta, conforme consignado no Parecer nª 6.2026.DTIC.2054079.2025.007562, a unidade técnica concluiu que a declaração de pessoal técnico, instalações e aparelhamento atende, formal e materialmente, ao item 3.2.2 do Termo de Referência, bem como que a empresa CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA. comprovou satisfatoriamente sua capacitação técnico-operacional, atendendo integralmente às exigências estabelecidas no TR.
Sistema	30/01/2026 às 15:37:16	A íntegra do referido parecer encontra-se disponível para consulta na página eletrônica de acompanhamento deste certame, por meio do seguinte link:
Sistema	30/01/2026 às 15:37:30	https://www.mpam.mp.br/licitacoes/licitacoes-em-andamento?view=article&id=31037:pe-94-001-2026-cpl-mp-pgj-contratacao-de-empresa-especializada-para-fornecimento-de-solucao-de-datacenter&catid=47
Sistema	30/01/2026 às 15:43:21	Senhores, informo que foi verificada, por meio do SICAF, a autenticidade das certidões fiscais apresentadas, bem como a certidão de inexistência de ações de falência ou recuperação judicial junto ao Tribunal de Justiça do domicílio da licitante, não tendo sido identificadas inconsistências, inclusive quanto à situação falimentar da matriz.
Sistema	30/01/2026 às 15:43:33	Da mesma forma, procedeu-se à verificação dos demais documentos de habilitação apresentados pela interessada, cuja autenticidade foi validada por meio eletrônico.
Sistema	30/01/2026 às 15:43:49	Ressalte-se que a equipe de apoio deste certame utilizou as informações disponíveis no SICAF para complementar a análise documental da empresa CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA, procedendo às devidas verificações de autenticidade e regularidade por meio daquele sistema.
Sistema	30/01/2026 às 15:43:59	Na sequência, procedeu-se à verificação da situação da licitante quanto à inexistência de sanções aplicadas pela Administração Pública, mediante consulta ao SICAF (Compras.gov.br), à Relação de Empresas com Sanção Administrativa em Vigor, mantida pelo Tribunal de Contas do Estado do Amazonas – TCE/AM, bem como à Relação de Licitantes Inidôneos disponibilizada pelo Tribunal de Contas da União – TCU.
Sistema	30/01/2026 às 15:44:11	Igualmente, foram verificadas as condições da licitante quanto à regularidade perante a Lista de Empresas Suspensas/Impedidas da Comissão Geral de Licitação do Estado do Amazonas – CGL; o Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), da Controladoria-Geral da União – CGU; e o Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa (CNCIA), mantido pelo Conselho Nacional de Justiça – CNJ.
Sistema	30/01/2026 às 15:44:20	Ademais, foi realizada diligência junto à Relação de Pessoas Jurídicas impedidas de contratar com a Administração Pública, mantida pela Secretaria de Estado da Fazenda do Amazonas – SEFAZ-AM, não sendo constatado qualquer registro que indicasse restrição à contratação.
Sistema	30/01/2026 às 15:51:11	Oportunamente, registre-se que foi realizada consulta consolidada de pessoas jurídicas, a qual reúne, em um único ambiente, as seguintes bases: Relação de Licitantes Inidôneos do TCU; CNIA – Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade, do CNJ; Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS; e CNEP – Cadastro Nacional de Empresas Punidas

Termo de JULGAMENTO_PE 94001/2026_Compras.gov (2060330) SEI 2025.007562 / pg. 3586

Responsável	Data/Hora	Mensagem
Sistema	30/01/2026 às 15:51:39	Assim, será promovida a juntada da Consulta Consolidada de Pessoa Jurídica (TCU), bem como a Situação do Fornecedor (SICAF) da empresa CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA, CNPJ N.ª 02.092.332/0003-30, aos autos do procedimento interno desta Instituição.
Sistema	30/01/2026 às 15:51:59	O extrato do SICAF e a Consulta Consolidada de Pessoa Jurídica encontram-se disponíveis no seguinte endereço eletrônico:
Sistema	30/01/2026 às 15:52:03	https://www.mpam.mp.br/licitacoes/licitacoes-em-andamento?view=article&id=31037:pe-94-001-2026-cpl-mp-pgj-contratacao-de-empresa-especializada-para-fornecimento-de-solucao-de-datacenter&catid=47
Sistema	30/01/2026 às 15:55:24	Pelo exposto, concluída a análise dos documentos de habilitação, nos termos do item 11 do instrumento convocatório, verifica-se que a empresa CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA., CNPJ nª 02.092.332/0003-30, atendeu a todas as exigências editalícias, razão pela qual fica HABILITADA, com a respectiva habilitação promovida no sistema.
Sistema	30/01/2026 às 15:56:25	Agradeço a todos pela participação neste pregão eletrônico. Até a próxima oportunidade.

Eventos da compra

Data/Hora	Descrição
19/01/2026 às 10:00:06	Abertura da sessão pública
19/01/2026 às 10:30:43	Início da etapa de julgamento de propostas

Termo de JULGAMENTO_PE 94001/2026_Compras.gov (2060330) SEI 2025.007562 / pg. 3587

Grupo 1

Valor estimado: R$ 12.499.110,8600 (total)

Situação: Aguardando adjudicação

Tratamento Diferenciado ME/EPP: Sem benefícios ME/EPP (Art. 4ª, lei 14.133/2021)

Aceito e Habilitado por CPF ***.245.***-*2 - SARAH MADALENA BARBOSA CORTES DE MELO para CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, melhor lance: R$ 11.180.000,0000 (total), valor negociado: R$ 10.616.278,0000 (total)

Propostas do Grupo G1

Benefício Me/Epp: Conforme Art. 3ª da Lei Complementar nª 123, de 14 de dezembro de 2006
Equidade de gênero: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 11.430/2023
Programa de integridade: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 12.304/2024

Fornecedor	Valor ofertado	Situação
02.092.332/0003-30 - CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. Beneficio Me/Epp: Não Equidade de gênero: Bronze Programa de integridade: Sim UF endereço: ES	R$ 11.180.000,0000 (total)	Fornecedor habilitado
Valor proposta: R$ 12.960.776,0000 (total) Valor negociado: R$ 10.616.278,0000 (total)		
39.532.571/0001-02 - GIUSEPPE ANTONIO FOGACA GERBALDO Beneficio Me/Epp: Sim Equidade de gênero: Nenhum Programa de integridade: Não UF endereço: AM	R$ 99.000.000,0000 (total)	-
Valor proposta: R$ 214.000.000,0000 (total) Valor negociado: Não Realizado		

Mensagens do chat do Grupo G1

Responsável	Data/Hora	Mensagem
Sistema	19/01/2026 às 10:00:07	A abertura do item G1 para lances está agendada para daqui a 10 minutos. Mantenham-se conectados.
Sistema	19/01/2026 às 10:10:07	O item G1 foi aberto. Solicitamos o envio de lances.
Sistema	19/01/2026 às 10:26:49	O item G1 está aguardando decisão de reinício ou encerramento da etapa aberta pelo comprador.
Sistema	19/01/2026 às 10:30:38	O item G1 está encerrado.
Sistema para o participante 02.092.332/0003-30	19/01/2026 às 10:52:51	Bom dia, senhor. Solicito a reavaliação dos preços dos itens 1, 2, 4, 5 e 9 e a indicação de eventual possibilidade de negociação.
Pelo participante 02.092.332/0003-30	19/01/2026 às 10:54:35	Bom dia!

Termo de JULGAMENTO_PE 94001/2026_Compras.gov (2060330) SEI 2025.007562 / pg. 3588

Responsável	Data/Hora	Mensagem
Pelo participante 02.092.332/0003-30	19/01/2026 às 10:55:28	Sr. Pregoeiro, peço 15 minutos para avaliação interna de aplicação de desconto nos itens mencionados.
Sistema para o participante 02.092.332/0003-30	19/01/2026 às 11:01:38	Certamente. Permanecemos no aguardo.
Pelo participante 02.092.332/0003-30	19/01/2026 às 11:06:40	Sr. Após análise interna, informamos que foi possível aplicar os seguintes valores unitários para os itens solicitados:
Pelo participante 02.092.332/0003-30	19/01/2026 às 11:08:18	Item 1: R$ 608.000,00 - Item 2: R$ 838.000,00 - Item 4: R$ 185.000,00 - Item 5: R$ 10.190,00 - Item 9: R$ 430.000,00
Sistema para o participante 02.092.332/0003-30	19/01/2026 às 11:39:26	Senhor, nesses valores a empresa está considerando o preço unitário do item?
Pelo participante 02.092.332/0003-30	19/01/2026 às 11:39:52	informamos que foi possível aplicar os seguintes valores unitários dos itens solicitados
Pelo participante 02.092.332/0003-30	19/01/2026 às 11:41:26	Sim. Os valores informados referem-se ao preço unitário de cada item.
Sistema para o participante 02.092.332/0003-30	19/01/2026 às 11:45:47	Senhor, os preços estimados pela Administração para os itens em negociação são: Item 1 – R$ 588.062,67; Item 2 – R$ 832.942,67; Item 4 – R$ 164.252,40; Item 5 – R$ 9.250,98; Item 9 – R$ 262.143,66.
Sistema para o participante 02.092.332/0003-30	19/01/2026 às 11:47:27	Caso a empresa aceite esses preços, a negociação encontra-se aberta no sistema para registro dos novos valores.
Sistema para o participante 02.092.332/0003-30	19/01/2026 às 11:48:04	Sr. Fornecedor CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, você foi convocado para negociação de valor do item G1. Justificativa: Negociação via chat (limite: valor estimado pela Administração). .
Pelo participante 02.092.332/0003-30	19/01/2026 às 11:57:32	Solicitamos, por gentileza, a concessão de prazo para avaliação dos valores sugeridos junto ao fabricante. Considerando o horário de almoço, poderemos retornar com a avaliação até às 14h00?
Sistema para o participante 02.092.332/0003-30	19/01/2026 às 12:00:30	Considerando a sua solicitação, faremos um intervalo para almoço, com retorno programado para as 15h.
Pelo participante 02.092.332/0003-30	19/01/2026 às 12:01:20	obrigada
Pelo participante 02.092.332/0003-30	19/01/2026 às 14:25:40	O item G1 teve a negociação de valor encerrada pelo fornecedor CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30. A negociação do item G1 foi aceita pelo fornecedor CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, tendo informado R$ 10.616.278,0000.
Sistema para o participante 02.092.332/0003-30	19/01/2026 às 14:46:25	Senhor, agradeço a disponibilidade para negociação.
Sistema para o participante 02.092.332/0003-30	19/01/2026 às 15:03:42	Senhor, solicito, no prazo de 2 (duas) horas, a proposta ajustada aos valores negociados, acompanhada da documentação complementar, que será analisada pela equipe técnica desta Procuradoria-Geral de Justiça.
Sistema para o participante 02.092.332/0003-30	19/01/2026 às 15:04:07	Sr. Fornecedor CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, você foi convocado para enviar anexos para o item G1. Prazo para encerrar o envio: 17:05:00 do dia 19/01/2026. Justificativa: Proposta e documentos complementares. .
Pelo participante 02.092.332/0003-30	19/01/2026 às 15:32:21	O item G1 teve a convocação para envio de anexos encerrada às 15:32:21 de 19/01/2026. 5 anexos foram enviados pelo fornecedor CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30.
Pelo participante 02.092.332/0003-30	20/01/2026 às 10:55:27	Bom dia!

Termo de JULGAMENTO_PE 94001/2026_Compras.gov (2060330) SEI 2025.007562 / pg. 3589

Responsável	Data/Hora	Mensagem
Sistema	28/01/2026 às 14:32:02	O item G1 está na etapa de julgamento de proposta no período de intenção de recursos, com acréscimo de 10 minutos a partir de agora - até 28/01/2026 14:42:02.
Sistema	30/01/2026 às 15:56:42	O item G1 está na etapa de habilitação de fornecedores no período de intenção de recursos, com acréscimo de 10 minutos a partir de agora - até 30/01/2026 16:06:42.

Eventos do Grupo G1

Data/Hora	Descrição
19/01/2026 às 10:10:07	Item aberto para lances.
19/01/2026 às 10:26:49	Item aguardando decisão sobre reinício ou encerramento da etapa aberta.
19/01/2026 às 10:30:38	Item com etapa aberta encerrada.
19/01/2026 às 10:30:38	Item encerrado para lances.
19/01/2026 às 11:48:04	Fornecedor CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30 convocado para negociação de valor.
19/01/2026 às 14:25:40	Negociação encerrada. Fornecedor CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30 informou R$ 10.616.278,0000.
19/01/2026 às 15:04:07	Fornecedor CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30 convocado para o envio de anexo. Prazo para encerrar o envio: 17:05:00 do dia 19/01/2026. Justificativa: Proposta e documentos complementares. .
19/01/2026 às 15:32:21	Fornecedor CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30 finalizou o envio de anexo.
28/01/2026 às 14:32:02	Fornecedor CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30 teve a proposta aceita, melhor lance: R$ 11.180.000,0000, valor negociado: R$ 10.616.278,0000. Motivo: Parecer nª 5.2026.DTIC.2050482.2025.007562..
30/01/2026 às 15:56:42	Fornecedor CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30 foi habilitado.
30/01/2026 às 16:12:49	Encerramento da sessão 1 de julgamento / habilitação.

Item 1 do Grupo G1 - Outros Serviços de Gerenciamento de Infraestrutura De Tecnologia da Informação e

EQUIPAMENTO HIPERCONVERGENTE –PLATAFORMA NUTANIX G9.

A descrição completa do Item 1 deve ser verificada no Termo de Referência Nª 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Quantidade:	4	Valor estimado:	R$ 588.062,6700 (unitário)
Unidade de fornecimento:	UNIDADE		R$ 2.352.250,6800 (total)
Intervalo mínimo entre lances:	R$ 10,0000	Situação:	Aguardando adjudicação
Critério de julgamento:	Menor Preço		
Tratamento Diferenciado ME/EPP:	Sem benefícios ME/EPP (Art. 4ª, lei 14.133/2021)		

Aceito e Habilitado por CPF ***.245.***-*2 - SARAH MADALENA BARBOSA CORTES DE MELO para CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, melhor lance: R$ 610.000,0000 (unitário) / R$ 2.440.000,0000 (total), valor negociado: R$ 588.062,0000 (unitário) / R$ 2.352.248,0000 (total)

Propostas do Item 1

Benefício Me/Epp: Conforme Art. 3ª da Lei Complementar nª 123, de 14 de dezembro de 2006
Equidade de gênero: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 11.430/2023
Programa de integridade: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 12.304/2024

Termo de JULGAMENTO_PE 94001/2026_Compras.gov (2060330) SEI 2025.007562 / pg. 3590

Fornecedor	Valor ofertado	Situação
02.092.332/0003-30 - CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. Benefício Me/Epp: Não Equidade de gênero: Bronze Programa de integridade: Sim UF endereço: ES	R$ 610.000,0000 (unitário) R$ 2.440.000,0000 (total)	Fornecedor habilitado
Valor proposta: R$ 717.021,0000 (unitário) R$ 2.868.084,0000 (total)	Valor negociado: R$ 588.062,0000 (unitário) R$ 2.352.248,0000 (total)	Quantidade ofertada: 4
39.532.571/0001-02 - GIUSEPPE ANTONIO FOGACA GERBALDO Benefício Me/Epp: Sim Equidade de gênero: Nenhum Programa de integridade: Não UF endereço: AM	R$ 1.500.000,0000 (unitário) R$ 6.000.000,0000 (total)	-
Valor proposta: R$ 1.800.000,0000 (unitário) R$ 7.200.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 4

Lances do Item 1

Data/hora	Participante	Lance
19/01/2026 às 10:10:55	02.092.332/0003-30	R$ 717.000,0000
19/01/2026 às 10:15:38	02.092.332/0003-30	R$ 680.000,0000
19/01/2026 às 10:19:52	02.092.332/0003-30	R$ 650.000,0000
19/01/2026 às 10:20:57	39.532.571/0001-02	R$ 1.500.000,0000
19/01/2026 às 10:21:03	02.092.332/0003-30	R$ 630.000,0000
19/01/2026 às 10:24:48	02.092.332/0003-30	R$ 610.000,0000

Item 2 do Grupo G1 - Outros Serviços de Gerenciamento de Infraestrutura De Tecnologia da Informação e

EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU.

A descrição completa do Item 2 deve ser verificada no Termo de Referência Nª 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Quantidade:	1	Valor estimado:	R$ 832.942,6700 (unitário)
Unidade de fornecimento:	UNIDADE		R$ 832.942,6700 (total)
Intervalo mínimo entre lances:	R$ 10,0000	Situação:	Aguardando adjudicação
Critério de julgamento:	Menor Preço		
Tratamento Diferenciado ME/EPP:	Sem benefícios ME/EPP (Art. 4ª, lei 14.133/2021)		

Aceito e Habilitado por CPF ***.245.***-*2 - SARAH MADALENA BARBOSA CORTES DE MELO para CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, melhor lance: R$ 850.000,0000 (unitário) / R$ 850.000,0000 (total), valor negociado: R$ 832.942,0000 (unitário) / R$ 832.942,0000 (total)

Propostas do Item 2

Benefício Me/Epp: Conforme Art. 3ª da Lei Complementar nª 123, de 14 de dezembro de 2006
Equidade de gênero: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 11.430/2023
Programa de integridade: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 12.304/2024

Fornecedor	Valor ofertado	Situação

Termo de JULGAMENTO_PE 94001/2026_Compras.gov (2060330) SEI 2025.007562 / pg. 3591

Fornecedor	Valor ofertado	Situação
02.092.332/0003-30 - CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. Benefício Me/Epp: Não Equidade de gênero: Bronze Programa de integridade: Sim UF endereço: ES	R$ 850.000,0000 (unitário) R$ 850.000,0000 (total)	Fornecedor habilitado
Valor proposta: R$ 982.735,0000 (unitário) R$ 982.735,0000 (total)	Valor negociado: R$ 832.942,0000 (unitário) R$ 832.942,0000 (total)	Quantidade ofertada: 1
39.532.571/0001-02 - GIUSEPPE ANTONIO FOGACA GERBALDO Benefício Me/Epp: Sim Equidade de gênero: Nenhum Programa de integridade: Não UF endereço: AM	R$ 1.500.000,0000 (unitário) R$ 1.500.000,0000 (total)	-
Valor proposta: R$ 1.800.000,0000 (unitário) R$ 1.800.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1

Lances do Item 2

Data/hora	Participante	Lance
19/01/2026 às 10:12:01	02.092.332/0003-30	R$ 980.000,0000
19/01/2026 às 10:16:16	02.092.332/0003-30	R$ 920.000,0000
19/01/2026 às 10:21:04	39.532.571/0001-02	R$ 1.500.000,0000
19/01/2026 às 10:22:04	02.092.332/0003-30	R$ 870.000,0000
19/01/2026 às 10:24:06	02.092.332/0003-30	R$ 850.000,0000

Item 3 do Grupo G1 - Serviços de Gerenciamento de Sistemas Computacionais

SOFTWARE GESTÃO DAPLATAFORMA DE HIPERCONVERGENCIA NUTANIX.

A descrição completa do Item 3 deve ser verificada no Termo de Referência Nª 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Quantidade:	5	Valor estimado:	R$ 875.768,1500 (unitário)
Unidade de fornecimento:	UND SERVIÇO TÉCNICO		R$ 4.378.840,7500 (total)
Intervalo mínimo entre lances:	R$ 10,0000	Situação:	Aguardando adjudicação
Critério de julgamento:	Menor Preço		
Tratamento Diferenciado ME/EPP:	Sem benefícios ME/EPP (Art. 4ª, lei 14.133/2021)		

Aceito e Habilitado por CPF ***.245.***-*2 - SARAH MADALENA BARBOSA CORTES DE MELO para CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, melhor lance: R$ 790.000,0000 (unitário) / R$ 3.950.000,0000 (total)

Propostas do Item 3

Benefício Me/Epp: Conforme Art. 3ª da Lei Complementar nª 123, de 14 de dezembro de 2006
Equidade de gênero: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 11.430/2023
Programa de integridade: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 12.304/2024

Fornecedor	Valor ofertado	Situação

Termo de JULGAMENTO_PE 94001/2026_Compras.gov (2060330) SEI 2025.007562 / pg. 3592

Fornecedor	Valor ofertado	Situação
02.092.332/0003-30 - CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. Benefício Me/Epp: Não Equidade de gênero: Bronze Programa de integridade: Sim UF endereço: ES	R$ 790.000,0000 (unitário) R$ 3.950.000,0000 (total)	Fornecedor habilitado
Valor proposta: R$ 925.188,0000 (unitário) R$ 4.625.940,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 5
39.532.571/0001-02 - GIUSEPPE ANTONIO FOGACA GERBALDO Benefício Me/Epp: Sim Equidade de gênero: Nenhum Programa de integridade: Não UF endereço: AM	R$ 1.500.000,0000 (unitário) R$ 7.500.000,0000 (total)	-
Valor proposta: R$ 5.000.000,0000 (unitário) R$ 25.000.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 5

Lances do Item 3

Data/hora	Participante	Lance
19/01/2026 às 10:12:18	02.092.332/0003-30	R$ 900.000,0000
19/01/2026 às 10:15:08	02.092.332/0003-30	R$ 850.000,0000
19/01/2026 às 10:16:38	02.092.332/0003-30	R$ 820.000,0000
19/01/2026 às 10:19:33	02.092.332/0003-30	R$ 790.000,0000
19/01/2026 às 10:21:13	39.532.571/0001-02	R$ 1.500.000,0000

Item 4 do Grupo G1 - Serviços de Gerenciamento de Sistemas Computacionais

SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU.

A descrição completa do Item 4 deve ser verificada no Termo de Referência Nª 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Quantidade:	1	Valor estimado:	R$ 164.252,4000 (unitário)
Unidade de fornecimento:	UND SERVIÇO TÉCNICO		R$ 164.252,4000 (total)
Intervalo mínimo entre lances:	R$ 10,0000	Situação:	Aguardando adjudicação
Critério de julgamento:	Menor Preço		
Tratamento Diferenciado ME/EPP:	Sem benefícios ME/EPP (Art. 4ª, lei 14.133/2021)		

Aceito e Habilitado por CPF ***.245.***-*2 - SARAH MADALENA BARBOSA CORTES DE MELO para CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, melhor lance: R$ 190.000,0000 (unitário) / R$ 190.000,0000 (total), valor negociado: R$ 164.252,0000 (unitário) / R$ 164.252,0000 (total)

Propostas do Item 4

Benefício Me/Epp: Conforme Art. 3ª da Lei Complementar nª 123, de 14 de dezembro de 2006
Equidade de gênero: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 11.430/2023
Programa de integridade: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 12.304/2024

Fornecedor	Valor ofertado	Situação

Termo de JULGAMENTO_PE 94001/2026_Compras.gov (2060330) SEI 2025.007562 / pg. 3593

Fornecedor	Valor ofertado	Situação
02.092.332/0003-30 - CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. Benefício Me/Epp: Não Equidade de gênero: Bronze Programa de integridade: Sim UF endereço: ES	R$ 190.000,0000 (unitário) R$ 190.000,0000 (total)	Fornecedor habilitado
Valor proposta: R$ 217.972,0000 (unitário) R$ 217.972,0000 (total)	Valor negociado: R$ 164.252,0000 (unitário) R$ 164.252,0000 (total)	Quantidade ofertada: 1
39.532.571/0001-02 - GIUSEPPE ANTONIO FOGACA GERBALDO Benefício Me/Epp: Sim Equidade de gênero: Nenhum Programa de integridade: Não UF endereço: AM	R$ 1.500.000,0000 (unitário) R$ 1.500.000,0000 (total)	-
Valor proposta: R$ 5.000.000,0000 (unitário) R$ 5.000.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1

Lances do Item 4

Data/hora	Participante	Lance
19/01/2026 às 10:12:39	02.092.332/0003-30	R$ 200.000,0000
19/01/2026 às 10:20:15	02.092.332/0003-30	R$ 190.000,0000
19/01/2026 às 10:21:22	39.532.571/0001-02	R$ 1.500.000,0000

Item 5 do Grupo G1 - Serviços de Gerenciamento de Sistemas Computacionais

LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE.

A descrição completa do Item 5 deve ser verificada no Termo de Referência Nª 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Quantidade:	50	Valor estimado:	R$ 9.250,9800 (unitário)
Unidade de fornecimento:	UND SERVIÇO TÉCNICO		R$ 462.549,0000 (total)
Intervalo mínimo entre lances:	R$ 10,0000	Situação:	Aguardando adjudicação
Critério de julgamento:	Menor Preço		
Tratamento Diferenciado ME/EPP:	Sem benefícios ME/EPP (Art. 4ª, lei 14.133/2021)		

Aceito e Habilitado por CPF ***.245.***-*2 - SARAH MADALENA BARBOSA CORTES DE MELO para CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, melhor lance: R$ 11.000,0000 (unitário) / R$ 550.000,0000 (total), valor negociado: R$ 9.250,9800 (unitário) / R$ 462.549,0000 (total)

Propostas do Item 5

Benefício Me/Epp: Conforme Art. 3ª da Lei Complementar nª 123, de 14 de dezembro de 2006
Equidade de gênero: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 11.430/2023
Programa de integridade: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 12.304/2024

Fornecedor	Valor ofertado	Situação

Termo de JULGAMENTO_PE 94001/2026_Compras.gov (2060330) SEI 2025.007562 / pg. 3594

Fornecedor	Valor ofertado	Situação
02.092.332/0003-30 - CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. Benefício Me/Epp: Não Equidade de gênero: Bronze Programa de integridade: Sim UF endereço: ES	R$ 11.000,0000 (unitário) R$ 550.000,0000 (total)	Fornecedor habilitado
Valor proposta: R$ 12.336,0000 (unitário) R$ 616.800,0000 (total)	Valor negociado: R$ 9.250,9800 (unitário) R$ 462.549,0000 (total)	Quantidade ofertada: 50
39.532.571/0001-02 - GIUSEPPE ANTONIO FOGACA GERBALDO Benefício Me/Epp: Sim Equidade de gênero: Nenhum Programa de integridade: Não UF endereço: AM	R$ 1.500.000,0000 (unitário) R$ 75.000.000,0000 (total)	-
Valor proposta: R$ 3.000.000,0000 (unitário) R$ 150.000.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 50

Lances do Item 5

Data/hora	Participante	Lance
19/01/2026 às 10:12:59	02.092.332/0003-30	R$ 12.000,0000
19/01/2026 às 10:19:09	02.092.332/0003-30	R$ 11.500,0000
19/01/2026 às 10:21:29	39.532.571/0001-02	R$ 1.500.000,0000
19/01/2026 às 10:22:42	02.092.332/0003-30	R$ 11.000,0000

Item 6 do Grupo G1 - Serviços de Gerenciamento de Sistemas Computacionais

SOFTWARE DE BACKUP DE DADOS.

A descrição completa do Item 6 deve ser verificada no Termo de Referência Nª 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Quantidade:	1	Valor estimado:	R$ 2.005.354,2600 (unitário)
Unidade de fornecimento:	UND SERVIÇO TÉCNICO		R$ 2.005.354,2600 (total)
Intervalo mínimo entre lances:	R$ 10,0000	Situação:	Aguardando adjudicação
Critério de julgamento:	Menor Preço		
Tratamento Diferenciado ME/EPP:	Sem benefícios ME/EPP (Art. 4ª, lei 14.133/2021)		

Aceito e Habilitado por CPF ***.245.***-*2 - SARAH MADALENA BARBOSA CORTES DE MELO para CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, melhor lance: R$ 900.000,0000 (unitário) / R$ 900.000,0000 (total)

Propostas do Item 6

Benefício Me/Epp: Conforme Art. 3ª da Lei Complementar nª 123, de 14 de dezembro de 2006
Equidade de gênero: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 11.430/2023
Programa de integridade: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 12.304/2024

Fornecedor	Valor ofertado	Situação

Termo de JULGAMENTO_PE 94001/2026_Compras.gov (2060330) SEI 2025.007562 / pg. 3595

Fornecedor	Valor ofertado	Situação
02.092.332/0003-30 - CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. Benefício Me/Epp: Não Equidade de gênero: Bronze Programa de integridade: Sim UF endereço: ES	R$ 900.000,0000 (unitário) R$ 900.000,0000 (total)	Fornecedor habilitado
Valor proposta: R$ 994.639,0000 (unitário) R$ 994.639,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
39.532.571/0001-02 - GIUSEPPE ANTONIO FOGACA GERBALDO Benefício Me/Epp: Sim Equidade de gênero: Nenhum Programa de integridade: Não UF endereço: AM	R$ 1.500.000,0000 (unitário) R$ 1.500.000,0000 (total)	-
Valor proposta: R$ 5.000.000,0000 (unitário) R$ 5.000.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1

Lances do Item 6

Data/hora	Participante	Lance
19/01/2026 às 10:13:14	02.092.332/0003-30	R$ 950.000,0000
19/01/2026 às 10:17:16	02.092.332/0003-30	R$ 900.000,0000
19/01/2026 às 10:21:36	39.532.571/0001-02	R$ 1.500.000,0000

Item 7 do Grupo G1 - Outros Serviços de Gerenciamento de Infraestrutura De Tecnologia da Informação e

EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES.

A descrição completa do Item 7 deve ser verificada no Termo de Referência Nª 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Quantidade:	1	Valor estimado:	R$ 373.771,3800 (unitário)
Unidade de fornecimento:	UNIDADE		R$ 373.771,3800 (total)
Intervalo mínimo entre lances:	R$ 10,0000	Situação:	Aguardando adjudicação
Critério de julgamento:	Menor Preço		
Tratamento Diferenciado ME/EPP:	Sem benefícios ME/EPP (Art. 4ª, lei 14.133/2021)		

Aceito e Habilitado por CPF ***.245.***-*2 - SARAH MADALENA BARBOSA CORTES DE MELO para CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, melhor lance: R$ 230.000,0000 (unitário) / R$ 230.000,0000 (total)

Propostas do Item 7

Benefício Me/Epp: Conforme Art. 3ª da Lei Complementar nª 123, de 14 de dezembro de 2006
Equidade de gênero: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 11.430/2023
Programa de integridade: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 12.304/2024

Fornecedor	Valor ofertado	Situação

Termo de JULGAMENTO_PE 94001/2026_Compras.gov (2060330) SEI 2025.007562 / pg. 3596

Fornecedor	Valor ofertado	Situação
02.092.332/0003-30 - CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. Benefício Me/Epp: Não Equidade de gênero: Bronze Programa de integridade: Sim UF endereço: ES	R$ 230.000,0000 (unitário) R$ 230.000,0000 (total)	Fornecedor habilitado
Valor proposta: R$ 267.620,0000 (unitário) R$ 267.620,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
39.532.571/0001-02 - GIUSEPPE ANTONIO FOGACA GERBALDO Benefício Me/Epp: Sim Equidade de gênero: Nenhum Programa de integridade: Não UF endereço: AM	R$ 1.500.000,0000 (unitário) R$ 1.500.000,0000 (total)	-
Valor proposta: R$ 5.000.000,0000 (unitário) R$ 5.000.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1

Lances do Item 7

Data/hora	Participante	Lance
19/01/2026 às 10:13:28	02.092.332/0003-30	R$ 250.000,0000
19/01/2026 às 10:18:51	02.092.332/0003-30	R$ 230.000,0000
19/01/2026 às 10:21:43	39.532.571/0001-02	R$ 1.500.000,0000

Item 8 do Grupo G1 - Serviços de Gerenciamento de Sistemas Computacionais

SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES.

A descrição completa do Item 8 deve ser verificada no Termo de Referência Nª 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Quantidade:	1	Valor estimado:	R$ 1.404.862,4000 (unitário)
Unidade de fornecimento:	UND SERVIÇO TÉCNICO		R$ 1.404.862,4000 (total)
Intervalo mínimo entre lances:	R$ 10,0000	Situação:	Aguardando adjudicação
Critério de julgamento:	Menor Preço		
Tratamento Diferenciado ME/EPP:	Sem benefícios ME/EPP (Art. 4ª, lei 14.133/2021)		

Aceito e Habilitado por CPF ***.245.***-*2 - SARAH MADALENA BARBOSA CORTES DE MELO para CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, melhor lance: R$ 1.200.000,0000 (unitário) / R$ 1.200.000,0000 (total)

Propostas do Item 8

Benefício Me/Epp: Conforme Art. 3ª da Lei Complementar nª 123, de 14 de dezembro de 2006
Equidade de gênero: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 11.430/2023
Programa de integridade: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 12.304/2024

Fornecedor	Valor ofertado	Situação

Termo de JULGAMENTO_PE 94001/2026_Compras.gov (2060330) SEI 2025.007562 / pg. 3597

Fornecedor	Valor ofertado	Situação
02.092.332/0003-30 - CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. Benefício Me/Epp: Não Equidade de gênero: Bronze Programa de integridade: Sim UF endereço: ES	R$ 1.200.000,0000 (unitário) R$ 1.200.000,0000 (total)	Fornecedor habilitado
Valor proposta: R$ 1.355.400,0000 (unitário) R$ 1.355.400,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
39.532.571/0001-02 - GIUSEPPE ANTONIO FOGACA GERBALDO Benefício Me/Epp: Sim Equidade de gênero: Nenhum Programa de integridade: Não UF endereço: AM	R$ 1.500.000,0000 (unitário) R$ 1.500.000,0000 (total)	-
Valor proposta: R$ 5.000.000,0000 (unitário) R$ 5.000.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1

Lances do Item 8

Data/hora	Participante	Lance
19/01/2026 às 10:13:49	02.092.332/0003-30	R$ 1.300.000,0000
19/01/2026 às 10:17:41	02.092.332/0003-30	R$ 1.200.000,0000
19/01/2026 às 10:21:52	39.532.571/0001-02	R$ 1.500.000,0000

Item 9 do Grupo G1 - Switch

Switch Quantidade Portas: 48UN, Tipo Portas: Sfp28, Velocidade Porta: 25 Gb, Alimentação: 110/220V, Características Adicionais: 50 Cm De Cabo De Empilhamento, Tipo: Padrão Rack 19"

Quantidade:	2	Valor estimado:	R$ 262.143,6600 (unitário)
Unidade de fornecimento:	Unidade		R$ 524.287,3200 (total)
Intervalo mínimo entre lances:	R$ 10,0000	Situação:	Aguardando adjudicação
Critério de julgamento:	Menor Preço		
Tratamento Diferenciado ME/EPP:	Sem benefícios ME/EPP (Art. 4ª, lei 14.133/2021)		

Aceito e Habilitado por CPF ***.245.***-*2 - SARAH MADALENA BARBOSA CORTES DE MELO para CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, melhor lance: R$ 435.000,0000 (unitário) / R$ 870.000,0000 (total), valor negociado: R$ 262.143,5000 (unitário) / R$ 524.287,0000 (total)

Propostas do Item 9

Benefício Me/Epp: Conforme Art. 3ª da Lei Complementar nª 123, de 14 de dezembro de 2006
Equidade de gênero: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 11.430/2023
Programa de integridade: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 12.304/2024

Fornecedor	Valor ofertado	Situação

Termo de JULGAMENTO_PE 94001/2026_Compras.gov (2060330) SEI 2025.007562 / pg. 3598

Fornecedor	Valor ofertado	Situação
02.092.332/0003-30 - CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. Benefício Me/Epp: Não Equidade de gênero: Bronze Programa de integridade: Sim UF endereço: ES	R$ 435.000,0000 (unitário) R$ 870.000,0000 (total)	Fornecedor habilitado
Marca/Fabricante: JUNIPER Modelo/versão: QFX5120 Valor proposta: R$ 515.793,0000 (unitário) R$ 1.031.586,0000 (total) Valor negociado: R$ 262.143,5000 (unitário) R$ 524.287,0000 (total) Quantidade ofertada: 2		
39.532.571/0001-02 - GIUSEPPE ANTONIO FOGACA GERBALDO Benefício Me/Epp: Sim Equidade de gênero: Nenhum Programa de integridade: Não UF endereço: AM	R$ 1.500.000,0000 (unitário) R$ 3.000.000,0000 (total)	-
Marca/Fabricante: Switch Modelo/versão: Switch Valor proposta: R$ 5.000.000,0000 (unitário) R$ 10.000.000,0000 (total) Valor negociado: Não Realizado Quantidade ofertada: 2		

Lances do Item 9

Data/hora	Participante	Lance
19/01/2026 às 10:14:10	02.092.332/0003-30	R$ 512.000,0000
19/01/2026 às 10:18:06	02.092.332/0003-30	R$ 480.000,0000
19/01/2026 às 10:18:34	02.092.332/0003-30	R$ 450.000,0000
19/01/2026 às 10:22:02	39.532.571/0001-02	R$ 1.500.000,0000
19/01/2026 às 10:23:10	02.092.332/0003-30	R$ 435.000,0000

Termo de JULGAMENTO_PE 94001/2026_Compras.gov (2060330) SEI 2025.007562 / pg. 3599

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

RELATÓRIO DE LICITAÇÃO Nº 6.2026.CPL.2060332.2025.007562

RELATÓRIO CIRCUNSTANCIADO REFERENTE AO PREGÃO ELETRÔNICO N.º 94.001/2026-CPL/MP/PGJ

PROCESSO SEI N.º 2025.007562

Excelentíssimo Senhor Subprocurador-Geral de Justiça para Assuntos Administrativos,

A Pregoeira, Sra. **SARAH MADALENA BARBOSA CÔRTES DE MELO**, designada por força da PORTARIA N.º 66/2026/SUBADM, de 19/01/2026 (doc. 2048588), vem apresentar e submeter à apreciação de Vossa Excelência o **relatório circunstanciado** d o **Pregão Eletrônico n.º 94.001/2026-CPL/MP/PGJ**, tipo **MENOR PREÇO GLOBAL**, com modo de disputa "**ABERTO"**, concernente ao **Processo SEI N.º 2025.007562**, que tem por objeto a *contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma* ***solução de datacenter,*** *contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com* ***garantia de 60 (sessenta) meses****.*

1. DA EVOLUÇÃO DOS AUTOS

A evolução dos autos ocorreu conforme descrição e datas constantes n o **Histórico do Processo N.º 2025.007562**, disponível para consulta na rotina "Consultar Andamento".

2. DA PUBLICIDADE

O Aviso da Licitação foi publicado: no *Compras.gov*, em 30/12/2025, a fim de ser disponibilizado a partir do dia 05/01/2026 (doc. n.º 2038139), no matutino local "Jornal do Commercio", Edição n.º 44.459, de 3, 4 e 5/01/2026 (doc.

n.º 2038657); no Diário Oficial Eletrônico do Ministério Público do Estado do Amazonas – DOMPE, Edição n.º 3230, no dia 30/12/2025 (doc. n.º 2038649) e no sítio institucional do MPE/AM (www.mpam.mp.br).

3. DA SESSÃO PÚBLICA

3.1. Do Credenciamento – As licitantes credenciaram-se na Secretaria de Logística e Tecnologia de Informação – SLTI, do Ministério do Planejamento, Orçamento e Gestão, através das regras do sistema *Comprasnet*, no sítio eletrônico https://www.gov.br/compras/pt-br.

3.2. Da Proposta – As propostas foram enviadas pelos licitantes, através da internet, desde 05/01/2026 até a data e hora marcadas para a abertura da sessão, a saber, dia 19/01/2026, às 10h (horário de Brasília/DF).

3.3. Da Fase de Lances – Iniciada a disputa, o interessado, diante da informação divulgada pela Pregoeira de que o valor ofertado encontrava-se acima do preço estimado pela Administração, teve a oportunidade de apresentar, por meio de lances, condições mais favoráveis do que as inicialmente propostas, o que de fato ocorreu, encerrando-se a fase competitiva com a apresentação de proposta mais vantajosa para a Administração, conforme registrado no **Termo de Julgamento da Sessão** (doc. n.º 2060330).

3.4. Da Negociação e Aceitação da Proposta – Na sequência, a Pregoeira convocou a licitante para a fase de negociação, tendo em vista que os valores ofertados para determinados itens permaneceram acima dos estimados pela Administração. Concluídas com êxito as tratativas, a empresa **CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA (FILIAL)**, CNPJ N.º 02.092.332/0003-30, foi convocada a apresentar proposta ajustada aos valores negociados, acompanhada da documentação complementar exigida, para fins de posterior análise.

Considerando o cumprimento dos prazos estabelecidos, a observância dos requisitos formais exigidos por esta Instituição e a necessidade de análise técnica da proposta apresentada, os documentos foram encaminhados à **Diretoria de Tecnologia da Informação e Comunicação – DTIC**, para exame, nos termos do item 10.2 do Instrumento Convocatório.

Em resposta, por meio do **Parecer Nº 5.2026.DTIC.2050482.2025.007562**, a **Diretoria de Tecnologia da Informação e Comunicação – DTIC** manifestou-se nos seguintes termos, *in verbis*:

> **PARECER Nº 5.2026.DTIC.2050482.2025.007562**
>
> (...)
>
> **2.1 CONCLUSÃO TÉCNICA FINAL**
>
> Após análise individualizada de todos os itens constantes do Termo de Referência, verificou-se que a proposta

apresentada pela empresa **CLM Software Comércio Importação e Exportação Ltda.** atende integralmente às exigências técnicas estabelecidas, não sendo identificadas não conformidades, sejam elas sanáveis ou insanáveis.

Dessa forma, a proposta mostra-se tecnicamente compatível e aderente ao objeto licitado, encontrando-se apta ao prosseguimento do certame.

Diante do exposto, a equite técnica **OPINA** pela aceitação da proposta.

É o parecer.

Manaus, 22 de janeiro de 2026.

ANTOVLA FROTA BEZERRA JÚNIOR
Técnico em Computação

EUDO DE LIMA ASSIS JUNIOR
Diretor de Tecnologia da Informação e Comunicação

Assim, com base na manifestação da DTIC, a Pregoeira, com auxílio da equipe de apoio, procedeu à **aceitação** da seguinte proposta, conforme **Termo de Julgamento da Sessão** (doc. n.º 2060330):

- **CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA (FILIAL),** CNPJ N.º 02.092.332/0003-30 - valor total negociado de **R$ 10.616.278,00** (*dez milhões, seiscentos e dezesseis mil, duzentos e setenta e oito reais*) (docs. n.º 2050244, n.º 2050248 e n.º 2050251).

3.5. Da Habilitação – Dando regular prosseguimento ao feito, a Pregoeira e equipe de apoio passaram à verificação dos documentos de habilitação da empresa **CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA (FILIAL),** CNPJ N.º 02.092.332/0003-30.

Na oportunidade, registra-se que a **qualificação técnica** da empresa (doc. n.º 2052516), bem como DECLARAÇÃO DE INDICAÇÃO DE PESSOAL TÉCNICO, INSTALAÇÕES E APARELHAMENTO (doc. nº 2052494) foram submetidas ao crivo da Diretoria de Tecnologia da Informação e Comunicação – DTIC, a qual, por meio do **Parecer Nº 6.2026.DTIC.2054079.2025.007562, *opinou pela aceitação*** *da documentação de capacitação técnica apresentada pela licitante, por atender às exigências editalícias e demonstrar aptidão técnica compatível com o objeto licitado.*

Desta forma, procedeu-se ao julgamento das condições de habilitação da licitante, utilizando-se, inclusive, das informações do **Sistema de Cadastro de Fornecedores – SICAF** do Compras.gov, analisando-se, sobretudo, as condições da referida empresa quanto à inexistência de sanções impeditivas à contratação com a Administração Pública, conforme documentação n.º 2060318, n.º 2060322 e

n.º 2060326.

Nesse aspecto, verificou-se o relatório de sanções impeditivas pela Administração Pública, no SICAF do *Compras.gov*, bem como a Relação de Empresas com Sanção Administrativa em vigor, do **TRIBUNAL DE CONTAS DO ESTADO DO AMAZONAS – TCE**, a Relação de Licitantes Inidôneos do **TRIBUNAL DE CONTAS DA UNIÃO – TCU,** a Lista de Empresas Suspensas/Impedidas da **COMISSÃO GERAL DE LICITAÇÃO DO ESTADO DO AMAZONAS – CGL**, o Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), da **CONTROLADORIA GERAL DA UNIÃO – CGU**, o Cadastro Nacional de Condenações Civis por Ato de Improbidade Administrativa (CNCIA) do **CONSELHO NACIONAL DE JUSTIÇA – CNJ** e a Relação de pessoas jurídicas impedidas de contratar com a Administração Pública da **SEFAZ-AM, não** sendo constatados registros que indicassem restrições à contratação.

Cabe registrar que o **Tribunal de Contas da União** disponibiliza ferramenta que permite a consulta consolidada de pessoas jurídicas, que reúne, em relatório único, as Licitantes Inidôneos do TCU, CNIA - Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade do CNJ; Cadastro Nacional de Empresas Inidôneas e Suspensas e CNEP - Cadastro Nacional de Empresas Punidas ambos do Portal da Transparência. Assim, a Pregoeira promoveu a juntada aos presentes autos da **CONSULTA CONSOLIDADA DE PESSOA JURÍDICA** da empresa **CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA (FILIAL),** CNPJ N.º 02.092.332/0003-30 (doc. n.º 2060327)

Isto posto, concluída a análise dos documentos habilitatórios, conforme Item 11 do instrumento convocatório, procedeu-se à **HABILITAÇÃO** da licitante:

> - **CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA (FILIAL),** CNPJ N.º 02.092.332/0003-30 - valor total negociado de **R$ 10.616.278,00** (*dez milhões, seiscentos e dezesseis mil, duzentos e setenta e oito reais*) (Termo de Julgamento n.º 2060330).

4. DOS RECURSOS

Passo seguinte, ao encerrar a sessão pública, a Pregoeira observou que, concedido prazo legal para registro de intenção de recurso por parte das demais licitantes, não houve manifestação nesse sentido.

5. DA ECONOMICIDADE

Destaque-se que o valor estimado para referida contratação objeto deste certame foi de **R$ 12.499.110,86** (*doze milhões, quatrocentos e noventa e nove mil, cento e dez reais e oitenta e seis centavos*), conforme **QUADRO-RESUMO DO PROCESSO DE COMPRA Nº 547.2025.SCOMS.2023741.2025.007562.**

Assim, considerando o valor a ser adjudicado de **R$ 10.616.278,00** (*dez milhões, seiscentos e dezesseis mil, duzentos e setenta e oito reais*), a realização deste Pregão significou uma **economia de R$ 1.882.832,86** (*um milhão, oitocentos e oitenta e dois mil, oitocentos e trinta e dois reais e oitenta e seis centavos*), ou seja, uma **redução de aproximadamente 15,06% do valor estimado pela Administração**.

É o Relatório.

Manaus, 02 de fevereiro de 2026.

Sarah Madalena Barbosa Côrtes de Melo

Pregoeira - Portaria N.º 66/2026/SUBADM

Documento assinado eletronicamente por **Sarah Madalena Barbosa Santos Cortes**, **Presidente da Comissão Permanente de Licitação - CPL**, em 02/02/2026, às 17:16, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2060332** e o código CRC **EDEDE2C2**.

MINUTA

MINUTA Nº DESPACHO DE HOMOLOGAÇÃO_GRUPO 3_PE 94001/2026

*** MINUTA DE DOCUMENTO**

PROCESSO SEI n.º 2025.007562

Pregão Eletrônico n.º 94.001/2026-CPL/MP/PGJ

A D J U DI C A Ç Ã O E H O M O L O G A Ç Ã O

C O N S I D E R A N D O a solicitação constante do **Ofício Nº 298.2025.DTIC.**2009577.2025.007562, bem como o teor do **Termo de Referência Nº 28.2025.DTIC.2002143.2025.007562**;

CONSIDERANDO o disposto na Lei, no Termo de Julgamento de realização do Pregão Eletrônico n.º 94.001/2026-CPL/MP/PGJ e demais documentos pertinentes, lavrados pela Comissão Permanente de Licitação entre os dias 19/01/2026 a 02/02/2026, sobretudo, as ponderações do relatório circunstanciado de apreciação do certame de referência, tendo por objeto a *contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma* ***solução de datacenter****, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup,* ***com garantia de 60 (sessenta) meses,*** conforme as especificações e as condições constantes do Edital do certame e seus anexos;

CONSIDERANDO a aceitação da proposta e habilitação da empresa **CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA (FILIAL)** , CNPJ N.º 02.092.332/0003-30, nos seguintes valores: **a) ITEM 1** - pelo valor negociado unitário de R$ 588.062,00 (*quinhentos e oitenta e oito mil sessenta e dois reais*); **b) ITEM 2** - pelo valor negociado unitário de R$ 832.942,00 (*oitocentos e trinta e dois mil novecentos e quarenta e dois reais*); **c) ITEM 3** - pelo melhor lance unitário de R$ 790.000,00 (*setecentos e noventa mil reais*); **d) ITEM 4** - pelo valor negociado unitário de R$ 164.252,00 (*cento e sessenta e quatro mil duzentos e cinquenta e dois reais*); e) **ITEM 5** - pelo valor negociado unitário de R$ 9.250,98 (*nove mil duzentos e cinquenta reais e noventa e oito centavos*); **f) ITEM 6** - pelo melhor lance unitário de R$ 900.000,00 (*novecentos mil reais*) ; **g) ITEM 7** - pelo melhor lance unitário de R$ 230.000,00 (*duzentos e trinta mil reais*) ; h) **ITEM 8** - pelo melhor lance unitário de R$ 1.200.000,00 (*um milhão duzentos mil reais*); e i) **ITEM 9** - pelo valor negociado unitário de R$ 262.143,50 (*duzentos e sessenta e dois mil cento e quarenta e três reais e cinquenta centavos*);

CONSIDERANDO o **Relatório de Licitação n.º 6.2026.CPL**.2060332.2025.007562, no qual consta que a realização do Pregão significou uma **economia de R$ 1.882.832,86** (*um milhão, oitocentos e oitenta e dois mil, oitocentos e trinta e dois reais e oitenta e seis centavos*), o que corresponde a uma **redução aproximada 15,06% do valor estimado pela Administração;**

CONSIDERANDO o teor da Lei Federal n.º 14.133, de 01.04.2021, e do Ato n.º 008/2024/PGJ; e

CONSIDERANDO a não interposição de Recurso por parte dos interessados, no prazo e condições de que trata o art. 165, incisos I e II, da Lei Federal n.º 14.133/2021;

R E S O L V E:

I – **ADJUDICAR** o objeto do certame à empresa **CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA (FILIAL)** , CNPJ N.º 02.092.332/0003-30, pelos seguintes valores: **a) ITEM 1** - pelo valor negociado unitário de R$ 588.062,00 (*quinhentos e oitenta e oito mil sessenta e dois reais*) ; **b) ITEM 2** - pelo valor negociado unitário de R$ 832.942,00 (*oitocentos e trinta e dois mil novecentos e quarenta e dois reais*); **c) ITEM 3** - pelo melhor lance unitário de R$ 790.000,00 (*setecentos e noventa mil reais*); **d) ITEM 4** - pelo valor negociado unitário de R$ 164.252,00 (*cento e sessenta e quatro mil duzentos e cinquenta e dois reais*); e) **ITEM 5** - pelo valor negociado unitário de R$ 9.250,98 (*nove mil duzentos e cinquenta reais e noventa e oito centavos*); **f) ITEM 6** - pelo melhor lance unitário de R$ 900.000,00 (*novecentos mil reais*) ; **g) ITEM 7** - pelo melhor lance unitário de R$ 230.000,00 (*duzentos e trinta mil reais*) ; h) **ITEM 8** - pelo melhor lance unitário de R$ 1.200.000,00 (*um milhão duzentos mil reais*); e i) **ITEM 9** - pelo valor negociado unitário de R$ 262.143,50 (*duzentos e sessenta e dois mil cento e quarenta e três reais e cinquenta centavos*);

II – **HOMOLOGAR** o resultado do procedimento licitatório, referente ao **PREGÃO ELETRÔNICO N.º 94.001/2026-CPL/MP/PGJ**, em consonância com o Termo de Julgamento gerado automaticamente pelo Sistema Compras.gov e o Relatório de Licitação 6 (doc. n.º 2060332), bem como demais documentações complementares;

III – À **COMISSÃO PERMANENTE DE LICITAÇÃO – CPL**, para as providências cabíveis;

IV – Após, ao **SETOR DE COMPRAS E SERVIÇOS - SCOMS,** para prosseguimento do feito.

V – À **DIVISÃO DE CONTRATOS E CONVÊNIOS - DCCON**, para providências de estilo.

Cientifique-se. Publique-se. Cumpra-se.

GABINETE DA SUBPROCURADORA-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, em Manaus (AM), XX de fevereiro de 2026.

ANDRÉ VIRGÍLIO BELOTA SEFFAIR

Subprocurador-Geral de Justiça para Assuntos Administrativos

Ordenador de Despesas

Documento assinado eletronicamente por **Sarah Madalena Barbosa Santos Cortes**, **Presidente da Comissão Permanente de Licitação - CPL**, em 02/02/2026, às 17:16, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2060334** e o código CRC **715CBC32**.

2025.007562 2060334v8

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

DESPACHO Nº 5.2026.CPL.2060335.2025.007562

PROCESSO SEI N.º 2025.007562

Objeto: *Contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma* ***solução de datacenter,*** *contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com* ***garantia de 60 (sessenta) meses****.*

Considerando a realização do Pregão Eletrônico n.º 94.001/2026-CPL/MP/PGJ, iniciado no dia 19 de janeiro de 2026 e encerrado no dia 30 de janeiro do corrente ano;

Considerando a aceitação da proposta de preço e as condições de habilitação do licitante **CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA (FILIAL)**, CNPJ N.º 02.092.332/0003-30;

Considerando que, dentre os requisitos de validade, o resultado do certame necessita da adjudicação e homologação pelo Ordenador de Despesas desta Procuradoria-Geral de Justiça, nos termos da Lei Federal N.º 14.133, de 01.04.2021, e do Ato n.º 008/2024/PGJ;

Encaminhem-se os autos do Procedimento Interno ao Exmo. Sr. Dr. **SUBPROCURADOR-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS**, para fins de análise, adjudicação e homologação do certame licitatório em espeque, caso assim entenda.

Manaus, 02 de fevereiro de 2026.

Sarah Madalena Barbosa Côrtes de Melo

Pregoeira - Portaria N.º 66/2026/SUBADM

Documento assinado eletronicamente por **Sarah Madalena Barbosa Santos Cortes**, **Presidente da Comissão Permanente de Licitação - CPL**, em 02/02/2026, às 17:16, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2060335** e o código CRC **FBFF21F2**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

DESPACHO Nº 88.2026.01AJ-SUBADM.2061824.2025.007562

PROCESSO SEI n.º 2025.007562

Pregão Eletrônico n.º 94.001/2026-CPL/MP/PGJ

A D J U DI C A Ç Ã O E H O M O L O G A Ç Ã O

C O N S I D E R A N D O a solicitação constante do **Ofício n.º 298.2025.DTIC.**2009577.2025.007562, bem como o teor do **Termo de Referência n.º 28.2025.DTIC.2002143.2025.007562**;

CONSIDERANDO o disposto na Lei, no Termo de Julgamento de realização do Pregão Eletrônico n.º 94.001/2026-CPL/MP/PGJ e demais documentos pertinentes, lavrados pela Comissão Permanente de Licitação entre os dias 19/01/2026 a 02/02/2026, sobretudo, as ponderações do relatório circunstanciado de apreciação do certame de referência, tendo por objeto a *contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma* ***solução de datacenter****, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup,* ***com garantia de 60 (sessenta) meses,*** conforme as especificações e as condições constantes do Edital do certame e seus anexos;

CONSIDERANDO a aceitação da proposta e habilitação da empresa **CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA (FILIAL)** , CNPJ N.º 02.092.332/0003-30, nos seguintes valores: **a) ITEM 1** - pelo valor negociado unitário de R$ 588.062,00 (*quinhentos e oitenta e oito mil sessenta e dois reais*); **b) ITEM 2** - pelo valor negociado unitário de R$ 832.942,00 (*oitocentos e trinta e dois mil novecentos e quarenta e dois reais*); **c) ITEM 3** - pelo melhor lance unitário de R$ 790.000,00 (*setecentos e noventa mil reais*); **d) ITEM 4** - pelo valor negociado unitário de R$ 164.252,00 (*cento e sessenta e quatro mil duzentos e cinquenta e dois reais*); e) **ITEM 5** - pelo valor negociado unitário de R$ 9.250,98 (*nove mil duzentos e cinquenta reais e noventa e oito centavos*); **f) ITEM 6** - pelo melhor lance unitário de R$ 900.000,00 (*novecentos mil reais*) ; **g) ITEM 7** - pelo melhor lance unitário de R$ 230.000,00 (*duzentos e trinta mil reais*) ; h) **ITEM 8** - pelo melhor lance unitário de R$ 1.200.000,00 (*um milhão duzentos mil reais*); e i) **ITEM 9** - pelo valor negociado unitário de R$ 262.143,50 (*duzentos e sessenta e dois mil cento e quarenta e três reais e cinquenta centavos*);

CONSIDERANDO o **Relatório de Licitação n.º**

6.2026.CPL.2060332.2025.007562, no qual consta que a realização do Pregão com os seguintes resultados: a) **ITEM 1** – o valor unitário da proposta era **R$ 717.021,00** (**setecentos e dezessete mil e vinte e um reais**) e o valor unitário negociado foi de **R$ 588.062,00** (**quinhentos e oitenta e oito mil e sessenta e dois reais**), o que representa economia de **R$ 128.959,00** (**cento e vinte e oito mil novecentos e cinquenta e nove reais**), correspondente a **redução aproximada de 17,99%**; b) **ITEM 2** – o valor unitário da proposta era **R$ 982.735,00** (**novecentos e oitenta e dois mil setecentos e trinta e cinco reais**) e o valor unitário negociado foi de **R$ 832.942,00** (**oitocentos e trinta e dois mil novecentos e quarenta e dois reais**), o que representa economia de **R$ 149.793,00** (**cento e quarenta e nove mil setecentos e noventa e três reais**), correspondente a **redução aproximada de 15,24%**; c) **ITEM 3** – o valor unitário da proposta era **R$ 925.188,00** (**novecentos e vinte e cinco mil cento e oitenta e oito reais**) e o valor unitário negociado foi de **R$ 790.000,00** (**setecentos e noventa mil reais**), o que representa economia de **R$ 135.188,00** (**cento e trinta e cinco mil cento e oitenta e oito reais**), correspondente a **redução aproximada de 14,61%**; d) **ITEM 4** – o valor unitário da proposta era **R$ 217.972,00** (**duzentos e dezessete mil novecentos e setenta e dois reais**) e o valor unitário negociado foi de **R$ 164.252,00** (**cento e sessenta e quatro mil duzentos e cinquenta e dois reais**), o que representa economia de **R$ 53.720,00** (**cinquenta e três mil setecentos e vinte reais**), correspondente a **redução aproximada de 24,65%**; e) **ITEM 5** – o valor unitário da proposta era **R$ 12.336,00** (**doze mil trezentos e trinta e seis reais**) e o valor unitário negociado foi de **R$ 9.250,98** (**nove mil duzentos e cinquenta reais e noventa e oito centavos**), o que representa economia de **R$ 3.085,02** (**três mil e oitenta e cinco reais e dois centavos**), correspondente a **redução aproximada de 25,01%**; f) **ITEM 6** – o valor unitário da proposta era **R$ 994.639,00** (**novecentos e noventa e quatro mil seiscentos e trinta e nove reais**) e o valor unitário negociado foi de **R$ 900.000,00** (**novecentos mil reais**), o que representa economia de **R$ 94.639,00** (**noventa e quatro mil seiscentos e trinta e nove reais**), correspondente a **redução aproximada de 9,51%**; g) **ITEM 7** – o valor unitário da proposta era **R$ 267.620,00** (**duzentos e sessenta e sete mil seiscentos e vinte reais**) e o valor unitário negociado foi de **R$ 230.000,00** (**duzentos e trinta mil reais**), o que representa economia de **R$ 37.620,00** (**trinta e sete mil seiscentos e vinte reais**), correspondente a **redução aproximada de 14,06%**; h) **ITEM 8** – o valor unitário da proposta era **R$ 1.355.400,00** (**um milhão trezentos e cinquenta e cinco mil e quatrocentos reais**) e o valor unitário negociado foi de **R$ 1.200.000,00** (**um milhão e duzentos mil reais**), o que representa economia de **R$ 155.400,00** (**cento e cinquenta e cinco mil e quatrocentos reais**), correspondente a **redução aproximada de 11,47%**; e i) **ITEM 9** – o valor unitário da proposta era **R$ 515.793,00** (**quinhentos e quinze mil setecentos e noventa e três reais**) e o valor unitário negociado foi de **R$ 262.143,50** (**duzentos e sessenta e dois mil cento e quarenta e três reais e cinquenta centavos**), o que representa economia de **R$ 253.649,50** (**duzentos e cinquenta e três mil seiscentos e quarenta e nove reais e cinquenta centavos**), correspondente a **redução aproximada de 49,18%**, perfazendo uma **economia total de R$ 1.882.832,86** (*um milhão, oitocentos e oitenta e dois mil, oitocentos e trinta e dois reais e oitenta e seis centavos*), o que corresponde a **redução aproximada 15,06% do valor estimado pela Administração**;

CONSIDERANDO o teor da Lei Federal n.º 14.133, de 01.04.2021, e do Ato n.º 008/2024/PGJ; e

CONSIDERANDO a não interposição de Recurso por parte dos interessados, no prazo e condições de que trata o art. 165, incisos I e II, da Lei Federal n.º 14.133/2021;

R E S O L V E:

I – **ADJUDICAR** o objeto do certame à empresa **CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA (FILIAL)** , CNPJ N.º 02.092.332/0003-30, pelos seguintes valores: **a) ITEM 1** - pelo valor negociado unitário de R$ 588.062,00 (*quinhentos e oitenta e oito mil sessenta e dois reais*) ; **b) ITEM 2** - pelo valor negociado unitário de R$ 832.942,00 (*oitocentos e trinta e dois mil novecentos e quarenta e dois reais*); **c) ITEM 3** - pelo melhor lance unitário de R$ 790.000,00 (*setecentos e noventa mil reais*); **d) ITEM 4** - pelo valor negociado unitário de R$ 164.252,00 (*cento e sessenta e quatro mil duzentos e cinquenta e dois reais*); e) **ITEM 5** - pelo valor negociado unitário de R$ 9.250,98 (*nove mil duzentos e cinquenta reais e noventa e oito centavos*); **f) ITEM 6** - pelo melhor lance unitário de R$ 900.000,00 (*novecentos mil reais*) ; **g) ITEM 7** - pelo melhor lance unitário de R$ 230.000,00 (*duzentos e trinta mil reais*) ; h) **ITEM 8** - pelo melhor lance unitário de R$ 1.200.000,00 (*um milhão duzentos mil reais*); e i) **ITEM 9** - pelo valor negociado unitário de R$ 262.143,50 (*duzentos e sessenta e dois mil cento e quarenta e três reais e cinquenta centavos*);

II – **HOMOLOGAR** o resultado do procedimento licitatório, referente ao **PREGÃO ELETRÔNICO N.º 94.001/2026-CPL/MP/PGJ**, em consonância com o Termo de Julgamento gerado automaticamente pelo Sistema Compras.gov e o Relatório de Licitação 6 (doc. n.º 2060332), bem como demais documentações complementares;

III – À **COMISSÃO PERMANENTE DE LICITAÇÃO – CPL**, para as providências cabíveis;

IV – Após, ao **SETOR DE COMPRAS E SERVIÇOS - SCOMS,** para prosseguimento do feito.

V – À **DIVISÃO DE CONTRATOS E CONVÊNIOS - DCCON**, para providências de estilo.

Cientifique-se. Publique-se. Cumpra-se.

GABINETE DA SUBPROCURADORA-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, em Manaus (AM), *data da assinatura eletrônica*.

ANDRÉ VIRGÍLIO BELOTA SEFFAIR

Subprocurador-Geral de Justiça para Assuntos Administrativos

Documento assinado eletronicamente por **André Virgílio Belota Seffair**, **Subprocurador(a)-Geral de Justiça para Assuntos Administrativos**, em 05/02/2026, às 16:34, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2061824** e o código CRC **AECEB204**.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

CERTIDÃO Nº 141.2026.SUBADM.2063648.2025.007562

Certifica-se, para os devidos fins, que o **DESPACHO Nº 88.2026.01AJ-SUBADM.2061824.2025.007562** foi encaminhado ao DOMPE para publicação, nesta data.

Documento assinado eletronicamente por **Mayra Magalhaes Coelho Bezerra**, **Agente Técnico - Jurídico**, em 05/02/2026, às 16:47, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2063648** e o código CRC **1CAA9E4B**.

alterado pelo Ato PGJ n.º 067/2012, de 20.03.2012.

Publique-se, registre-se, cumpra-se.

SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, em Manaus/AM, na data da assinatura eletrônica.

ANDRÉ VIRGÍLIO BELOTA SEFFAIR
Subprocurador-Geral de Justiça para Assuntos Administrativos

PORTARIA Nº 136/2026/SUBADM

O SUBPROCURADOR-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, no uso de suas atribuições legais, e

CONSIDERANDO o teor do Procedimento Interno nº 2026.002505 – SEI;

CONSIDERANDO ainda o disposto no art. 4.º, II, do ATO PGJ N.º 002/2011, datado de 06.01.2011, que dispõe sobre o deslocamento dos membros e servidores do Ministério Público para fora da sede de exercício, estabelece normas para a concessão de passagens e diárias e dá outras providências,

RESOLVE:

I - AUTORIZAR o deslocamento dos servidores ELVIS CLEBE MACIEL CHAVES, Assessor de Comunicação, e ULISSES HERMESON CASTRO DE FARIAS, Requisitado (cinegrafista/fotógrafo), ao município de Novo Aripuanã/AM, no período de 19 a 22 de fevereiro de 2026, com a finalidade de realizarem cobertura jornalística e audiovisual da solenidade de inauguração da sede própria do Ministério Público do Estado do Amazonas;

II - CONCEDER-LHES 3 (três) diárias, na forma da lei, para o custeio de alimentação, pousada e locomoção urbana;

III – DETERMINAR, dentro do prazo legal, a apresentação do relatório de prestação de contas de diárias, em conformidade com as exigências do Ato PGJ n.° 002/2011, de 06.01.2011, alterado pelo Ato PGJ n.º 067/2012, de 20.03.2012.

Publique-se, registre-se, cumpra-se.

SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, em Manaus/AM, na data da assinatura eletrônica.

ANDRÉ VIRGÍLIO BELOTA SEFFAIR
Subprocurador-Geral de Justiça para Assuntos Administrativos

PORTARIA Nº 137/2026/SUBADM

O SUBPROCURADOR-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, no uso de suas atribuições legais, e

CONSIDERANDO o disposto no art. 4.º, inciso I, do ATO PGJ N.º 076/2013, de 03 de maio de 2013,

CONSIDERANDO o teor do Procedimento Administrativo n.º 2026.001596 – SEI,

RESOLVE:

RELOTAR o servidor MÁRCIO BATISTA MACHADO, Agente Técnico - Jurídico, para exercer suas funções junto à 70ª Promotoria de Justiça, a contar de 09/02/2026.

Publique-se, registre-se, cumpra-se.

SUBPROCURADORIA-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, em Manaus/AM, na data da assinatura eletrônica.

ANDRÉ VIRGÍLIO BELOTA SEFFAIR
Subprocurador-Geral de Justiça para Assuntos Administrativos

DESPACHO Nº 88.2026.01AJ-SUBADM.2061824.2025.007562

PROCESSO SEI n.º 2025.007562
Pregão Eletrônico n.º 94.001/2026-CPL/MP/PGJ

A D J U DI C A Ç Ã O E H O M O L O G A Ç Ã O

CONSIDERANDO a solicitação constante do Ofício n.º 298.2025.DTIC.2009577.2025.007562, bem como o teor do Termo de Referência n.º 28.2025.DTIC.2002143.2025.007562;

CONSIDERANDO o disposto na Lei, no Termo de Julgamento de realização do Pregão Eletrônico n.º 94.001/2026-CPL/MP/PGJ e demais documentos pertinentes, lavrados pela Comissão Permanente de Licitação entre os dias 19/01/2026 a 02/02/2026, sobretudo, as ponderações do relatório circunstanciado de apreciação do certame de referência, tendo por objeto a contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses, conforme as especificações e as condições constantes do Edital do certame e seus anexos;

CONSIDERANDO a aceitação da proposta e habilitação da empresa CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA (FILIAL), CNPJ N.º 02.092.332/0003-30, nos seguintes valores: a) ITEM 1 - pelo valor negociado unitário de R$ 588.062,00 (quinhentos e oitenta e oito mil sessenta e dois reais); b) ITEM 2 - pelo valor negociado unitário de R$ 832.942,00 (oitocentos e trinta e dois mil novecentos e quarenta e dois reais); c) ITEM 3 - pelo melhor lance unitário de R$ 790.000,00 (setecentos e noventa mil reais); d) ITEM 4 - pelo valor negociado unitário de R$ 164.252,00 (cento e sessenta e quatro mil duzentos e cinquenta e dois reais); e) ITEM 5 - pelo valor negociado unitário de R$ 9.250,98 (nove mil duzentos e cinquenta reais e noventa e oito centavos); f) ITEM 6 - pelo melhor lance unitário de R$ 900.000,00 (novecentos mil reais) ; g) ITEM 7 - pelo melhor lance unitário de R$ 230.000,00 (duzentos e trinta mil reais) ; h) ITEM 8 - pelo melhor lance unitário de R$ 1.200.000,00 (um milhão duzentos mil reais); e i) ITEM 9 - pelo valor negociado unitário de R$ 262.143,50 (duzentos e sessenta e dois mil cento e quarenta e três reais e cinquenta centavos);

CONSIDERANDO o Relatório de Licitação n.º 6.2026.CPL.2060332.2025.007562, no qual consta que a realização do Pregão com os seguintes resultados: a) ITEM 1 – o valor unitário da proposta era R$ 717.021,00 (setecentos e dezessete mil e vinte e um reais) e o valor unitário negociado foi de R$ 588.062,00 (quinhentos e oitenta e oito mil e sessenta e dois reais), o que representa economia de R$ 128.959,00 (cento e vinte e oito mil novecentos e cinquenta e nove reais), correspondente a redução aproximada de 17,99%; b) ITEM 2 – o valor unitário da proposta era R$ 982.735,00 (novecentos e oitenta e dois mil setecentos e trinta e cinco reais) e o valor unitário negociado foi de R$ 832.942,00 (oitocentos e trinta e dois mil novecentos e quarenta e dois reais), o que representa economia de R$ 149.793,00 (cento e quarenta e nove mil setecentos e noventa

PROCURADORIA-GERAL DE JUSTIÇA

Procuradora-Geral de Justiça:
Leda Mara Nascimento Albuquerque
Subprocuradora-Geral de Justiça para Assuntos Jurídicos e Institucionais:
Anabel Vitória Pereira Mendonça de Souza
Subprocurador-Geral de Justiça para Assuntos Administrativos:
André Virgílio Belota Seffair
Corregedora-Geral do Ministério Público:
Silvana Nobre de Lima Cabral
Secretária-Geral do Ministério Público:
Wandete de Oliveira Netto

PROCURADORES DE JUSTIÇA

Câmaras Cíveis
Elvys de Paula Freitas
Sandra Cal Oliveira
Jussara Maria Pordeus e Silva
Mara Nóbia Albuquerque da Cunha
Suzete Maria dos Santos
Nilda Silva de Sousa
Delisa Olívia Vieiralves Ferreira
Jorge Michel Ayres Martins
Anabel Vitória Pereira Mendonça de Souza
Marco Aurélio Lisciotto

Câmaras Criminais
Carlos Lélio Lauria Ferreira
Marlene Franco da Silva
Mauro Roberto Veras Bezerra
Sarah Pirangy de Souza
Aguinelo Balbi Júnior
Liani Mônica Guedes de Freitas Rodrigues
Adelton Albuquerque Matos

Câmaras Reunidas
Karla Fregapani Leite
Públio Caio Bessa Cyrino
Sílvia Abdala Tuma
José Bernardo Ferreira Júnior
Neyde Regina Demósthenes Trindade
Silvana Nobre de Lima Cabral

CONSELHO SUPERIOR

Leda Mara Nascimento Albuquerque (Presidente)
Silvana Nobre de Lima Cabral
Mara Nóbia Albuquerque da Cunha
Adelton Albuquerque Matos
Elvys de Paula Freitas
Jorge Michel Ayres Martins
Nilda Silva de Sousa

OUVIDORIA
Sílvia Abdala Tuma

e três reais), correspondente a redução aproximada de 15,24%; c) ITEM 3 – o valor unitário da proposta era R$ 925.188,00 (novecentos e vinte e cinco mil cento e oitenta e oito reais) e o valor unitário negociado foi de R$ 790.000,00 (setecentos e noventa mil reais), o que representa economia de R$ 135.188,00 (cento e trinta e cinco mil cento e oitenta e oito reais), correspondente a redução aproximada de 14,61%; d) ITEM 4 – o valor unitário da proposta era R$ 217.972,00 (duzentos e dezessete mil novecentos e setenta e dois reais) e o valor unitário negociado foi de R$ 164.252,00 (cento e sessenta e quatro mil duzentos e cinquenta e dois reais), o que representa economia de R$ 53.720,00 (cinquenta e três mil setecentos e vinte reais), correspondente a redução aproximada de 24,65%; e) ITEM 5 – o valor unitário da proposta era R$ 12.336,00 (doze mil trezentos e trinta e seis reais) e o valor unitário negociado foi de R$ 9.250,98 (nove mil duzentos e cinquenta reais e noventa e oito centavos), o que representa economia de R$ 3.085,02 (três mil e oitenta e cinco reais e dois centavos), correspondente a redução aproximada de 25,01%; f) ITEM 6 – o valor unitário da proposta era R$ 994.639,00 (novecentos e noventa e quatro mil seiscentos e trinta e nove reais) e o valor unitário negociado foi de R$ 900.000,00 (novecentos mil reais), o que representa economia de R$ 94.639,00 (noventa e quatro mil seiscentos e trinta e nove reais), correspondente a redução aproximada de 9,51%; g) ITEM 7 – o valor unitário da proposta era R$ 267.620,00 (duzentos e sessenta e sete mil seiscentos e vinte reais) e o valor unitário negociado foi de R$ 230.000,00 (duzentos e trinta mil reais), o que representa economia de R$ 37.620,00 (trinta e sete mil seiscentos e vinte reais), correspondente a redução aproximada de 14,06%; h) ITEM 8 – o valor unitário da proposta era R$ 1.355.400,00 (um milhão trezentos e cinquenta e cinco mil e quatrocentos reais) e o valor unitário negociado foi de R$ 1.200.000,00 (um milhão e duzentos mil reais), o que representa economia de R$ 155.400,00 (cento e cinquenta e cinco mil e quatrocentos reais), correspondente a redução aproximada de 11,47%; e i) ITEM 9 – o valor unitário da proposta era R$ 515.793,00 (quinhentos e quinze mil setecentos e noventa e três reais) e o valor unitário negociado foi de R$ 262.143,50 (duzentos e sessenta e dois mil cento e quarenta e três reais e cinquenta centavos), o que representa economia de R$ 253.649,50 (duzentos e cinquenta e três mil seiscentos e quarenta e nove reais e cinquenta centavos), correspondente a redução aproximada de 49,18%, perfazendo uma economia total de R$ 1.882.832,86 (um milhão, oitocentos e oitenta e dois mil, oitocentos e trinta e dois reais e oitenta e seis centavos), o que corresponde a redução aproximada 15,06% do valor estimado pela Administração;

CONSIDERANDO o teor da Lei Federal n.º 14.133, de 01.04.2021, e do Ato n.º 008/2024/PGJ; e

CONSIDERANDO a não interposição de Recurso por parte dos interessados, no prazo e condições de que trata o art. 165, incisos I e II, da Lei Federal n.º 14.133/2021;

RESOLVE:

I – ADJUDICAR o objeto do certame à empresa CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA (FILIAL), CNPJ N.º 02.092.332/0003-30, pelos seguintes valores: a) ITEM 1 - pelo valor negociado unitário de R$ 588.062,00 (quinhentos e oitenta e oito mil sessenta e dois reais); b) ITEM 2 - pelo valor negociado unitário de R$ 832.942,00 (oitocentos e trinta e dois mil novecentos e quarenta e dois reais); c) ITEM 3 - pelo melhor lance unitário de R$ 790.000,00 (setecentos e noventa mil reais); d) ITEM 4 - pelo valor negociado unitário de R$ 164.252,00 (cento e sessenta e quatro mil duzentos e cinquenta e dois reais); e) ITEM 5 - pelo valor negociado unitário de R$ 9.250,98 (nove mil duzentos e cinquenta reais e noventa e oito centavos); f) ITEM 6 - pelo melhor lance unitário de R$ 900.000,00 (novecentos mil reais) ; g) ITEM 7 - pelo melhor lance unitário de R$ 230.000,00 (duzentos e trinta mil reais) ; h) ITEM 8 - pelo melhor lance unitário de R$ 1.200.000,00 (um milhão duzentos mil reais); e i) ITEM 9 - pelo valor negociado unitário de R$ 262.143,50 (duzentos e sessenta e dois mil cento e quarenta e três reais e cinquenta centavos);

II – HOMOLOGAR o resultado do procedimento licitatório, referente ao PREGÃO ELETRÔNICO N.º 94.001/2026-CPL/MP/PGJ, em consonância com o Termo de Julgamento gerado automaticamente pelo Sistema Compras.gov e o Relatório de Licitação 6 (doc. n.º 2060332), bem como demais documentações complementares;

III – À COMISSÃO PERMANENTE DE LICITAÇÃO – CPL, para as providências cabíveis;

IV – Após, ao SETOR DE COMPRAS E SERVIÇOS - SCOMS, para prosseguimento do feito.

V – À DIVISÃO DE CONTRATOS E CONVÊNIOS - DCCON, para providências de estilo.

Cientifique-se. Publique-se. Cumpra-se.

GABINETE DA SUBPROCURADORA-GERAL DE JUSTIÇA PARA ASSUNTOS ADMINISTRATIVOS, em Manaus (AM), data da assinatura eletrônica.

ANDRÉ VIRGÍLIO BELOTA SEFFAIR
Subprocurador-Geral de Justiça para Assuntos Administrativos
Ordenador de Despesas

DESPACHO Nº 97.2026.01AJ-SUBADM.2063108.2026.001230

Processo n.º 2026.001230

ADESÃO À ARP

CONSIDERANDO a solicitação formalizada por meio do Memorando Nº 5.2026.ARPC.2049984.2026.001230, visando adesão à Ata de Registro de Preços n.º 24/2024, decorrente do Pregão Eletrônico n.º 020/2024/TJAM, realizado pelo Tribunal de Justiça do Estado do Amazonas (TJAM), a fim de atender demanda referente à contratação de serviço de buffet para a Abertura dos Trabalhos do Colégio de Procuradores de Justiça do Ministério Público do Estado do Amazonas, no dia 06 de fevereiro de 2026;

CONSIDERANDO o disposto na legislação aplicável, especialmente a Lei n.º 14.133/2021, o Decreto Federal n.º 11.462/2023, o edital do Pregão Eletrônico para Registro de Preços n.º 020/2024, conforme Processo Administrativo n.º 2024/000018121-00, promovido pelo Tribunal de Justiça do Estado do Amazonas –TJAM, bem como os termos da Ata de Registro de Preço n° 24/2024, de 27/08/2024, firmada com a empresa CONTEMPORANEO FESTAS E EVENTOS LTDA, registrada sob o CNPJ n.º 09.199.109/0001-74;

CONSIDERANDO a homologação do Pregão Eletrônico n.° 020/2024-TJAM, publicada no Diário da Justiça Eletrônico, Edição n.º 3860, datada de 22/08/2024, página 2;

CONSIDERANDO a publicação da Ata de Registro de Preço (ARP) n.° 24/2024, vinculada ao Pregão Eletrônico n.° 020/2024-TJAM, no Portal Nacional de Contratações Públicas - PNCP, sob a Id ata PNCP: 04312369000190-1-000195/2024-

PROCURADORIA-GERAL DE JUSTIÇA

Procuradora-Geral de Justiça:
Leda Mara Nascimento Albuquerque
Subprocuradora-Geral de Justiça para Assuntos Jurídicos e Institucionais:
Anabel Vitória Pereira Mendonça de Souza
Subprocurador-Geral de Justiça para Assuntos Administrativos:
André Virgílio Belota Seffair
Corregedora-Geral do Ministério Público:
Silvana Nobre de Lima Cabral
Secretária-Geral do Ministério Público:
Wandete de Oliveira Netto

PROCURADORES DE JUSTIÇA

Câmaras Cíveis
Elvys de Paula Freitas
Sandra Cal Oliveira
Jussara Maria Pordeus e Silva
Mara Nóbia Albuquerque da Cunha
Suzete Maria dos Santos
Nilda Silva de Sousa
Delisa Olívia Vieiralves Ferreira
Jorge Michel Ayres Martins
Anabel Vitória Pereira Mendonça de Souza
Marco Aurélio Lisciotto

Câmaras Criminais
Carlos Lélio Lauria Ferreira
Marlene Franco da Silva
Mauro Roberto Veras Bezerra
Sarah Pirangy de Souza
Aguinelo Balbi Júnior
Liani Mônica Guedes de Freitas Rodrigues
Adelton Albuquerque Matos

Câmaras Reunidas
Karla Fregapani Leite
Públio Caio Bessa Cyrino
Sílvia Abdala Tuma
José Bernardo Ferreira Júnior
Neyde Regina Demósthenes Trindade
Silvana Nobre de Lima Cabral

CONSELHO SUPERIOR

Leda Mara Nascimento Albuquerque (Presidente)
Silvana Nobre de Lima Cabral
Mara Nóbia Albuquerque da Cunha
Adelton Albuquerque Matos
Elvys de Paula Freitas
Jorge Michel Ayres Martins
Nilda Silva de Sousa

OUVIDORIA
Sílvia Abdala Tuma

PROCURADORIA GERAL DE JUSTIÇA

TERMO DE HOMOLOGAÇÃO

UASG 925849 - PROCURADORIA GERAL DE JUSTIÇA - AM

PREGÃO 94001/2026

Às 10:51 horas do dia 09 de fevereiro do ano de 2026, após constatada a regularidade dos atos procedimentais, a autoridade competente, ANDRE VIRGILIO BELOTA SEFFAIR, HOMOLOGA a adjudicação referente ao Processo nª 2025.007562, Pregão nª 94001/2026.

Fundamentação legal:	Lei 14.133/2021	Característica:	SISPP - Tradicional
Critério de julgamento:	Menor Preço / Maior Desconto	Modo de disputa:	Aberto
Compra emergencial:	Não	UF da UASG:	AM
Objeto da compra:	Contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses.		
Entrega de propostas:	De 05/01/2026 às 08:00 até 19/01/2026 às 10:00		
Abertura da sessão pública:	Dia 19/01/2026 às 10:00 (horário de Brasília)		

Mensagens do chat da compra

Responsável	Data/Hora	Mensagem
Sistema	19/01/2026 às 10:00:06	A sessão pública está aberta. Até 20 itens poderão estar em disputa simultaneamente e o período de abertura para disputa será entre 08:00 e 18:00. Haverá aviso prévio de abertura dos itens de 10 minutos. Mantenham-se conectados.
Sistema	19/01/2026 às 10:05:55	Bom dia, senhores!
Sistema	19/01/2026 às 10:06:25	Estamos iniciando a sessão pública do pregão eletrônico n.ª 94.001/2026-CPL/MP/PGJ, promovido pelo Ministério Público do Estado do Amazonas/Procuradoria-Geral de Justiça do Amazonas. Antes de iniciar a fase competitiva, peço a atenção de todos para alguns breves avisos a respeito da presente licitação.
Sistema	19/01/2026 às 10:07:12	Senhores, o Pregão Eletrônico n.ª 94.001/2026-CPL/MP/PGJ tem por objeto a contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma solução de datacenter, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup, com garantia de 60 (sessenta) meses.
Sistema	19/01/2026 às 10:07:40	A licitação será pelo MENOR PREÇO GLOBAL.
Sistema	19/01/2026 às 10:09:07	A especificação técnica dos produtos consta do Termo de Referência Nª 28.2025.DTIC.2002143.2025.007562 (Anexo I do Edital).
Sistema	19/01/2026 às 10:10:19	O envio de lances, sejam eles intermediários ou destinados a cobrir a melhor oferta, devem respeitar o intervalo mínimo de R$ 10,00 (dez reais).de modo que as ofertas em desacordo com este critério não serão processadas pelo sistema (item 8.8 do Edital).
Sistema	19/01/2026 às 10:10:41	É importante destacar que o licitante é responsável por todas as transações efetuadas em seu nome, especialmente o cadastramento de proposta e o oferecimento de lances, ainda que o acesso ao sistema seja realizado por terceiros.
Sistema	19/01/2026 às 10:13:59	Prezados, os valores ofertados ainda estão acima do valor estimado pela Administração.
Sistema	19/01/2026 às 10:30:43	A etapa de julgamento de propostas foi iniciada. Para acompanhá-la acesse a opção "Seleção de fornecedores" na linha do tempo.

Termo de HOMOLOGAÇÃO_Compras.gov (2065377) SEI 2025.007562 / pg. 3617

Responsável	Data/Hora	Mensagem
Sistema	19/01/2026 às 10:31:52	Senhores, encerrada a fase de lances, passemos à fase de julgamento das propostas.
Sistema	19/01/2026 às 10:33:55	Assim, o licitante mais bem classificado na fase de lances será convocado, nos termos dos itens 9 e 10 do instrumento convocatório, a encaminhar, por meio do Sistema, sua proposta e os documentos complementares, no prazo de 02 (duas) horas.
Sistema	19/01/2026 às 10:50:45	Senhores, em verificação preliminar, a equipe de apoio constatou que alguns itens apresentam valores superiores ao estimado pela Administração.
Sistema	19/01/2026 às 10:50:51	Portanto, será aberta a etapa de negociação, previamente à solicitação da proposta formal.
Sistema	19/01/2026 às 11:38:28	Senhor, nesses valores a empresa está considerando o preço unitário do item?
Sistema	19/01/2026 às 14:43:39	Boa tarde, senhores. Em instantes, retomaremos os trabalhos.
Sistema	19/01/2026 às 15:02:26	Senhores, dando prosseguimento ao certame, uma vez concluída a negociação dos valores de determinados itens, a empresa será convocada, nos termos dos itens 9 e 10 do instrumento convocatório, a encaminhar, por meio do Sistema Compras.gov, a proposta e os respectivos documentos complementares, no prazo de 02 (duas) horas.
Sistema	19/01/2026 às 15:08:19	Senhores, a sessão fica suspensa, sem prejuízo do atendimento ao prazo de convocação. A reabertura ocorrerá amanhã, dia 20/01/2026, às 10h30.
Sistema	20/01/2026 às 10:36:02	Bom dia, senhores!
Sistema	20/01/2026 às 10:56:39	Senhores, verificado o atendimento, pela empresa CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA., inscrita no CNPJ nª 02.092.332/0003-30, à convocação realizada, os documentos apresentados serão encaminhados para análise técnica pela equipe da Diretoria de Tecnologia da Informação e Comunicação - DTIC, nos termos do item 10.2 do Edital.
Sistema	20/01/2026 às 13:09:51	Senhores, considerando que a proposta encontra-se em análise pela equipe técnica, ficam encerrados os trabalhos na presente data. A reabertura da sessão será oportunamente informada por meio do chat, com antecedência mínima de 24 (vinte e quatro) horas.
Sistema	27/01/2026 às 09:38:25	Bom dia, Senhores! Informo que a reabertura da sessão está agendada para amanhã, 28/01/2026, às 10h30.
Sistema	28/01/2026 às 10:28:13	Bom dia, senhores! Em instantes, retomaremos os trabalhos.
Sistema	28/01/2026 às 12:05:57	Senhores, em razão de compromisso institucional, a reabertura da sessão fica adiada para hoje, às 14h. Agradeço a todos pela compreensão.
Sistema	28/01/2026 às 14:06:22	Senhores, boa tarde! Como providência anterior, a proposta apresentada pela empresa CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA., inscrita no CNPJ (MF) nª 02.092.332/0003-30, foi encaminhada à Diretoria de Tecnologia da Informação e Comunicação - DTIC para análise técnica e manifestação conclusiva.
Sistema	28/01/2026 às 14:06:43	Em resposta, conforme consignado no Parecer nª 5.2026.DTIC.2050482.2025.007562, a unidade técnica concluiu que, após análise individualizada dos itens constantes do Termo de Referência, a proposta apresentada atende integralmente às exigências técnicas estabelecidas, não tendo sido identificadas não conformidades, sejam sanáveis ou insanáveis.
Sistema	28/01/2026 às 14:07:13	Assim, a proposta foi considerada tecnicamente compatível com o objeto licitado, encontrando-se apta ao prosseguimento do certame, motivo pelo qual a equipe técnica opinou pela sua aceitação.
Sistema	28/01/2026 às 14:07:22	A íntegra do referido parecer encontra-se disponível para consulta na página eletrônica de acompanhamento deste certame, por meio do seguinte link:
Sistema	28/01/2026 às 14:07:29	https://www.mpam.mp.br/licitacoes/licitacoes-em-andamento?view=article&id=31037:pe-94-001-2026-cpl-mp-pgj-contratacao-de-empresa-especializada-para-fornecimento-de-solucao-de-datacenter&catid=47
Sistema	28/01/2026 às 14:31:07	Diante do exposto, e considerando o atendimento às exigências do instrumento convocatório, decido aceitar a proposta apresentada pela empresa CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA., CNPJ (MF) nª 02.092.332/0003-30.

Termo de HOMOLOGAÇÃO_Compras.gov (2065377) SEI 2025.007562 / pg. 3618

Responsável	Data/Hora	Mensagem
Sistema	28/01/2026 às 14:33:12	Dando prosseguimento ao certame, passa-se à fase de verificação das condições de habilitação da empresa CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA., CNPJ (MF) nª 02.092.332/0003-30.
Sistema	28/01/2026 às 16:22:32	Senhores, considerando a necessidade de análise detalhada dos documentos de habilitação apresentados pela empresa CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA., CNPJ (MF) nª 02.092.332/0003-30, a sessão será suspensa para realização da respectiva verificação. A reabertura da sessão fica designada para o dia 30/01/2026, sexta-feira, às 11h.
Sistema	30/01/2026 às 10:56:15	Bom dia, senhores!
Sistema	30/01/2026 às 11:01:19	Senhores, informo que a equipe de apoio encontra-se em fase de conclusão da conferência e convalidação das certidões apresentadas pela empresa.
Sistema	30/01/2026 às 13:10:55	Senhores, informo que, a partir de 14h30, será divulgado o resultado da análise dos documentos de habilitação da empresa.
Sistema	30/01/2026 às 14:56:29	Boa tarde, senhores!
Sistema	30/01/2026 às 15:29:35	Senhores, dando prosseguimento ao certame, destaco que a documentação de habilitação da empresa CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA., inscrita no CNPJ (MF) nª 02.092.332/0003-30, também foi encaminhada à Diretoria de Tecnologia da Informação e Comunicação – DTIC para análise técnica e manifestação.
Sistema	30/01/2026 às 15:37:07	Em resposta, conforme consignado no Parecer nª 6.2026.DTIC.2054079.2025.007562, a unidade técnica concluiu que a declaração de pessoal técnico, instalações e aparelhamento atende, formal e materialmente, ao item 3.2.2 do Termo de Referência, bem como que a empresa CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA. comprovou satisfatoriamente sua capacitação técnico-operacional, atendendo integralmente às exigências estabelecidas no TR.
Sistema	30/01/2026 às 15:37:16	A íntegra do referido parecer encontra-se disponível para consulta na página eletrônica de acompanhamento deste certame, por meio do seguinte link:
Sistema	30/01/2026 às 15:37:30	https://www.mpam.mp.br/licitacoes/licitacoes-em-andamento?view=article&id=31037:pe-94-001-2026-cpl-mp-pgj-contratacao-de-empresa-especializada-para-fornecimento-de-solucao-de-datacenter&catid=47
Sistema	30/01/2026 às 15:43:21	Senhores, informo que foi verificada, por meio do SICAF, a autenticidade das certidões fiscais apresentadas, bem como a certidão de inexistência de ações de falência ou recuperação judicial junto ao Tribunal de Justiça do domicílio da licitante, não tendo sido identificadas inconsistências, inclusive quanto à situação falimentar da matriz.
Sistema	30/01/2026 às 15:43:33	Da mesma forma, procedeu-se à verificação dos demais documentos de habilitação apresentados pela interessada, cuja autenticidade foi validada por meio eletrônico.
Sistema	30/01/2026 às 15:43:49	Ressalte-se que a equipe de apoio deste certame utilizou as informações disponíveis no SICAF para complementar a análise documental da empresa CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA, procedendo às devidas verificações de autenticidade e regularidade por meio daquele sistema.
Sistema	30/01/2026 às 15:43:59	Na sequência, procedeu-se à verificação da situação da licitante quanto à inexistência de sanções aplicadas pela Administração Pública, mediante consulta ao SICAF (Compras.gov.br), à Relação de Empresas com Sanção Administrativa em Vigor, mantida pelo Tribunal de Contas do Estado do Amazonas – TCE/AM, bem como à Relação de Licitantes Inidôneos disponibilizada pelo Tribunal de Contas da União – TCU.
Sistema	30/01/2026 às 15:44:11	Igualmente, foram verificadas as condições da licitante quanto à regularidade perante a Lista de Empresas Suspensas/Impedidas da Comissão Geral de Licitação do Estado do Amazonas – CGL; o Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), da Controladoria-Geral da União – CGU; e o Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa (CNCIA), mantido pelo Conselho Nacional de Justiça – CNJ.
Sistema	30/01/2026 às 15:44:20	Ademais, foi realizada diligência junto à Relação de Pessoas Jurídicas impedidas de contratar com a Administração Pública, mantida pela Secretaria de Estado da Fazenda do Amazonas – SEFAZ-AM, não sendo constatado qualquer registro que indicasse restrição à contratação.

Termo de HOMOLOGAÇÃO_Compras.gov (2065377) SEI 2025.007562 / pg. 3619

Responsável	Data/Hora	Mensagem
Sistema	30/01/2026 às 15:51:11	Oportunamente, registre-se que foi realizada consulta consolidada de pessoas jurídicas, a qual reúne, em um único ambiente, as seguintes bases: Relação de Licitantes Inidôneos do TCU; CNIA – Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade, do CNJ; Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS; e CNEP – Cadastro Nacional de Empresas Punidas
Sistema	30/01/2026 às 15:51:39	Assim, será promovida a juntada da Consulta Consolidada de Pessoa Jurídica (TCU), bem como a Situação do Fornecedor (SICAF) da empresa CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA, CNPJ N.ª 02.092.332/0003-30, aos autos do procedimento interno desta Instituição.
Sistema	30/01/2026 às 15:51:59	O extrato do SICAF e a Consulta Consolidada de Pessoa Jurídica encontram-se disponíveis no seguinte endereço eletrônico:
Sistema	30/01/2026 às 15:52:03	https://www.mpam.mp.br/licitacoes/licitacoes-em-andamento?view=article&id=31037:pe-94-001-2026-cpl-mp-pgj-contratacao-de-empresa-especializada-para-fornecimento-de-solucao-de-datacenter&catid=47
Sistema	30/01/2026 às 15:55:24	Pelo exposto, concluída a análise dos documentos de habilitação, nos termos do item 11 do instrumento convocatório, verifica-se que a empresa CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA., CNPJ nª 02.092.332/0003-30, atendeu a todas as exigências editalícias, razão pela qual fica HABILITADA, com a respectiva habilitação promovida no sistema.
Sistema	30/01/2026 às 15:56:25	Agradeço a todos pela participação neste pregão eletrônico. Até a próxima oportunidade.

Eventos da compra

Data/Hora	Descrição
19/01/2026 às 10:00:06	Abertura da sessão pública
19/01/2026 às 10:30:43	Início da etapa de julgamento de propostas

Termo de HOMOLOGAÇÃO_Compras.gov (2065377) SEI 2025.007562 / pg. 3620

Grupo 1

Valor estimado: R$ 12.499.110,8600 (total)

Situação: Adjudicado e Homologado

Tratamento Diferenciado ME/EPP: Sem benefícios ME/EPP (Art. 4ª, lei 14.133/2021)

Adjudicado e Homologado por CPF ***.287.***-*3 - ANDRE VIRGILIO BELOTA SEFFAIR para CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, melhor lance: R$ 11.180.000,0000 (total), valor negociado: R$ 10.616.278,0000 (total)

Propostas do Grupo G1

Benefício Me/Epp: Conforme Art. 3ª da Lei Complementar nª 123, de 14 de dezembro de 2006
Equidade de gênero: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 11.430/2023
Programa de integridade: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 12.304/2024

Fornecedor	Valor ofertado	Situação
02.092.332/0003-30 - CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. Beneficio Me/Epp: Não Equidade de gênero: Bronze Programa de integridade: Sim UF endereço: ES	R$ 11.180.000,0000 (total)	Proposta adjudicada
Valor proposta: R$ 12.960.776,0000 (total) Valor negociado: R$ 10.616.278,0000 (total)		
39.532.571/0001-02 - GIUSEPPE ANTONIO FOGACA GERBALDO Beneficio Me/Epp: Sim Equidade de gênero: Nenhum Programa de integridade: Não UF endereço: AM	R$ 99.000.000,0000 (total)	-
Valor proposta: R$ 214.000.000,0000 (total) Valor negociado: Não Realizado		

Mensagens do chat do Grupo G1

Responsável	Data/Hora	Mensagem
Sistema	19/01/2026 às 10:00:07	A abertura do item G1 para lances está agendada para daqui a 10 minutos. Mantenham-se conectados.
Sistema	19/01/2026 às 10:10:07	O item G1 foi aberto. Solicitamos o envio de lances.
Sistema	19/01/2026 às 10:26:49	O item G1 está aguardando decisão de reinício ou encerramento da etapa aberta pelo comprador.
Sistema	19/01/2026 às 10:30:38	O item G1 está encerrado.
Sistema para o participante 02.092.332/0003-30	19/01/2026 às 10:52:51	Bom dia, senhor. Solicito a reavaliação dos preços dos itens 1, 2, 4, 5 e 9 e a indicação de eventual possibilidade de negociação.
Pelo participante 02.092.332/0003-30	19/01/2026 às 10:54:35	Bom dia!
Pelo participante 02.092.332/0003-30	19/01/2026 às 10:55:28	Sr. Pregoeiro, peço 15 minutos para avaliação interna de aplicação de desconto nos itens mencionados.
Sistema para o participante 02.092.332/0003-30	19/01/2026 às 11:01:38	Certamente. Permanecemos no aguardo.
Pelo participante 02.092.332/0003-30	19/01/2026 às 11:06:40	Sr. Após análise interna, informamos que foi possível aplicar os seguintes valores unitários para os itens solicitados:

Termo de HOMOLOGAÇÃO_Compras.gov (2065377) SEI 2025.007562 / pg. 3621

Responsável	Data/Hora	Mensagem
Pelo participante 02.092.332/0003-30	19/01/2026 às 11:08:18	Item 1: R$ 608.000,00 - Item 2: R$ 838.000,00 - Item 4: R$ 185.000,00 - Item 5: R$ 10.190,00 - Item 9: R$ 430.000,00
Sistema para o participante 02.092.332/0003-30	19/01/2026 às 11:39:26	Senhor, nesses valores a empresa está considerando o preço unitário do item?
Pelo participante 02.092.332/0003-30	19/01/2026 às 11:39:52	informamos que foi possível aplicar os seguintes valores unitários dos itens solicitados
Pelo participante 02.092.332/0003-30	19/01/2026 às 11:41:26	Sim. Os valores informados referem-se ao preço unitário de cada item.
Sistema para o participante 02.092.332/0003-30	19/01/2026 às 11:45:47	Senhor, os preços estimados pela Administração para os itens em negociação são: Item 1 - R$ 588.062,67; Item 2 - R$ 832.942,67; Item 4 - R$ 164.252,40; Item 5 - R$ 9.250,98; Item 9 - R$ 262.143,66.
Sistema para o participante 02.092.332/0003-30	19/01/2026 às 11:47:27	Caso a empresa aceite esses preços, a negociação encontra-se aberta no sistema para registro dos novos valores.
Sistema para o participante 02.092.332/0003-30	19/01/2026 às 11:48:04	Sr. Fornecedor CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, você foi convocado para negociação de valor do item G1. Justificativa: Negociação via chat (limite: valor estimado pela Administração). .
Pelo participante 02.092.332/0003-30	19/01/2026 às 11:57:32	Solicitamos, por gentileza, a concessão de prazo para avaliação dos valores sugeridos junto ao fabricante. Considerando o horário de almoço, poderemos retornar com a avaliação até às 14h00?
Sistema para o participante 02.092.332/0003-30	19/01/2026 às 12:00:30	Considerando a sua solicitação, faremos um intervalo para almoço, com retorno programado para as 15h.
Pelo participante 02.092.332/0003-30	19/01/2026 às 12:01:20	obrigada
Pelo participante 02.092.332/0003-30	19/01/2026 às 14:25:40	O item G1 teve a negociação de valor encerrada pelo fornecedor CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30. A negociação do item G1 foi aceita pelo fornecedor CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, tendo informado R$ 10.616.278,0000.
Sistema para o participante 02.092.332/0003-30	19/01/2026 às 14:46:25	Senhor, agradeço a disponibilidade para negociação.
Sistema para o participante 02.092.332/0003-30	19/01/2026 às 15:03:42	Senhor, solicito, no prazo de 2 (duas) horas, a proposta ajustada aos valores negociados, acompanhada da documentação complementar, que será analisada pela equipe técnica desta Procuradoria-Geral de Justiça.
Sistema para o participante 02.092.332/0003-30	19/01/2026 às 15:04:07	Sr. Fornecedor CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, você foi convocado para enviar anexos para o item G1. Prazo para encerrar o envio: 17:05:00 do dia 19/01/2026. Justificativa: Proposta e documentos complementares. .
Pelo participante 02.092.332/0003-30	19/01/2026 às 15:32:21	O item G1 teve a convocação para envio de anexos encerrada às 15:32:21 de 19/01/2026. 5 anexos foram enviados pelo fornecedor CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30.
Pelo participante 02.092.332/0003-30	20/01/2026 às 10:55:27	Bom dia!
Sistema	28/01/2026 às 14:32:02	O item G1 está na etapa de julgamento de proposta no período de intenção de recursos, com acréscimo de 10 minutos a partir de agora - até 28/01/2026 14:42:02.
Sistema	30/01/2026 às 15:56:42	O item G1 está na etapa de habilitação de fornecedores no período de intenção de recursos, com acréscimo de 10 minutos a partir de agora - até 30/01/2026 16:06:42.

Termo de HOMOLOGAÇÃO_Compras.gov (2065377) SEI 2025.007562 / pg. 3622

Eventos do Grupo G1

Data/Hora	Descrição
19/01/2026 às 15:04:07	Fornecedor CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30 convocado para o envio de anexo. Prazo para encerrar o envio: 17:05:00 do dia 19/01/2026. Justificativa: Proposta e documentos complementares. .
19/01/2026 às 15:32:21	Fornecedor CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30 finalizou o envio de anexo.
09/02/2026 às 10:51:06	Fornecedor CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30 teve a proposta adjudicada, melhor lance: R$ 11.180.000,0000, valor negociado: R$ 10.616.278,0000.
09/02/2026 às 10:51:16	Item homologado.

Item 1 do Grupo G1 - Outros Serviços de Gerenciamento de Infraestrutura De Tecnologia da Informação e

EQUIPAMENTO HIPERCONVERGENTE –PLATAFORMA NUTANIX G9.

A descrição completa do Item 1 deve ser verificada no Termo de Referência Nª 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Quantidade:	4	Valor estimado:	R$ 588.062,6700 (unitário)
Unidade de fornecimento:	UNIDADE		R$ 2.352.250,6800 (total)
Intervalo mínimo entre lances:	R$ 10,0000	Situação:	Adjudicado e Homologado
Critério de julgamento:	Menor Preço		
Tratamento Diferenciado ME/EPP:	Sem benefícios ME/EPP (Art. 4ª, lei 14.133/2021)		

Adjudicado e Homologado por CPF ***.287.***-*3 - ANDRE VIRGILIO BELOTA SEFFAIR para CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, melhor lance: R$ 610.000,0000 (unitário) / R$ 2.440.000,0000 (total), valor negociado: R$ 588.062,0000 (unitário) / R$ 2.352.248,0000 (total)

Propostas do Item 1

Benefício Me/Epp: Conforme Art. 3ª da Lei Complementar nª 123, de 14 de dezembro de 2006
Equidade de gênero: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 11.430/2023
Programa de integridade: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 12.304/2024

Fornecedor	Valor ofertado	Situação
02.092.332/0003-30 - CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. Benefício Me/Epp: Não Equidade de gênero: Bronze Programa de integridade: Sim UF endereço: ES	R$ 610.000,0000 (unitário) R$ 2.440.000,0000 (total)	Proposta adjudicada

Valor proposta:	R$ 717.021,0000 (unitário) R$ 2.868.084,0000 (total)	Valor negociado:	R$ 588.062,0000 (unitário) R$ 2.352.248,0000 (total)	Quantidade ofertada:	4

Termo de HOMOLOGAÇÃO_Compras.gov (2065377) SEI 2025.007562 / pg. 3623

Fornecedor	Valor ofertado	Situação
39.532.571/0001-02 - GIUSEPPE ANTONIO FOGACA GERBALDO Benefício Me/Epp: Sim Equidade de gênero: Nenhum Programa de integridade: Não UF endereço: AM	R$ 1.500.000,0000 (unitário) R$ 6.000.000,0000 (total)	-

Valor proposta: R$ 1.800.000,0000 (unitário) R$ 7.200.000,0000 (total) Valor negociado: Não Realizado Quantidade ofertada: 4

Lances do Item 1

Data/hora	Participante	Lance
19/01/2026 às 10:10:55	02.092.332/0003-30	R$ 717.000,0000
19/01/2026 às 10:15:38	02.092.332/0003-30	R$ 680.000,0000
19/01/2026 às 10:19:52	02.092.332/0003-30	R$ 650.000,0000
19/01/2026 às 10:20:57	39.532.571/0001-02	R$ 1.500.000,0000
19/01/2026 às 10:21:03	02.092.332/0003-30	R$ 630.000,0000
19/01/2026 às 10:24:48	02.092.332/0003-30	R$ 610.000,0000

Item 2 do Grupo G1 - Outros Serviços de Gerenciamento de Infraestrutura De Tecnologia da Informação e

EQUIPAMENTO HIPERCONVERGENTE – PLATAFORMA NUTANIX G9 COM GPU.

A descrição completa do Item 2 deve ser verificada no Termo de Referência Nª 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Quantidade:	1	Valor estimado:	R$ 832.942,6700 (unitário)
Unidade de fornecimento:	UNIDADE		R$ 832.942,6700 (total)
Intervalo mínimo entre lances:	R$ 10,0000	Situação:	Adjudicado e Homologado
Critério de julgamento:	Menor Preço		
Tratamento Diferenciado ME/EPP:	Sem benefícios ME/EPP (Art. 4ª, lei 14.133/2021)		

Adjudicado e Homologado por CPF ***.287.***-*3 - ANDRE VIRGILIO BELOTA SEFFAIR para CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, melhor lance: R$ 850.000,0000 (unitário) / R$ 850.000,0000 (total), valor negociado: R$ 832.942,0000 (unitário) / R$ 832.942,0000 (total)

Propostas do Item 2

Benefício Me/Epp: Conforme Art. 3ª da Lei Complementar nª 123, de 14 de dezembro de 2006
Equidade de gênero: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 11.430/2023
Programa de integridade: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 12.304/2024

Fornecedor	Valor ofertado	Situação

Termo de HOMOLOGAÇÃO_Compras.gov (2065377) SEI 2025.007562 / pg. 3624

Fornecedor	Valor ofertado	Situação
02.092.332/0003-30 - CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. Benefício Me/Epp: Não Equidade de gênero: Bronze Programa de integridade: Sim UF endereço: ES	R$ 850.000,0000 (unitário) R$ 850.000,0000 (total)	Proposta adjudicada
Valor proposta: R$ 982.735,0000 (unitário) R$ 982.735,0000 (total)	Valor negociado: R$ 832.942,0000 (unitário) R$ 832.942,0000 (total)	Quantidade ofertada: 1
39.532.571/0001-02 - GIUSEPPE ANTONIO FOGACA GERBALDO Benefício Me/Epp: Sim Equidade de gênero: Nenhum Programa de integridade: Não UF endereço: AM	R$ 1.500.000,0000 (unitário) R$ 1.500.000,0000 (total)	-
Valor proposta: R$ 1.800.000,0000 (unitário) R$ 1.800.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1

Lances do Item 2

Data/hora	Participante	Lance
19/01/2026 às 10:12:01	02.092.332/0003-30	R$ 980.000,0000
19/01/2026 às 10:16:16	02.092.332/0003-30	R$ 920.000,0000
19/01/2026 às 10:21:04	39.532.571/0001-02	R$ 1.500.000,0000
19/01/2026 às 10:22:04	02.092.332/0003-30	R$ 870.000,0000
19/01/2026 às 10:24:06	02.092.332/0003-30	R$ 850.000,0000

Item 3 do Grupo G1 - Serviços de Gerenciamento de Sistemas Computacionais

SOFTWARE GESTÃO DAPLATAFORMA DE HIPERCONVERGENCIA NUTANIX.

A descrição completa do Item 3 deve ser verificada no Termo de Referência Nª 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Quantidade:	5	Valor estimado:	R$ 875.768,1500 (unitário)
Unidade de fornecimento:	UND SERVIÇO TÉCNICO		R$ 4.378.840,7500 (total)
Intervalo mínimo entre lances:	R$ 10,0000	Situação:	Adjudicado e Homologado
Critério de julgamento:	Menor Preço		
Tratamento Diferenciado ME/EPP:	Sem benefícios ME/EPP (Art. 4ª, lei 14.133/2021)		

Adjudicado e Homologado por CPF ***.287.***-*3 - ANDRE VIRGILIO BELOTA SEFFAIR para CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, melhor lance: R$ 790.000,0000 (unitário) / R$ 3.950.000,0000 (total)

Propostas do Item 3

Benefício Me/Epp: Conforme Art. 3ª da Lei Complementar nª 123, de 14 de dezembro de 2006
Equidade de gênero: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 11.430/2023
Programa de integridade: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 12.304/2024

Fornecedor	Valor ofertado	Situação

Termo de HOMOLOGAÇÃO_Compras.gov (2065377) SEI 2025.007562 / pg. 3625

Fornecedor	Valor ofertado	Situação
02.092.332/0003-30 - CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. Benefício Me/Epp: Não Equidade de gênero: Bronze Programa de integridade: Sim UF endereço: ES	R$ 790.000,0000 (unitário) R$ 3.950.000,0000 (total)	Proposta adjudicada
Valor proposta: R$ 925.188,0000 (unitário) R$ 4.625.940,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 5
39.532.571/0001-02 - GIUSEPPE ANTONIO FOGACA GERBALDO Benefício Me/Epp: Sim Equidade de gênero: Nenhum Programa de integridade: Não UF endereço: AM	R$ 1.500.000,0000 (unitário) R$ 7.500.000,0000 (total)	-
Valor proposta: R$ 5.000.000,0000 (unitário) R$ 25.000.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 5

Lances do Item 3

Data/hora	Participante	Lance
19/01/2026 às 10:12:18	02.092.332/0003-30	R$ 900.000,0000
19/01/2026 às 10:15:08	02.092.332/0003-30	R$ 850.000,0000
19/01/2026 às 10:16:38	02.092.332/0003-30	R$ 820.000,0000
19/01/2026 às 10:19:33	02.092.332/0003-30	R$ 790.000,0000
19/01/2026 às 10:21:13	39.532.571/0001-02	R$ 1.500.000,0000

Item 4 do Grupo G1 - Serviços de Gerenciamento de Sistemas Computacionais

SOFTWARE PARA PROCESSAMENTO DA PLATAFORMA DE HIPERCONVERGENCIA NUTANIX COM GPU.

A descrição completa do Item 4 deve ser verificada no Termo de Referência Nª 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Quantidade:	1	Valor estimado:	R$ 164.252,4000 (unitário)
Unidade de fornecimento:	UND SERVIÇO TÉCNICO		R$ 164.252,4000 (total)
Intervalo mínimo entre lances:	R$ 10,0000	Situação:	Adjudicado e Homologado
Critério de julgamento:	Menor Preço		
Tratamento Diferenciado ME/EPP:	Sem benefícios ME/EPP (Art. 4ª, lei 14.133/2021)		

Adjudicado e Homologado por CPF ***.287.***-*3 - ANDRE VIRGILIO BELOTA SEFFAIR para CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, melhor lance: R$ 190.000,0000 (unitário) / R$ 190.000,0000 (total), valor negociado: R$ 164.252,0000 (unitário) / R$ 164.252,0000 (total)

Propostas do Item 4

Benefício Me/Epp: Conforme Art. 3ª da Lei Complementar nª 123, de 14 de dezembro de 2006
Equidade de gênero: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 11.430/2023
Programa de integridade: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 12.304/2024

Fornecedor	Valor ofertado	Situação

Termo de HOMOLOGAÇÃO_Compras.gov (2065377) SEI 2025.007562 / pg. 3626

Fornecedor	Valor ofertado	Situação
02.092.332/0003-30 - CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. Benefício Me/Epp: Não Equidade de gênero: Bronze Programa de integridade: Sim UF endereço: ES	R$ 190.000,0000 (unitário) R$ 190.000,0000 (total)	Proposta adjudicada
Valor proposta: R$ 217.972,0000 (unitário) R$ 217.972,0000 (total)	Valor negociado: R$ 164.252,0000 (unitário) R$ 164.252,0000 (total)	Quantidade ofertada: 1
39.532.571/0001-02 - GIUSEPPE ANTONIO FOGACA GERBALDO Benefício Me/Epp: Sim Equidade de gênero: Nenhum Programa de integridade: Não UF endereço: AM	R$ 1.500.000,0000 (unitário) R$ 1.500.000,0000 (total)	-
Valor proposta: R$ 5.000.000,0000 (unitário) R$ 5.000.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1

Lances do Item 4

Data/hora	Participante	Lance
19/01/2026 às 10:12:39	02.092.332/0003-30	R$ 200.000,0000
19/01/2026 às 10:20:15	02.092.332/0003-30	R$ 190.000,0000
19/01/2026 às 10:21:22	39.532.571/0001-02	R$ 1.500.000,0000

Item 5 do Grupo G1 - Serviços de Gerenciamento de Sistemas Computacionais

LICENÇA PARA ARMAZENAMENTO DE DADOS NÃO ESTRUTURADOS - NUTANIX UNIFIED STORAGE.

A descrição completa do Item 5 deve ser verificada no Termo de Referência Nª 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Quantidade:	50	Valor estimado:	R$ 9.250,9800 (unitário)
Unidade de fornecimento:	UND SERVIÇO TÉCNICO		R$ 462.549,0000 (total)
Intervalo mínimo entre lances:	R$ 10,0000	Situação:	Adjudicado e Homologado
Critério de julgamento:	Menor Preço		
Tratamento Diferenciado ME/EPP:	Sem benefícios ME/EPP (Art. 4ª, lei 14.133/2021)		

Adjudicado e Homologado por CPF ***.287.***-*3 - ANDRE VIRGILIO BELOTA SEFFAIR para CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, melhor lance: R$ 11.000,0000 (unitário) / R$ 550.000,0000 (total), valor negociado: R$ 9.250,9800 (unitário) / R$ 462.549,0000 (total)

Propostas do Item 5

Benefício Me/Epp: Conforme Art. 3ª da Lei Complementar nª 123, de 14 de dezembro de 2006
Equidade de gênero: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 11.430/2023
Programa de integridade: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 12.304/2024

Fornecedor	Valor ofertado	Situação

Termo de HOMOLOGAÇÃO_Compras.gov (2065377) SEI 2025.007562 / pg. 3627

Fornecedor	Valor ofertado	Situação
02.092.332/0003-30 - CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. Benefício Me/Epp: Não Equidade de gênero: Bronze Programa de integridade: Sim UF endereço: ES	R$ 11.000,0000 (unitário) R$ 550.000,0000 (total)	Proposta adjudicada
Valor proposta: R$ 12.336,0000 (unitário) R$ 616.800,0000 (total)	Valor negociado: R$ 9.250,9800 (unitário) R$ 462.549,0000 (total)	Quantidade ofertada: 50
39.532.571/0001-02 - GIUSEPPE ANTONIO FOGACA GERBALDO Benefício Me/Epp: Sim Equidade de gênero: Nenhum Programa de integridade: Não UF endereço: AM	R$ 1.500.000,0000 (unitário) R$ 75.000.000,0000 (total)	-
Valor proposta: R$ 3.000.000,0000 (unitário) R$ 150.000.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 50

Lances do Item 5

Data/hora	Participante	Lance
19/01/2026 às 10:12:59	02.092.332/0003-30	R$ 12.000,0000
19/01/2026 às 10:19:09	02.092.332/0003-30	R$ 11.500,0000
19/01/2026 às 10:21:29	39.532.571/0001-02	R$ 1.500.000,0000
19/01/2026 às 10:22:42	02.092.332/0003-30	R$ 11.000,0000

Item 6 do Grupo G1 - Serviços de Gerenciamento de Sistemas Computacionais

SOFTWARE DE BACKUP DE DADOS.

A descrição completa do Item 6 deve ser verificada no Termo de Referência Nª 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Quantidade:	1	Valor estimado:	R$ 2.005.354,2600 (unitário)
Unidade de fornecimento:	UND SERVIÇO TÉCNICO		R$ 2.005.354,2600 (total)
Intervalo mínimo entre lances:	R$ 10,0000	Situação:	Adjudicado e Homologado
Critério de julgamento:	Menor Preço		
Tratamento Diferenciado ME/EPP:	Sem benefícios ME/EPP (Art. 4ª, lei 14.133/2021)		

Adjudicado e Homologado por CPF ***.287.***-*3 - ANDRE VIRGILIO BELOTA SEFFAIR para CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, melhor lance: R$ 900.000,0000 (unitário) / R$ 900.000,0000 (total)

Propostas do Item 6

Benefício Me/Epp: Conforme Art. 3ª da Lei Complementar nª 123, de 14 de dezembro de 2006
Equidade de gênero: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 11.430/2023
Programa de integridade: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 12.304/2024

Fornecedor	Valor ofertado	Situação

Termo de HOMOLOGAÇÃO_Compras.gov (2065377) SEI 2025.007562 / pg. 3628

Fornecedor	Valor ofertado	Situação
02.092.332/0003-30 - CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. Benefício Me/Epp: Não Equidade de gênero: Bronze Programa de integridade: Sim UF endereço: ES	R$ 900.000,0000 (unitário) R$ 900.000,0000 (total)	Proposta adjudicada
Valor proposta: R$ 994.639,0000 (unitário) R$ 994.639,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
39.532.571/0001-02 - GIUSEPPE ANTONIO FOGACA GERBALDO Benefício Me/Epp: Sim Equidade de gênero: Nenhum Programa de integridade: Não UF endereço: AM	R$ 1.500.000,0000 (unitário) R$ 1.500.000,0000 (total)	-
Valor proposta: R$ 5.000.000,0000 (unitário) R$ 5.000.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1

Lances do Item 6

Data/hora	Participante	Lance
19/01/2026 às 10:13:14	02.092.332/0003-30	R$ 950.000,0000
19/01/2026 às 10:17:16	02.092.332/0003-30	R$ 900.000,0000
19/01/2026 às 10:21:36	39.532.571/0001-02	R$ 1.500.000,0000

Item 7 do Grupo G1 - Outros Serviços de Gerenciamento de Infraestrutura De Tecnologia da Informação e

EQUIPAMENTO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES.

A descrição completa do Item 7 deve ser verificada no Termo de Referência Nª 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Quantidade:	1	Valor estimado:	R$ 373.771,3800 (unitário)
Unidade de fornecimento:	UNIDADE		R$ 373.771,3800 (total)
Intervalo mínimo entre lances:	R$ 10,0000	Situação:	Adjudicado e Homologado
Critério de julgamento:	Menor Preço		
Tratamento Diferenciado ME/EPP:	Sem benefícios ME/EPP (Art. 4ª, lei 14.133/2021)		

Adjudicado e Homologado por CPF ***.287.***-*3 - ANDRE VIRGILIO BELOTA SEFFAIR para CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, melhor lance: R$ 230.000,0000 (unitário) / R$ 230.000,0000 (total)

Propostas do Item 7

Benefício Me/Epp: Conforme Art. 3ª da Lei Complementar nª 123, de 14 de dezembro de 2006
Equidade de gênero: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 11.430/2023
Programa de integridade: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 12.304/2024

Fornecedor	Valor ofertado	Situação

Termo de HOMOLOGAÇÃO_Compras.gov (2065377) SEI 2025.007562 / pg. 3629

Fornecedor	Valor ofertado	Situação
02.092.332/0003-30 - CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. Benefício Me/Epp: Não Equidade de gênero: Bronze Programa de integridade: Sim UF endereço: ES	R$ 230.000,0000 (unitário) R$ 230.000,0000 (total)	Proposta adjudicada
Valor proposta: R$ 267.620,0000 (unitário) R$ 267.620,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
39.532.571/0001-02 - GIUSEPPE ANTONIO FOGACA GERBALDO Benefício Me/Epp: Sim Equidade de gênero: Nenhum Programa de integridade: Não UF endereço: AM	R$ 1.500.000,0000 (unitário) R$ 1.500.000,0000 (total)	-
Valor proposta: R$ 5.000.000,0000 (unitário) R$ 5.000.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1

Lances do Item 7

Data/hora	Participante	Lance
19/01/2026 às 10:13:28	02.092.332/0003-30	R$ 250.000,0000
19/01/2026 às 10:18:51	02.092.332/0003-30	R$ 230.000,0000
19/01/2026 às 10:21:43	39.532.571/0001-02	R$ 1.500.000,0000

Item 8 do Grupo G1 - Serviços de Gerenciamento de Sistemas Computacionais

SOFTWARE DO REPOSITÓRIO DE ARMAZENAMENTO DE DADOS DE BACKUP ON-PREMISES.

A descrição completa do Item 8 deve ser verificada no Termo de Referência Nª 28.2025.DTIC.2002143.2025.007562, Anexo I ao Edital do certame.

Quantidade:	1	Valor estimado:	R$ 1.404.862,4000 (unitário)
Unidade de fornecimento:	UND SERVIÇO TÉCNICO		R$ 1.404.862,4000 (total)
Intervalo mínimo entre lances:	R$ 10,0000	Situação:	Adjudicado e Homologado
Critério de julgamento:	Menor Preço		
Tratamento Diferenciado ME/EPP:	Sem benefícios ME/EPP (Art. 4ª, lei 14.133/2021)		

Adjudicado e Homologado por CPF ***.287.***-*3 - ANDRE VIRGILIO BELOTA SEFFAIR para CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, melhor lance: R$ 1.200.000,0000 (unitário) / R$ 1.200.000,0000 (total)

Propostas do Item 8

Benefício Me/Epp: Conforme Art. 3ª da Lei Complementar nª 123, de 14 de dezembro de 2006
Equidade de gênero: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 11.430/2023
Programa de integridade: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 12.304/2024

Fornecedor	Valor ofertado	Situação

Termo de HOMOLOGAÇÃO_Compras.gov (2065377) SEI 2025.007562 / pg. 3630

Fornecedor	Valor ofertado	Situação
02.092.332/0003-30 - CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. Benefício Me/Epp: Não Equidade de gênero: Bronze Programa de integridade: Sim UF endereço: ES	R$ 1.200.000,0000 (unitário) R$ 1.200.000,0000 (total)	Proposta adjudicada
Valor proposta: R$ 1.355.400,0000 (unitário) R$ 1.355.400,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1
39.532.571/0001-02 - GIUSEPPE ANTONIO FOGACA GERBALDO Benefício Me/Epp: Sim Equidade de gênero: Nenhum Programa de integridade: Não UF endereço: AM	R$ 1.500.000,0000 (unitário) R$ 1.500.000,0000 (total)	-
Valor proposta: R$ 5.000.000,0000 (unitário) R$ 5.000.000,0000 (total)	Valor negociado: Não Realizado	Quantidade ofertada: 1

Lances do Item 8

Data/hora	Participante	Lance
19/01/2026 às 10:13:49	02.092.332/0003-30	R$ 1.300.000,0000
19/01/2026 às 10:17:41	02.092.332/0003-30	R$ 1.200.000,0000
19/01/2026 às 10:21:52	39.532.571/0001-02	R$ 1.500.000,0000

Item 9 do Grupo G1 - Switch

Switch Quantidade Portas: 48UN, Tipo Portas: Sfp28, Velocidade Porta: 25 Gb, Alimentação: 110/220V, Características Adicionais: 50 Cm De Cabo De Empilhamento, Tipo: Padrão Rack 19"

Quantidade:	2	Valor estimado:	R$ 262.143,6600 (unitário)
Unidade de fornecimento:	Unidade		R$ 524.287,3200 (total)
Intervalo mínimo entre lances:	R$ 10,0000	Situação:	Adjudicado e Homologado
Critério de julgamento:	Menor Preço		
Tratamento Diferenciado ME/EPP:	Sem benefícios ME/EPP (Art. 4ª, lei 14.133/2021)		

Adjudicado e Homologado por CPF ***.287.***-*3 - ANDRE VIRGILIO BELOTA SEFFAIR para CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ 02.092.332/0003-30, melhor lance: R$ 435.000,0000 (unitário) / R$ 870.000,0000 (total), valor negociado: R$ 262.143,5000 (unitário) / R$ 524.287,0000 (total)

Propostas do Item 9

Benefício Me/Epp: Conforme Art. 3ª da Lei Complementar nª 123, de 14 de dezembro de 2006
Equidade de gênero: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 11.430/2023
Programa de integridade: Conforme termos previsos na Lei nª 14.133/2021 e no Decreto nª 12.304/2024

Fornecedor	Valor ofertado	Situação

Termo de HOMOLOGAÇÃO_Compras.gov (2065377) SEI 2025.007562 / pg. 3631

Fornecedor	Valor ofertado	Situação
02.092.332/0003-30 - CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. Benefício Me/Epp: Não Equidade de gênero: Bronze Programa de integridade: Sim UF endereço: ES	R$ 435.000,0000 (unitário) R$ 870.000,0000 (total)	Proposta adjudicada

Marca/Fabricante: JUNIPER
Modelo/versão: QFX5120
Valor proposta: R$ 515.793,0000 (unitário) R$ 1.031.586,0000 (total)
Valor negociado: R$ 262.143,5000 (unitário) R$ 524.287,0000 (total)
Quantidade ofertada: 2

39.532.571/0001-02 - GIUSEPPE ANTONIO FOGACA GERBALDO Benefício Me/Epp: Sim Equidade de gênero: Nenhum Programa de integridade: Não UF endereço: AM	R$ 1.500.000,0000 (unitário) R$ 3.000.000,0000 (total)	-

Marca/Fabricante: Switch
Modelo/versão: Switch
Valor proposta: R$ 5.000.000,0000 (unitário) R$ 10.000.000,0000 (total)
Valor negociado: Não Realizado
Quantidade ofertada: 2

Lances do Item 9

Data/hora	Participante	Lance
19/01/2026 às 10:14:10	02.092.332/0003-30	R$ 512.000,0000
19/01/2026 às 10:18:06	02.092.332/0003-30	R$ 480.000,0000
19/01/2026 às 10:18:34	02.092.332/0003-30	R$ 450.000,0000
19/01/2026 às 10:22:02	39.532.571/0001-02	R$ 1.500.000,0000
19/01/2026 às 10:23:10	02.092.332/0003-30	R$ 435.000,0000

Fase Recursal do Item/Grupo *

* Maiores detalhes sobre recursos, contrarrazões, decisões e revisões deverão ser consultados no sistema.

Sessão 1

Prazos:

Intenção de recurso no julgamento: 28/01/2026 14:42:02
Intenção de recurso na habilitação: 30/01/2026 16:06:42

Termo de HOMOLOGAÇÃO_Compras.gov (2065377) SEI 2025.007562 / pg. 3632

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS
Avenida Coronel Teixeira, 7995 - Bairro Nova Esperança - CEP 69037-473 - Manaus - AM - www.mpam.mp.br

OFÍCIO Nº 51.2026.CPL.2065378.2025.007562

Manaus, 09 de fevereiro de 2026.

Ao Senhor

IURY FECHINE RAMOS

Chefe do Setor de Compras e Serviços

Ao Senhor

ADENILSON ROBERTO DE OLIVEIRA FILHO

Chefe da Divisão de Constratos e Convêcnios - DCCON

Ao Senhor

EUDO LIMA DE ASSIS JUNIOR

Diretor de Tecnologia da Informação e Comunicação - DTIC

Assunto: Encerramento do Pregão Eletrônico N.° 94.001/2026-CPL/MP/PGJ - Adjudicação e homologação do resultado.

Senhores Chefes e Diretor,

Cumprimentando-os cordialmente, sirvo-me do presente para informar que, no âmbito do **PREGÃO ELETRÔNICO N.º 94.001/2026-CPL/MP/PGJ,** cujo objeto consiste na *contratação de empresa especializada para o fornecimento, implantação, configuração e transferência de conhecimento de uma* ***solução de datacenter****, contemplando infraestrutura integrada de hardware e software, incluindo unidade de processamento gráfico (GPU) e ambiente dedicado para proteção e armazenamento de dados de backup,* ***com garantia de 60 (sessenta) meses,*** o referido certame foi devidamente encerrado, com a adjudicação e homologação do resultado do procedimento licitatório, conforme abaixo destacado:

CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA (FILIAL),CNPJ N.º 02.092.332/0003-30, pelos seguintes valores:

a) ITEM 1 - pelo valor negociado unitário de R$ 588.062,00

(*quinhentos e oitenta e oito mil sessenta e dois reais*);

b) ITEM 2 - pelo valor negociado unitário de R$ 832.942,00 (*oitocentos e trinta e dois mil novecentos e quarenta e dois reais*);

c) ITEM 3 - pelo melhor lance unitário de R$ 790.000,00 (*setecentos e noventa mil reais*);

d) ITEM 4 - pelo valor negociado unitário de R$ 164.252,00 (*cento e sessenta e quatro mil duzentos e cinquenta e dois reais*);

e) ITEM 5 - pelo valor negociado unitário de R$ 9.250,98 (*nove mil duzentos e cinquenta reais e noventa e oito centavos*);

f) ITEM 6 - pelo melhor lance unitário de R$ 900.000,00 (*novecentos mil reais*);

g) ITEM 7 - pelo melhor lance unitário de R$ 230.000,00 (*duzentos e trinta mil reais*);

h) ITEM 8 - pelo melhor lance unitário de R$ 1.200.000,00 (*um milhão duzentos mil reais*); e

i) ITEM 9 - pelo valor negociado unitário de R$ 262.143,50 (*duzentos e sessenta e dois mil cento e quarenta e três reais e cinquenta centavos*);

Desta forma, encaminham-se os autos para conhecimento e adoção das providências que entenderem cabíveis.

Atenciosamente,

Sarah Madalena B. Côrtes de Melo
Pregoeira - Portaria nº 66/2026/SUBADM

Documento assinado eletronicamente por **Sarah Madalena Barbosa Santos Cortes**, **Presidente da Comissão Permanente de Licitação - CPL**, em 09/02/2026, às 11:40, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.mpam.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2065378** e o código CRC **688AC71A**.